Financial Action Task Force

Groupe d'action financière

Asia/Pacific Group
on Money Laundering

Financial action Task Force
Asia/Pacific Group on money laundering

THIRD MUTUAL EVALUATION REPORT ON
ANTI-MONEY LAUNDERING AND
COMBATING THE FINANCING OF TERRORISM

UNITED STATES OF AMERICA

AS ADTOPED BY THE FATF ON 23 JUNE 2006

ADOPTED BY THE APG ON 4 JULY 2006

© 2006 FATF/OECD
All rights reserved. No reproduction or translation of this publication may be made without prior written permission.
Applications for such permission should be made to:
FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France
Fax 33-1-44306137 or contact@fatf-gafi.org

TABLE OF CONTENTS

Preface - information and methodology used for the evaluation 2
1. Section 1 3
1.1 General information on the country and its economy 3
1.2 General Situation of Money Laundering and Financing of Terrorism 6
1.3 Overview of the Financial Sector and DNFBP 8
1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements 13
1.5 Overview of strategy to prevent money laundering and terrorist financing 14
2 Legal System and Related Institutional Measures 24
2.1 Criminalization of Money Laundering (R.1 & 2) 24
2.2 Criminalization of Terrorist Financing (SR.II) 37
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3) 42
2.4 Freezing of funds used for terrorist financing (SR.III) 49
2.5 The Financial Intelligence Unit and its functions (R.26) 57
2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offenses, and for confiscation and freezing (R.27 & 28) 65
2.7 Cross Border Declaration or Disclosure (SR.IX) 69
3. Preventive Measures - Financial Institutions 79
3.1 Risk of money laundering or terrorist financing 82
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8) 87
3.3 Third parties and introduced business (R.9) 116
3.4 Financial institution secrecy or confidentiality (R.4) 118
3.5 Record keeping and wire transfer rules (R.10 & SR.VII) 120
3.6 Monitoring of transactions and relationships (R.11 & 21) 129
3.7 Suspicious transaction and other reporting (R.13-14, 19, 25 & SR.IV) 134
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22) 145
3.9 Shell banks (R.18) 155
3.10 Supervision and oversight (R.17, 23, 25 & 29) 156
3.11 Money or value transfer services (SR.VI) 181
4. Preventive Measures – Designated Non-Financial Businesses and Professions 189
4.1 Customer due diligence and record-keeping (R.12) 192
4.2 Monitoring transactions and other issues (R.16) 196
4.3 Regulation, supervision and monitoring (R. 17, 24 & 25) 201
4.4 Other non-financial businesses and professions - Modern secure transaction techniques (R.20) 213
5. Legal Persons and Arrangements & Non-Profit Organizations 215
5.1 Legal Persons – Access to beneficial ownership and control information (R.33) 215
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34) 225
5.3 Non-profit organizations (SR.VIII) 228
6. National and International Cooperation 238
6.1 National cooperation and coordination (R.31) 238
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I) 245
6.3 Mutual Legal Assistance (R.36-38 & SR.V) 246
6.4 Extradition (R.39, 37 & SR.V) 255
6.5 Other Forms of International Co-operation (R.40 & SR.V) 259
7 Resources and Statistics 268
7.1 Resources of Competent Authorities (R.30) 268
7.2 Statistics (R.32) 280
7.3 Other relevant AML/CFT measures or issues 283
7.4 General framework for AML/CFT system (see also section 1.1) 283

Preface - information and methodology used for the evaluation[1]

1. The evaluation of the anti-money laundering (AML)[2] and combating the financing of terrorism (CFT) regime of the United States (U.S.) was based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004.[3] The evaluation considered the laws, regulations and other materials supplied by the U.S., and information obtained by the evaluation team during its two on-site visits to the U.S. from 7-18 November 2005 and 9-23 January 2006, and subsequently. During the on-sites the evaluation team met with officials and representatives of relevant U.S. federal, state, and local government agencies and the private sector. A list of the agencies and organizations met is set out in Annex 2 to the mutual evaluation report.

2. This was a joint evaluation of the FATF and the Asia Pacific Group (APG). The evaluation was conducted by an assessment team which consisted of experts from the FATF and APG in criminal law, law enforcement and regulatory issues. The team was led by Mr. Alain Damais, Executive Secretary of the FATF, and Mr. Rick McDonell, Head of the APG Secretariat, and included: Mr. Dick Bos, Deputy Head of the Dutch FIU MOT (Netherlands) who participated as a law enforcement expert; Mr. Richard Chalmers, Adviser, International Strategy and Policy Co-ordination, Financial Services Authority (United Kingdom) who participated as a financial expert; Ms. Koid Swee Lian, Director, Bank Negara Malaysia's (Central Bank of Malaysia), Financial Intelligence Unit (Malaysia) who participated as a financial expert; Ms. Judith Pini, Senior Legal Adviser, Criminal Justice Division, Attorney-General's Department (Australia) who participated as a legal expert; Dr. Riccardo Sansonetti, Head of Section, Federal Finance Administration (Switzerland) who participated as a financial expert; Ms. Valerie Schilling, Administrator, FATF Secretariat; and Mr. Boudewijn Verhelst, Deputy Attorney-General, Deputy Director of the Belgian FIU CTIF/CFI (Belgium) who participated as a legal expert. The assessment team reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all these systems.[4]

3. This report provides a summary of the AML/CFT measures in place in the U.S. as of the date of the second on-site visit, and up to 5 May 2006[5]. It describes and analyses those measures, and provides recommendations on how certain aspects of the system could be strengthened (see Table 2). It also sets out the U.S.'s levels of compliance with the FATF 40+9 Recommendations (see Table 1).[6]

[1] Generally, FATF reports are written in United Kingdom English; however, this report is written in United States (U.S.) English to avoid any confusion that may be caused by the spellings of U.S. agencies or citations from U.S. laws, regulations and other sources.

[2] See Annex 1 for a complete list of abbreviations and acronyms.

[3] As updated on 14 October 2005.

[4] See Annex 2 for a detailed list of all bodies met during the on-site mission. See Annex 3 for copies of the key laws, regulations and other measures. See Annex 4 for a list of all laws, regulations and other materials received and reviewed by the assessors.

[5] The measures taken into account after the on-site visit were restricted to issues that the assessment team had been able to discuss with the authorities during the on-site visits, but which may have been published or come into effect at a later date.

[6] Also see Table 1 for an explanation of the compliance ratings (C, LC, PC and NC).

MUTUAL EVALUATION REPORT

1. SECTION 1

1.1 General information on the country and its economy

1. The United States of America (U.S.) is comprised of 50 states and one district. The U.S. covers an area of 9.6 million square kilometers, shares borders with Canada to the north and Mexico to the south, and is flanked by the Atlantic Ocean to the east and the Pacific Ocean to the west. The U.S. holds fourteen territories, nine of which are uninhabited or have no indigenous inhabitants: American Samoa, Baker Island, Guam, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Northern Mariana Islands, Palmyra Atoll, Puerto Rico, the U.S. Virgin Islands, and Wake Island.[7] The capital of the U.S. is Washington, District of Columbia (DC). As of 2005, the estimated population is 295,734,134 having a mean age of 36 and life expectancy averaging 77.7 years. The official language is English and the literacy rate is 97% (as of 1999). The U.S. is a developed, industrial country with a free-market economy. The U.S. is the largest economy in the world with GDP valued in 2004 at USD 11.75 trillion, broken up into the service (79.4%), industry (19.7%) and agricultural (0.9%) sectors.

System of government

2. The U.S. is a constitution-based federal republic with executive, legislative, and judicial branches. The executive branch comprises an elected President and Vice-President, and an appointed Cabinet. The federal legislative branch, known as Congress, consists of a House of Representatives (containing 435 members, with each state's number of representatives commensurate with its population) and the Senate (containing 100 members—two per state). The judicial branch is made up of the U.S. Supreme Court, Federal Courts of Appeal, and Federal District Courts. There are also courts on the state level, including state-wide and local county-level courts.

Legal system and hierarchy of laws

3. The federal court system is based on English common law. Each state has its own unique legal system, of which all but one (Louisiana) is based on common law. The U.S. Constitution (adopted in 1789) enumerates the broad areas where the federal government has legislative authority. Some powers are exclusively federal because the Constitution limits or prohibits the use of the power by states (e.g. treaty power, coinage of money) or because the nature of the power itself is such that it can be exercised only by the federal government (e.g. declaration of war, federal citizenship). All powers not explicitly delegated to the federal government are reserved to the states. However, because federal powers are given an expansive interpretation, little state power is exclusive.

4. Regulations are promulgated in accordance with the practices and procedures set out in the Administrative Procedure Act (APA) [5 United States Code (USC) 500 (1946)]. Among other requirements, the APA generally requires all government agencies with powers to administer federal laws to give public notice and solicit public comment on substantive rules of general applicability adopted as authorized by law. This procedure: informs the public of "proposed rules" before they take effect; allows the public to comment on the proposed rules and provide additional data to the agency; and enables the public to access the "rulemaking record" and analyze the data and analysis behind a proposed rule. Additionally, the relevant agency can analyze and respond to the public's comments. The process also creates an administrative record of the agency's analysis and the procedures which can be reviewed by a judge or others to ensure that the correct process was followed.

[7] American Samoa, Guam, the Northern Mariana Islands, Puerto Rico and the Virgin Islands are inhabited.

5. A self implementing statute is enforceable on and after its effective date. Some laws, however, require implementing regulations to give them effect and are not fully enforceable until such implementing regulations have been issued. Implementing regulations adopted pursuant to a law are fully enforceable once they have been properly promulgated in accordance with the procedure set out below and on the published effective date.

6. In general, the agency that is undertaking to promulgate a new regulation publishes a "notice of proposed rulemaking" (NPRM) in the Federal Register (FR), and specifically seeks public comment on its proposed action within a prescribed time frame. Such a notice includes the legal authority for the agency's issuance of the rule, proposed regulatory language (the "proposed rule"), and a full discussion of the justification and analysis behind the rule. Proposed rules have no force and effect. After the close of the comment period, the promulgating agency considers all comments timely submitted in response to the notice of proposed rulemaking. The agency may then adopt and publish a "final rule" which provides notice to the public of the text of the rule as adopted, a summary and analysis of comments received and the rationale for adopting the rule in the form published. In general, a final rule does not become effective immediately, but rather specifies an effective date, usually 30 days after publication of the final rule in the Federal Register. A final rule becomes effective following publication, on its effective date. If after publishing the notice of proposed rulemaking the agency feels there are certain issues upon which it wishes to receive additional comments, the agency may take various steps to continue to solicit additional comments, before issuing a final rule, including the issuance of an "interim final rule" (IFR). An IFR is enforceable as a final rule upon its effective date. After receiving additional public input, the agency may then publish a final rule. The IFR remains in effect until superseded by the issuance of a subsequent final rule.

Court system

7. The U.S. court system is comprised of many different court systems: a federal system and 50 state systems. Each has its own organization, structure, procedures and budget. Depending on the specific structure of the state's court system, trial courts may be city or municipal courts, justice of the peace courts, county or circuit courts, or even regional trial courts. Every state has a tier of appellate courts and a court of last resort, generally called the "supreme court." Although supreme court decisions are final within a state court system, in appropriate circumstances, review may be made by a federal court with jurisdiction. The federal system consists of 94 Federal District Courts, 13 U.S. Courts of Appeals, and the U.S. Supreme Court which is the country's highest court. As federal judges are appointed for their lifetime, they are free from political pressures concerning their tenure. The Speedy Trial Act imposes statutory time limits in federal criminal cases. Defendants are defended by lawyers who are required to represent their clients. The judiciary has many tools to enforce court decisions, including the power to order the seizure and sale of property to satisfy a judgment, or to imprison a defendant who has violated a restraining or injunction order.

Compliance culture

8. Financial institutions and non-financial businesses have focused more on anti-money laundering (AML)/counter-terrorist financing (CFT) compliance since the enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) in 2001. Title III of the USA PATRIOT Act amended the Bank Secrecy Act (BSA) (the primary statute which establishes anti-money laundering compliance requirements) to require certain financial institutions and businesses through regulations issued by the Financial Crimes Enforcement Network (FinCEN), to establish proactive AML Programs. These AML/CFT compliance requirements have also fostered the involvement of other entities, such as industry associations, trade groups, and independent consultants that participate in creating industry standards, provide individualized guidance, suggest best practices and reinforce the necessity of compliance. Transparency, good corporate governance and strong AML Programs are further encouraged as a result of a social stigma against doing business with entities that are associated with

criminal activity. The culture of the U.S. is one in which individuals expect that the businesses they interact with will not have criminal ties, will protect themselves from abuse by money launderers and terrorist financiers, and will sever ties with any entity that is abusing their business relationships. Institutions with vulnerabilities associated with money laundering (ML) or terrorist financing (FT), significantly increase their potential risk for loss of income and loss of reputation, in addition to civil and/or criminal penalties. Moreover, the U.S. media takes an active interest in these investigations and publicizes details of money laundering and terrorist financing abuses discovered involving financial institutions or non-financial businesses. All of this contributes to a strong culture of AML/CFT compliance in financial institutions and non-financial businesses.

Transparency, good governance, ethics and measures against corruption

9. The U.S. signed the Organization for Economic Co-operation and Development (OECD) 1997 Convention on Combating Bribery of Foreign Public Officials in International Transactions (the OECD Bribery Convention) on 17 December 1997 and ratified it on 10 November 1998. The U.S. signed the United Nations Convention against Transnational Organized Crime (2001) (Palermo Convention) on 13 December 2000 and ratified it on 3 November 2005.

10. The U.S. system of government promotes transparency and good governance through its tripartite structure of three co-equal branches (the executive, legislative and judicial branches) checking and balancing each other, and the constitutional guarantees of free speech and free press. Additionally, each level of government has various independent and semi-independent organizations that were established to prevent waste, fraud and corruption.

11. Public corruption is addressed through multiple federal, state, and local mechanisms. At the federal level, the Code of Federal Regulations (CFR) sets out standards of ethical conduct that are enforced by the Office of Government Ethics (which is an executive branch-wide office). The Federal Criminal Code (FCC) prohibits bribery, gratuities, conflicts of interest, theft, and fraud by government employees. These laws are actively enforced. The FCC also contains a broad spectrum of statutes that prohibit, not only corrupt conduct by federal officials, but also relationships that can lead to corruption, such as various conflicts of interest. The FCC also addresses corruption by state and local officials where federal jurisdiction is found to exist.

12. High ranking federal officials, as well as those in certain sensitive positions, are required to file annual financial disclosure statements that are kept on file, in the former case, publicly, and in the latter case, with supervisors who review them for conflicts of interest. Federal salaries are structured to be reasonably high and commensurate with the employees' responsibilities. Police agencies at all levels have regulations governing conduct. Government lawyers are also bound by ethical rules of their licensing organizations, usually state supreme courts and/or state bar organizations.

13. The U.S. Congress has broad investigative authority to address general issues related to public corruption as well as specific allegations of corrupt activity at all levels of government. The Department of Justice (DOJ) is the principal government agency responsible for investigating and prosecuting public corruption offenses at the federal level through its U.S. Attorney's Offices in 94 districts and through specialized components in Washington, DC. The DOJ has dedicated anti-corruption units in most of these locations. Additionally, it directs the primary federal investigative function through the Federal Bureau of Investigation (FBI). Other federal agencies—such as the Internal Revenue Service (IRS), the Securities and Exchange Commission (SEC), and the Office of Government Ethics—also have specialized components responsible for addressing pertinent aspects of public corruption. There is also an extensive network of Inspectors General (IG) with broad authority to identify and investigate fraud, waste, and abuse within their respective agencies. All of these investigative components conduct criminal investigations under the DOJ umbrella. Federal, state and local authorities co-ordinate investigations and prosecutions as appropriate; however, only the DOJ can bring federal criminal charges.

14. Other federal organizations that are dedicated to ethics and anti-corruption are: the Treasury Inspector General for Tax Administration (TIGTA); Offices of Professional Responsibility for the DOJ, DEA and the FBI; the Office of Government Ethics; the Government Accountability Office (GAO) (an independent federal agency that, upon request from Congress, evaluates federal programs, audits federal expenditures, issues legal opinions and advises Congress and the heads of executive agencies about how to make government more effective and responsive); the House and Senate Ethics Committees; the Public Integrity Section of DOJ; and various anti-corruption units in field offices of the DOJ and the FBI. State and large local governments tend to have similar bodies. Each of these organizations has enabling legislation or regulations that set out their duties and the proper scope of their work. All of these anti-corruption efforts are reinforced by a vigorous free press and an array of non-government organizations that comprehensively monitor government activities to promote transparency and accountability.

1.2 General Situation of Money Laundering and Financing of Terrorism

15. The U.S. government is reviewing, on an ongoing basis, the money laundering and terrorist financing risk at the national level. It recently published the "U.S. Money Laundering Threat Assessment" (in January 2006) which is the product of an interagency working group comprised of a spectrum of U.S. government agencies that study and combat money laundering. This is the first such assessment done on a national level, and is a compilation of views of 16 government agencies, bureaus and offices. This report reviews the threats and vulnerabilities in a number of sectors, including banking, money services businesses (MSBs), insurance companies, casinos, shell companies and trusts.

Money Laundering

16. Proceeds from the sale of illicit narcotics are a major source of demand for money laundering in the U.S. There is ample evidence that drug arrests continue to climb and that the cities topping the asset seizure list in terms of the total dollar amount seized (New York, Miami and Los Angeles) are centers of the drug trade (Annex 5, Table 1 and 2). However, the top ten cities identified from the asset seizure data are not all necessarily the top drug markets in the U.S., confirming that other criminal activity contributes to the demand for money laundering.[8] The primary offenses for which individuals were sentenced in the top ten cities on the asset seizure list are drug trafficking, immigration violations, fraud, and firearms violations (Annex 5, Table 3).

17. Historically, the most prevalent method of money laundering reported in suspicious activity reports (SAR) is structured cash deposits followed by immediate and regular international wire transfers that are conducted through correspondent accounts either by individuals or businesses. Other methods include the use of bulk-cash smuggling, trade-based money laundering, insurance products, casinos and MSBs, including informal value transfer services (IVTS) to transmit illicit proceeds. Since the implementation of stricter customer due diligence and recordkeeping requirements, the IRS-Criminal Investigation (IRS-CI) has noted that financial institutions are less used to facilitate money laundering. Techniques and trends that continue to be observed by law enforcement agencies can be summarized as follows.

18. **Banking sector:** Money launderers may smurf transactions at different locations of the same or different financial institutions. Cash-intensive businesses may inflate legitimate cash revenues to disguise the deposit of cash proceeds. Correspondent and payable through accounts may have "nested" accounts that provide indirect access to the U.S. financial system by allowing a foreign bank that may not have a direct relationship with a U.S. financial institution to use another bank's U.S. account.

[8] Washington, DC, Tampa, and Philadelphia are examples of cities that have larger drug markets than several of the cities on the top ten asset seizure list.

19. **Insurance sector:** Money laundering through insurance has been generally confined to life insurance and annuity products. The inclusion of investment products with the usual portfolio of insurance policies has increased the potential for insurance companies to be used as ML conduits.

20. **Money services businesses (MSB) sector:** FBI field offices consistently identified the use of MSBs as the third-most utilized money laundering method that they encounter, after formal banking systems and cash businesses. SARs indicate that there is a concentration of suspicious, and potentially illicit, financial activity in the U.S. in densely populated cities and along the southwest border. Law enforcement reporting indicates that a large amount of illicit funds laundered through money transmitter services are sent to the southwest border of the U.S.—particularly southern Arizona, where 12 U.S. dollars (USD) is received for every USD 1 sent. This is accounted for in bulk cash smuggling to Mexico. FBI field offices throughout the U.S. are observing increased money laundering through commercial check cashing services and structured deposits involving check cashing services. Certain elements of the currency exchange sector, such as casas de cambio, may play a major role in money laundering operations, particularly for narcotics organizations.

21. **On-line payment systems:** Money laundering through on-line payment systems (some of which may function as on-line money transmitters) has proven problematic for law enforcement given that the investigative trail often ends when cyber systems are outside of any jurisdictional requirements for AML/CFT programs, customer identification or record-keeping—particularly when those online systems accept cash and money orders to fund accounts.

22. **Bulk cash smuggling:** Between 2001 and 2003, seized currency (mostly drug proceeds)[9] often originated in California, Illinois, New York, and Texas and was bound for Arizona, California, Florida, and Texas [seizure data from the El Paso Intelligence Center (EPIC)]. SARs filed by U.S. financial institutions tend to support the view that some of the cash smuggled out of the U.S. to Mexico is immediately repatriated. SARs have reported patterns of large wire transactions (USD 1.5 million or more per transaction) to U.S. payees from Mexican money exchange houses and other financial institutions.

23. **Trade-based money laundering:** The Black Market Peso Exchange (BMPE) is the largest known money laundering system in the western hemisphere, responsible for moving an estimated USD 5 billion worth of drug proceeds per year from the U.S. back to Colombia.[10] Other trade-based methods of money laundering include manipulating trade documents to over- or under-pay for imports and exports, and using criminal proceeds to buy gems or precious metals.

24. **Shell companies:** FinCEN reports that 397 SARs (representing an aggregate of USD 4 billion) were filed between April 1996 and January 2004 involving shell companies, and the use of foreign correspondent bank accounts.

25. **Casinos:** Money laundering methods that involve casinos include exchanging illicit cash for casino chips and then either: (1) holding the chips for a period of time and later cashing them in for a casino check or having the casino wire the money elsewhere; (2) using the chips as currency to purchase narcotics, with the drug dealer later cashing in the chips; or (3) using the chips to gamble in hopes of generating certifiable winnings. Casinos are also used to launder counterfeit money and large currency notes that would be conspicuous and difficult to use elsewhere. Suspicious activities at casinos often involve structuring transactions to avoid recordkeeping or reporting thresholds, using agents to cash-out multiple transactions for an anonymous individual, providing false documents or identifying information, or layering transactions to disguise their source.

[9] National Drug Threat Assessment 2005, National Drug Intelligence Center.

[10] Karen P. Tandy, Administrator, Drug Enforcement Administration, testimony before the U.S. Senate Caucus on International Narcotics Control, 4 March 2004.

26. Privately-owned automated teller machines (ATM): Both law enforcement and regulatory agencies have identified a material money laundering risk in relation to privately owned ATMs.

Terrorist financing

27. Terrorist financing remains a concern in the U.S. The volume of SARs for suspected terrorist financing, which peaked immediately after the events of 9/11 and then declined, began increasing again in the second quarter of 2003. The increase is partially attributed to the greater number of financial institutions that are now required to file SARs regarding terrorist financing (e.g. MSBs, casinos, securities broker-dealers, and futures commission merchants). Another possible explanation may be the publicity surrounding the investigations of some financial institutions with customers and transactions with possible ties to terrorism.

28. The U.S. authorities believe that wire transfers and funds raised by non-profit organizations (NPOs) are vulnerable to misuse by terrorists. Before the enactment of the terrorist financing laws, some terrorist financiers were far more open about the intended terrorist use of solicited funds. Given the substantial criminal penalties associated with providing material support or resources to terrorists or terrorist organizations, it is now quite rare for a terrorist fundraiser to openly acknowledge the intended terrorist-related use to which raised funds are to be applied. However, there are still instances when fundraisers cautiously make it clear to donors that their funds are destined to support terrorists or terrorism.

29. The analysis of wire transfers plays a role in many terrorist financing investigations ranging from the determination of source funding to establishing connections between the terrorist or terrorist organization and other associates, organizations, or countries. U.S. law enforcement has observed the following trends regarding wire transfers in terrorist financing investigations: (1) using "nominees" to provide clean names to terrorist financing transactions or accounts; (2) using front companies; (3) using multiple financial institutions; and (4) avoiding mainstream financial institutions, through the use of licensed money remitters, thereby avoiding or reducing the risk of SAR reporting. U.S. law enforcement also has been receiving unverified reports that many organizations under investigation are using larger amounts of cash to minimize financial paper trails.

1.3 Overview of the Financial Sector and DNFBP

Banking sector

30. Depository institutions in the U.S. may be chartered at either national or state level, and may be involved in any of the following activities: safeguarding money and valuables; providing loans and credit; offering payment services, such as checking accounts, money orders, and cashier's checks; dealing and holding Treasury and agency debt securities. With the passage of the Gramm-Leach-Bliley Financial Modernization Act in 1999, depository institutions also may affiliate more broadly with securities and insurance underwriters. This was previously generally prohibited.

31. Commercial banks in the U.S. offer a full range of services for individuals, businesses, and governments and range in size from global banks to regional and community banks. Global banks are involved in international lending and foreign currency trading, in addition to the more typical banking services. Regional banks have numerous branches and ATM locations throughout a multi-state area that provide banking services to individuals. Community banks are based locally and typically target retail and small businesses markets in their respective communities. In recent years, online banks, which provide all services entirely over the Internet, have entered the market. Moreover, many traditional banks also have expanded to offer online banking, and some formerly Internet-only banks are opting to open branches. Savings banks and savings and loan associations (frequently called thrift institutions) cater mostly to the savings and lending needs of individuals. A credit union is a member-owned, member-controlled, not-for-profit cooperative financial institution formed to permit groups of

persons who share a "common bond" to save, borrow, and obtain related financial services and to participate in its management.

32. The following numbers and types of depository institutions (all of which are defined as banks for the purposes of the BSA) were operating in the U.S. as of 31 December 2005:

(a) 1,818 Federal Deposit Insurance Corporation (FDIC)-insured nationally chartered commercial banks with USD 6.0 trillion total assets and 50 federal branches (including 5 FDIC-insured with total assets of USD 3 trillion) and agencies of foreign banking organizations with USD 110 billion in total assets, which are all supervised by Office of the Comptroller of the Currency (OCC);

(b) 907 FDIC-insured state chartered banks with USD 1.3 trillion total assets that are members of the Federal Reserve System, 5,153 bank holding companies with total assets of USD 11.6 trillion, and 204 uninsured U.S. branches and agencies of foreign banking organizations with USD 1.2 trillion total assets, which are all supervised by the Federal Reserve;

(c) 5,245 FDIC-insured state-chartered commercial and savings banks that are not members of the Federal Reserve with USD 2.0 trillion total assets, and 8 FDIC-insured U.S. branches of foreign banking organizations, which are all supervised by the FDIC;

(d) 862 FDIC-insured savings associations, with USD 1.5 trillion total assets, which are supervised by the Office of Thrift Supervision (OTS); and,

(e) 8,695 credit unions (of which 5,393 are National Credit Union Administration (NCUA) insured, federally chartered, and regulated by NCUA, and 3,302 are NCUA insured, state chartered, and regulated by state supervisory authorities); and 319 credit unions that are privately insured and state chartered and regulated.

Securities sector

33. Brokerage firms may be operated as full-service, discount, or online organizations, or any combination thereof. Full-service brokers help clients develop an investment portfolio, manage their investments, or make recommendations regarding which investments to buy. Discount firms often do not offer advice about specific securities, although they may provide third party analysis. Online brokerage firms offer their services over the Internet in order to keep costs down and fees low. Brokerage firms also provide investment-banking services (i.e. they act as intermediaries between companies and governments that would like to raise money and those with money or capital to invest). Investment bankers also advise businesses on merger and acquisition strategies and may arrange for the transfer of ownership.

34. Companies that specialize in providing investment advice, portfolio management, and trust, fiduciary, and custody activities are also included in these industries. These companies range from very large mutual fund management companies to self-employed personal financial advisers or financial planners. Also included are managers of pension funds, commodity pools, trust funds, and other investment accounts. Portfolio or asset management companies direct the investment decisions for investors who have chosen to pool their assets in order to have them professionally managed. Many brokerage firms also provide these services. Personal financial advisers can manage investments for individuals as well, but their main objective is to provide a comprehensive financial plan that meets a wide variety of financial needs. These firms also offer a number of other services, including cash management accounts that allow account holders to deposit money into a money market fund against which they can write checks, take out margin loans or use a debit card. Some brokerage firms offer mortgages and other types of loans and lines of credit. They also may offer trust services, help businesses set up benefit plans for their employees or sell annuities and other life insurance products.

35. As of 31 December 2005, there were 6,296 broker-dealers registered with the SEC, 5,363 of which do business with the public. These firms had USD 5.4 trillion in assets and USD 256 billion in capital, and their total market capitalization was USD 14.9 trillion.

36. Equity securities are primarily traded on registered securities exchanges, like the New York Stock Exchange (NYSE) and the National Association of Securities Dealers Automated Quotation Systems (NASDAQ), and to a much lesser extent on over-the-counter markets (OTC markets). As of 31 March 2006, there were eleven registered securities exchanges. In 2005, there was USD 131.0 billion in equity dollar volume on all exchanges, and OTC markets.

37. Mutual funds, which are also known as open-end registered investment companies, closed-end investment companies, and Unit Investment Trusts (UITs), are popular investment vehicles in the U.S. As of 28 February 2006, there were 8,000 mutual funds with assets of USD 9.2 trillion. As of 31 December 2005, there were 619 closed-end funds with assets of USD 276.3 billion, and over 6,019 UITs with a value of USD 40.9 billion. Investment advisers manage assets of investors, both on an individual and on a pooled account basis. As of 31 March 2006, there were 10,283 investment advisers registered with the SEC. Collectively, those registered investment advisers managed USD 31.1 trillion in assets, including assets of the managed investment companies described above.

38. Additionally, as of September 2005, there were 211 futures commission merchants, 1,711 registered introducing brokers in commodities, 2,635 commodity trading advisors and 1,783 commodity pool operators. In fiscal year 2005, 1.5 billion futures and options contracts were traded on U.S. exchanges. Individual customers, commission houses, financial institutions and commodity producers, among others, who wish to buy or sell futures or options must execute trades through a member of an exchange. The exchanges operate either through a trading floor or electronic network where all transactions in futures and options are executed.[11]

Insurance sector

39. In 2004, the U.S. insurance industry consisted of 7,789 domestic insurance companies, of which 1,179 were life insurers, and premiums increased to more than USD 1.7 trillion. The five states with the most premiums written in all lines were California, Florida, New York, Pennsylvania and Texas. These five states accounted for more than thirty-seven percent of all insurance premiums in the country. In 2004, more than 4.6 million insurance companies and agents were licensed to provide and sell insurance services.[12]

40. The insurance industry in the U.S. can be divided into three major sectors: life, property/casualty and health. Life insurers have developed products that offer a variety of investment components, including variable life (where the amount and duration of benefits are linked to investment experience), and that offer the insured the ability to overpay the premium for a fixed rate of return. Such products are marketed to investors as part of a diversified portfolio, often with tax benefits. Annuities, variable and fixed, are a popular new part of the life insurance sector, are purchased to provide an income stream over a period of time, and are frequently used for retirement planning purposes. Many insurance companies, particularly the larger ones, offer more than one kind of insurance product.

41. Insurance companies operating in the U.S. offer their products through a number of different distribution channels. Some sell their products through direct response marketing in which the insurance company sells a policy directly to the insured. Others employ agents, who may either be captive or independent. Captive agents represent only one insurance company or group of affiliated companies; independent agents may represent a variety of insurance carriers. Insurance may also be purchased through other third parties, depending on the product. A limited number of companies offer certain types of policies via the Internet. A customer also may employ a broker (i.e., a salesperson who searches the marketplace for insurance in the interest of the customer rather than the insurer) to obtain insurance.

[11] Futures and options on futures are financial instruments used to transfer price risk, related to the purchase and sale of commodities and financial instruments, to persons and entities willing to accept the risk. The markets on which the instruments are traded also provide price information used to establish the value of the underlying commodity or financial instrument.

[12] National Association of Insurance Commissioners, 2004 Insurance Department Resources Report.

Money Services Businesses (MSBs) (including money remitters and foreign exchange offices)

42. The money services business industry is very diverse, ranging from very large companies with worldwide reach to small convenience stores in inner city neighborhoods where English is rarely spoken. The term "money services businesses" includes: (1) money transmitters; (2) currency dealers or exchangers; (3) check cashers; (4) issuers of traveler's checks, money orders or stored value; and (5) sellers or redeemers of traveler's checks, money orders or stored value (other than a person who does not offer one or more of these financial services in an amount greater than USD 1 000 in currency or monetary or other instruments for any person on any day in one or more transactions). The U.S. Postal Service, except with respect to the sale of postage or philatelic products, is defined as a money services business.

43. Determining the exact number of MSBs operating in the U.S. is difficult. As of 5 April 2006, 24,884 money services businesses had registered with FinCEN. It has been estimated that, the total number of MSBs could exceed 200,000.[13] However, of these, approximately 40,000 are U.S. Postal Service outlets that sell money orders. It is also possible that a large number are agents that are exempt from registration due to primary MSB requirements to maintain lists of all agents through which they conduct business. The MSB sector is highly concentrated, with an estimated eight business enterprises accounting for the bulk of money services business financial products sold within the U.S., and accounting, through systems of agents, for the bulk of locations at which these financial products are sold.

Accountants

44. Public accountants provide accounting and auditing services on a fee basis. Certified public accountants have received a qualifying certificate from an authorized state entity. Accounting firms also provide financial and investment advice.

Casinos

45. As an adjunct to their primary purpose of providing gaming facilities, casinos offer a wide range of financial services including customer deposit or credit accounts, facilities for transmitting and receiving funds transfers directly from other institutions, check cashing and currency exchange services. Card clubs operate in much of the same manner as traditional casinos except that they do not offer house-banked games such as baccarat, craps, roulette, slot machines, etc. Instead, card clubs offer non-house banked card games to customers and earn revenue by receiving a fee from customers (e.g. when they deal each hand, rent a seat at a table, and/or take a fixed percentage of each "pot").

46. FinCEN estimates that there are approximately 845 casinos and card clubs operating in at least 34 jurisdictions in the U.S. (including a number of states, Tribal nations, and U.S. territories) that are subject to the requirements of the BSA. There has been a rapid growth in riverboat and tribal casino gaming as well as card room gaming over the last ten years. Fourteen states/territories license and regulate casino gaming operations: Colorado, Illinois, Indiana, Iowa, Louisiana, Michigan, Mississippi, Missouri, Nevada, New Jersey, South Dakota, the Commonwealth of Puerto Rico, Tinian (in the Commonwealth of the Northern Mariana Islands) and the U.S. Virgin Islands. More than USD 800 billion was wagered at casinos and card clubs in the U.S. in 2004, accounting for approximately 85% of the total amount of money wagered for all legal gaming activities throughout the U.S.

47. There are 567 federally recognized Indian Tribes (half of which are in Alaska)—223 of which operate 411 gaming facilities in 28 states.[14] Of these, 307 are considered casino operations; the others are basically bingo halls. Tribal casinos are licensed and regulated by tribal commissions and also

[13] Coopers & Lybrand L.L.P, "Non-Bank Financial Institutions: A Study of Five Sectors for the Financial Crimes Enforcement Network" (28 February 1997).

[14] National Indian Gaming Association, An Analysis of the Economic Impact of Indian Gaming in 2004.

may be subject to the jurisdiction of the National Indian Gaming Commission (NIGC). Collectively, tribal casinos earned around USD 18 billion per year—twice the amount generated by Nevada casinos.[15] The largest casino in the U.S. is a tribal gaming operation—Foxwoods Resort and Casino, located in Mashantucket, Connecticut and owned by the Mashantucket Pequot Tribe. Gaming operations in the populous areas of the West Coast (primarily California) represent the fastest growing sector of the Indian gaming industry.[16]

Dealers in Precious Metals or Stones

48. FinCEN estimates that there are approximately 20,000 dealers in precious metals, stones, or jewels in the U.S. that are subject to BSA requirements. The size of businesses in each segment of the industry varies substantially from a single artisan goldsmith to publicly traded commercial manufacturers employing hundreds of people and producing millions of finished pieces every year. The sources of supply and business models vary as well, from large-scale producers of fabricated precious metals materials to small dealers selling unique and rare gemstones on an individualized basis. There is also an active secondary market for jewelry, loose gemstones and precious metals.

Lawyers and other independent legal professionals

49. To practice law, an attorney or lawyer must be licensed by an appropriate authority (such as a state bar). The American Bar Association (ABA) reports that as of 2005, there were a total of approximately 1,104,766 resident and active lawyers in the U.S. The ABA has approximately 400,000 members.

Notaries Public

50. A notary public is a ministerial officer of the state who has been given specific duties under state law that are limited to attesting to the genuineness of writings, authenticating signatures, and administering oaths.

Real Estate Agents

51. A real estate agent is one who has entered into a fiduciary relationship with either a seller or purchaser or both to manage a real estate transaction. The 2002 Economic Census indicates that there were over 76,166 real estate businesses in the U.S. Real estate may be held directly or through various investment vehicles, such as real estate investment trusts, real estate limited partnerships, real estate mortgage investment conduits (REMICs) or other collateralized mortgage obligations, or entities commonly referred to as ‘‘syndicates’’ of real estate investors.

Trust and Company Service Providers (TCSPs)

52. Trust companies, which are licensed to provide a range of fiduciary services, are chartered at either national or state level, and are generally regulated on the same basis as banks. Trust services providers (i.e. persons and entities that assist in the setting up of trusts) generally are unregulated for AML/CFT purposes. Likewise, company service providers generally are unregulated and may provide a variety of services, including incorporation and routine filings, resident agency and accommodation address facilities (which may include an office that is staffed during business hours, a local telephone listing with a live receptionist and 24-hour personalized voicemail), assistance in opening local and foreign bank accounts and the sale of "shelf" companies. Such services may be provided by professionals (e.g. lawyers and accountants) or existing financial institutions as a part of their broader business, or by businesses formed solely for this purpose.

[15]MSNBC, Tribal Casinos Revenues Double Nevada's, 15 February 2005

[16] Ibid

Non-profit sector (NPO sector)

53. The U.S. charitable sector consists of nearly one million public charities and private foundations on file with the IRS that control approximately USD 3 trillion of assets and raised an estimated USD 240 billion in 2003. Additionally, the IRS estimates that about 350,000 religiously-affiliated or smaller public charities operate in the United States. These are exempt from applying to the IRS for tax-exempt status.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements

Types of legal persons and arrangements

54. In 2004, there were a total of 13,484,336 active legal entities registered in 50 states in the U.S. (This figure does not include the U.S. Territories[17]). Public corporations raise capital by selling equity securities (e.g. common or preferred stock) or debt securities to the general public or in private offerings. The securities of about 10,000 corporations are publicly traded on the U.S. securities markets. Private corporations ("closely held" corporations) are created by private persons for non-governmental purposes, have relatively few shareholders and do not sell their shares to the public at large. Private corporations can be run less formally than other corporations in that the stockholders can dispense with the board of directors and manage the corporation directly. Person-service corporations can be formed under the laws of many states by one or more persons rendering professional services (e.g. accountants, attorneys, etc.) and allow these professionals to enjoy limited liability as to most obligations and liabilities not involving malpractice. Limited liability companies (LLC) are a hybrid of a corporation and a partnership designed to provide its owners (called "members") with the limited liability enjoyed by corporate stockholders and the greater economic flexibility ordinarily associated with a partnership arrangement.

55. Corporate law is primarily handled at the state level. Many states follow the Model Business Corporation Act that was developed in 1984 to encourage uniformity amongst the state corporation laws. Many states have supplemented their general corporation statutes with special statutes providing relaxed rules for closely held corporations that elect to take advantage of their provisions or allow for the creation of hybrid or special purpose entities such as business trusts.

56. The following additional types of legal persons and arrangements are also available.

(a) Trusts are legal entities that are created under state law. There is a more detailed discussion of trusts in section 5.2 of this report.

(b) A non-profit organization (NPO) is an organization not intending or intended to earn a profit.

(c) A sole proprietorship is an unincorporated business that is owned by one individual and has no legal existence apart from the owner. Its liabilities are the owner's personal liabilities.

(d) A partnership is the relationship existing between two or more persons who join to carry on a trade or business. Each person contributes money, property, labor, or skill, and expects to share in the profits and losses of the business. Different types of partnerships exist, including general partnerships (in which each partner is potentially liable for the debts of the company) and limited liability partnerships (LLP). Law firms and accounting firms are often organized as LLPs. LLPs may also be used as vehicles for investing in capital funds. In Delaware, for instance, private wealthy individuals can establish family limited partnerships; however, the number of these is very small. Transactional entities, such as limited liability companies that are set up to be a merger subsidiary, are much more common. An LLP has the same organizational flexibility as other types of partnerships. However, in general (but with some

[17] Source is data from the International Association of Commercial Administrators provided by Delaware state officials.

state variations), an LLP has a form of limited liability that is similar to a corporation's (meaning that the partners are not personally liable) [Uniform Partnership Act, s.306(c)]. Like a general partnership or LLC, an LLP is not taxed separately at the entity level; its profits and losses flow to and are distributed among the partners for tax purposes.

1.5 Overview of strategy to prevent money laundering and terrorist financing

a. AML/CFT Strategies and Priorities

57. The U.S. is committed to identifying, disrupting, and dismantling money laundering and terrorist financing networks. The U.S. seeks to combat money laundering and terrorist financing on all fronts, including by aggressively pursing financial investigations. Overall, the U.S. AML/CFT strategy focuses on three major goals: (1) to more effectively cut off access to the international financial system by money launderers and terrorist financiers; (2) to enhance the federal government's ability to target major terrorist financing and money laundering organizations and systems; and (3) to strengthen and refine the AML/CFT regime for financial services providers to improve the effectiveness of compliance and enforcement efforts and to prevent and deter abuses.

58. The U.S. legislates and regulates financial institutions, examines them for compliance with the statutory and regulatory system, and enforces those requirements through civil and criminal actions. The U.S. reviews industry sectors to identify ML/FT vulnerabilities, with a view to imposing appropriate controls (such as record-keeping, reporting, licensing/registration, and AML Program requirements) based on an assessment of risk. Transparency and accountability are promoted throughout the financial services sector, as well as within relevant non-financial sectors. The U.S. considers private sector outreach to be an important component in implementation of its AML/CFT strategy. The U.S. government has developed its efforts in the following key areas: (1) enhancing interagency coordination; (2) ensuring that law enforcement agencies and task forces use and share financial databases and analytical tools; (3) focusing law enforcement personnel and other resources on highest-impact targets and financial systems; (4) utilizing new and improved statutory and regulatory authorities; (5) increasing international operational cooperation; (6) improving U.S. government interaction with the financial community; and (7) helping state/local governments investigate and prosecute money laundering and financial crimes.

59. The U.S. government prioritizes its AML/CFT domestic and international initiatives based on perceived systemic vulnerabilities and the relative risk to U.S. interests. The U.S. states that the highest priority has been given to keeping the core financial system secure, in particular banks and other depository financial institutions that form the financial backbone of the U.S. The U.S. also reports that MSBs, including IVTS, serve as an alternative to banks for many individuals in the U.S. and also receive high priority within the AML/CFT strategy. The following areas have also been prioritized for AML/CFT efforts:

(a) preventing the misuse of charities to aid terrorists;

(b) developing specific measures against the risk posed by cash couriers operating in support of terrorist or other criminal activities;

(c) examining the feasibility of regulating entities offering new payment technologies that provide financial services in a non-face-to-face environment;

(d) increasing the emphasis on comprehensive examination and effective enforcement of BSA regulatory requirements;

(e) enhancing active consultations with the private sector, particularly in the course of developing and implementing AML regulations;

(f) balancing the goal of ensuring that U.S. regulatory scheme meets its enforcement goals without imposing undue burden on and expense to industry, in recognition of the important role played by the financial services industry;

(g) providing more and better guidance to financial institutions;

(h) improving consistency in the implementation of AML/CFT regulation by engaging partners at the federal, state, tribal and local government levels;

(i) improving the process for raising and discussing issues with non-federal regulators; and

(j) launching BSA Direct, a new FinCEN initiative to better address its mandate to establish and maintain a government-wide data access service to information collected under the BSA and other data. The BSA Direct project involves the improvement of the technology used to store, process, retrieve and analyze this critical data and will provide significant improvements in end users' ability to query, retrieve, and analyze BSA data.

60. The U.S. is also seeking to extend AML/CFT measures to new sectors. In particular, advance notices of proposed rulemakings (ANPRM) have been issued for persons involved in real estate settlements and closings.

The institutional framework for combating money laundering and terrorist financing

U.S. Department of the Treasury

61. The U.S. Department of the Treasury (Treasury) has several offices that develop AML/CFT policy and strategy:

62. **Office of Terrorism and Financial Intelligence (TFI):** The TFI and its constituent parts (including the Office of Terrorist Financing and Financial Crime and the Office of Intelligence and Analysis) work domestically and internationally to ensure that all possible diplomatic, policy and strategic steps are taken to combat money laundering and terrorist financing. TFI's leadership is comprised of the Under Secretary for Terrorism and Financial Intelligence who reports through the Deputy Secretary of the Treasury to the Secretary of the Treasury. TFI is responsible for oversight, policy direction and integration of the Office of Foreign Assets Control (OFAC) and Treasury Executive Office for Asset Forfeiture (TEOAF), and oversees FinCEN. TFI is also responsible for the following: (1) developing and implementing U.S. government strategies to combat terrorist financing domestically and internationally; (2) developing and implementing the National Money Laundering Strategy as well as other policies and programs to fight financial crimes; (3) working with FinCEN to develop and implement U.S. government policies and regulations in support of the BSA and the USA PATRIOT Act, including outreach to the private sector; (4) representing the U.S. in international bodies dedicated to fighting terrorist financing, money laundering, and other financial crimes; and (5) overseeing and providing policy guidance for the implementation and administration of the nation's economic sanctions laws and programs.

63. **Office of Terrorist Financing and Financial Crime (TFFC):** TFFC is responsible for the policy and strategy functions within TFI concerning money laundering, terrorist financing, and other financial crimes. It is headed by the Assistant Secretary for Terrorist Financing and Financial Crimes. TFFC represents the U.S. at relevant international bodies, including heading the U.S. delegation to the FATF and FATF-style regional bodies (FSRBs). TFFC works closely with Treasury's Office of International Affairs and Office of Domestic Finance in the formulation of AML/CFT policy and strategies. Additionally, TFFC works on behalf of the Treasury, with DOJ, the Department of Homeland Security (DHS), and others, to continue developing and implementing the U.S. government's National Money Laundering Strategy as well as other policies and programs to fight financial crimes.

64. **Office of Intelligence and Analysis (OIA-T):** The OIA-T is the intelligence analysis branch for the Treasury within the TFI. This office develops financial intelligence and conducts analysis with a view to filling gaps in intelligence targets, and adding value and expertise. Its priorities include identifying and attacking the financial infrastructure of terrorist groups; identifying and addressing vulnerabilities that may be exploited by terrorists and criminals in domestic and international financial systems; and promoting stronger relationships with Treasury's partners in the U.S. and around the world.

65. **Financial Crimes Enforcement Network (FinCEN):** FinCEN is a bureau within the Treasury. In addition to being the financial intelligence unit (FIU) of the U.S., FinCEN is responsible for the development, issuance, administration and civil enforcement of regulations implementing the BSA; in concert with the IRS, for collecting and maintaining BSA data and providing government-wide data access service to information collected under the BSA and other data; and, in concert with the federal functional regulators, certain self-regulatory organizations and the IRS, for ensuring compliance with that regime. The agency is also charged with protecting the integrity and confidentiality of the information collected under the BSA and for accounting for the proper use of that information.

66. **Office of Foreign Assets Control (OFAC):** OFAC is an office within Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under the President's wartime and national emergency powers, as well as under authority granted by specific legislation, to impose controls on transactions and assets subject to U.S. jurisdiction.

67. **Treasury Executive Office for Asset Forfeiture (TEOAF):** The TEOAF administers the Treasury Forfeiture Fund (TFF). The TFF was established in 1992 as the successor to the Customs Forfeiture Fund.

U.S. Department of Justice (DOJ)

68. The DOJ is the principal government entity responsible for overseeing the investigation and prosecution of money laundering and terrorist financing offenses at the federal level. Led by the Attorney General, the DOJ comprises 40 separate component organizations including: the 94 Presidentially-appointed United States Attorneys (USAs) who prosecute offenders and represent the United States government in court; several of the major investigative agencies–the FBI, the Drug Enforcement Administration (DEA) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) which deter and investigate crimes, and arrest criminal suspects; the U.S. Marshals Services (USMS) which protects the federal judiciary, apprehends fugitives, detains persons in federal custody and manage seized assets and the sale of forfeiture of assets for the Justice Forfeiture Fund; and the Bureau of Prisons (BOP), which confines convicted offenders. The agencies and offices of the DOJ that are involved in AML/CFT are briefly described below (listed alphabetically by acronym).

69. **Asset Forfeiture and Money Laundering Section, Criminal Division (AFMLS):** The AFMLS of the Criminal Division leads DOJ's asset forfeiture and AML enforcement efforts. AFMLS provides centralized management for DOJ's asset forfeiture program to ensure its integrity and maximize its law enforcement potential, while also providing managerial direction to the Department's components in prosecuting money laundering. The Section initiates, coordinates and reviews legislative and policy proposals impacting on the asset forfeiture program and money laundering enforcement agencies. AFMLS also: (1) prosecutes and coordinates complex, sensitive and multi-district and international money laundering and asset forfeiture investigations and cases; (2) provides legal and policy assistance and training to federal, state and local prosecutors and law enforcement personnel, as well as to foreign governments and in multilateral fora; (3) assists Departmental and interagency policymakers by developing and reviewing legislative, regulatory and policy initiatives; and (4) manages DOJ's Asset Forfeiture Program, including distributing forfeited funds and properties to appropriate domestic and foreign law enforcement agencies and to community groups within the U.S., as well as adjudicating petitions for remission or mitigation of forfeited assets. Because asset forfeiture and money laundering are aspects of all proceeds-generating crimes, the Section's portfolio cuts across all of the different criminal cases handled by the DOJ.

70. **Counterterrorism Section, Criminal Division (CTS)**[18]: The CTS designs, implements, and supports law enforcement efforts, legislative initiatives, policies and strategies relating to combating international and domestic terrorism. The CTS assists in preventing and disrupting acts of terrorism anywhere which impact on significant U.S. interests and persons through criminal investigation and prosecution and other means. The CTS participates in investigating and prosecuting domestic and international terrorism cases in a number of ways, that include: (1) coordinating with headquarters of U.S. government agencies (such as the Treasury and State Departments, FBI, intelligence agencies and the DHS) to facilitate prevention of terrorist activity through daily detection and analysis and to provide information and support to the field; (2) investigating and prosecuting terrorist financing and cases involving torture, genocide and war crimes that are linked to terrorist groups and individuals; (3) formulating legislative initiatives and DOJ policies and guidelines relating to terrorism; (4) assisting the 93 Anti-Terrorism Advisory Council (ATAC) Coordinators through the Regional Coordinator system involving information sharing between and among prosecutors nationwide on terrorist matters, cases and threat information; (5) participating in the foreign terrorist organization and specially designated global terrorists designation processes with the Departments of State and Treasury and other DOJ components; and (6) providing legal advice to federal prosecutors concerning numerous federal statutes associated with terrorism, including acts of terrorism.

71. **National Drug Intelligence Center (NDIC):** The NDIC's mission is to develop strategic domestic drug intelligence. NDIC created a Money Laundering Unit in January 2005 to provide a multi-source capability for money laundering-related information. The mission of this unit is to identify strategic money laundering trends and patterns for national policy makers.

72. **Office of International Affairs, Criminal Division (OIA):** The OIA conducts the DOJ's international law enforcement activity in the areas of extradition and legal assistance, among others. In particular, OIA coordinates the extradition or other legal rendition of international fugitives and all international evidence gathering. OIA attorneys also participate on a number of committees established under the auspices of the United Nations (UN) and other international organizations that are directed at resolving a variety of international law enforcement problems, such as terrorism, money laundering, narcotics trafficking, organized crime, cyber-crime, and corruption. OIA is the U.S. central authority for mutual legal assistance matters, which includes the production of evidence in the U.S. for use in foreign investigations and proceedings, as well as obtaining evidence from abroad for use in U.S. investigations and prosecutions. OIA attorneys advise prosecutors on when a formal request for assistance is required; assist in drafting requests for various types of evidence from abroad; and act as liaison between U.S. and foreign prosecutors, helping to ensure that evidence obtained from abroad can be used in U.S. proceedings. On a day-to-day basis, OIA attorneys assist prosecutors in requesting the return of fugitives located abroad and in executing foreign requests for extradition.

State Department

73. The State Department represents the U.S. government in several multilateral institutions, including the UN 1267 Sanctions and Counter-Terrorism Committees, the G-8 Roma-Lyon Group, the Dublin Group, the Organization of American States (OAS), the FATF and the FSRBs. State Department personnel also take part in multi-agency diplomatic missions relating to money laundering and terrorist financing. The State Department conducts a wide variety of regional and bilateral initiatives relating to money laundering and terrorist financing. It also has shared policy making responsibilities with Treasury and DOJ with respect to money laundering, terrorist financing, and other financial crime, ranging from planning and implementing Presidential Decision Directives and is a lead agency and a major source of funding for the provision of foreign AML/CFT training and technical assistance. The departments and offices of the State Department that are involved in AML/CFT are described below (listed alphabetically by acronym).

[18] In March 2006 the U.S. government announced its intention to create in DOJ a new National Security Division. It is expected that CTS will be among the units moved into this new Division.

74. **Bureau of Economic and Business Affairs (EB):** EB works to deny terrorist states the economic benefits of trade with the U.S. and to deny terrorists access to the global financial system. It provides foreign policy guidance to other U.S. agencies and works with regional bureaus and State Department's Office of the Coordinator for Counterterrorism (S/CT) to develop, implement and calibrate sanctions programs to support diplomatic and policy objectives. EB also chairs the interagency Coalition Building Group, which coordinates U.S. bilateral, regional and multilateral diplomatic engagements regarding terrorist financing, including submission to the UN of Al Qaida, Usama bin Laden and Taliban-linked individuals and groups. EB leads U.S. diplomatic initiatives to support implementation of these sanctions, providing U.S. overseas missions with regular guidance on terrorism finance, including training for U.S. officials.

75. **Bureau of International Narcotics and Law Enforcement Affairs (INL):** The INL is vested with primary responsibility for issues dealing with money laundering and financial crimes. It creates and publishes, with Presidential approval, the International Narcotics Control Strategy Report (INCSR), which includes a separate volume on international money laundering and terrorist financing. INL also provides a coordinating function on intelligence relating to money laundering and other financial crimes, and meets regularly with intelligence agencies to monitor worldwide trends and developments.

76. **State's Office of the Coordinator for Counterterrorism (S/CT):** S/CT leads the State Department's efforts relating to designating Foreign Terrorist Organizations (FTO) in order to freeze assets, stigmatize and isolate designated terrorist organizations internationally by restricting their ability to travel, and to deter donations to and economic transactions with named organizations. S/CT also has lead responsibility in the State Department for preparing Executive Order (EO) 13224 designations, which block assets and prohibit contributions of terrorists and terrorist organizations, and works closely with the State Department's Economics Bureaux and the Treasury in recommending EO 13224 designations. Likewise, S/CT works with the DOJ and Department of Homeland Security (DHS) to designate groups to the Terrorism Exclusion List (TEL).

Law Enforcement Agencies

77. **Drug Enforcement Administration (DEA):** The DEA is responsible for investigations of illicit drug trafficking. Its Office of Financial Operations (FO) (which was created in 2004) enhances investigations by providing the necessary assistance on the financial component of those investigations. (See section 2.6 of this report for a more detailed description of the DEA.)

78. **Federal Bureau of Investigation (FBI):** The FBI is the primary agency responsible for investigating federal crimes. Responsibility for the investigation of terrorism and terrorist financing rests with the FBI-led multi agency Joint Terrorism Task Forces (JTTF). Additionally, the FBI promotes the investigation and prosecution of money laundering across all of its investigations. (See section 2.6 of this report for a more detailed description of the FBI.)

79. **Department of Homeland Security, Immigration and Customs Enforcement (ICE):** With the creation of the DHS in March 2003, the investigative and intelligence functions of the former U.S. Customs Service (including its AML activities) and the Immigration and Naturalization Service were merged to form ICE. In addition, ICE includes the Detention and Removal Program, and the Federal Protective Service. In part, the mission of ICE is to protect the U.S. and its citizens by deterring, interdicting, and investigating ML/FT threats arising from the movement of people and goods into and out of the U.S.

80. **Department of Homeland Security, Customer and Border Protection (CBP):** CBP is the nation's unified border agency. CBP includes more than 41,000 employees who manage, control and protect the nation's borders, at and between the official ports of entry. CBP has the authority to search outbound and inbound shipments, and uses targeting to carry out its mission in this area. CBP works with ICE to seize both cash and monetary instruments.

81. **Internal Revenue Service Criminal Investigation (IRS-CI):** The IRS-CI enforces money laundering, terrorist financing and criminal tax statutes. IRS-CI targets high-profile money laundering investigations, particularly those that directly or indirectly enhance tax compliance. The IRS-CI is implementing the Lead Development Center (LDC) concept that is focused on developing investigation leads relating to specific types of crimes using a combination of tax and publicly available information. There are currently five LDCs. The Garden City LDC has been designated the research site for the terrorist financing investigations and the Tampa LDC for money laundering investigations.

82. **U.S. Postal Inspection Service:** The U.S. Postal Inspection Service is charged with safeguarding more than 200 billion pieces of mail a year and with protecting more than 700,000 postal employees, 38,000 postal facilities, 200,000 postal vehicles, and billions of dollars in postal assets.

Supervisors/Regulators responsible for ensuring AML/CFT compliance in the financial sector

Banking sector supervisors/regulators

83. **Board of Governors of the Federal Reserve System (Federal Reserve):** The Federal Reserve (the U.S. central bank) supervises and examines state-chartered banks that elect to become members of the Federal Reserve System (state member banks), bank holding companies (BHCs), Edge and Agreement corporations, and uninsured U.S. state-chartered branches and agencies of foreign banking organizations. The Federal Reserve is an independent agency created by the U.S. Congress.

84. **Federal Deposit Insurance Corporation (FDIC):** The FDIC is the deposit insurer for all federally insured depository institutions (other than credit unions). This includes both national and state chartered institutions. In this capacity the FDIC has either direct or back-up supervisory responsibility for about 8,800 financial institutions. The FDIC also identifies, monitors and addresses risks to the deposit insurance funds, and limits the effects on the economy and the financial system when one of its insured institutions fails. The FDIC is an independent agency created by the U.S. Congress.

85. **Office of the Comptroller of the Currency (OCC):** The OCC charters, regulates, and supervises national banks and the U.S. Federal branches and agencies of foreign banking organizations. The OCC is a bureau of the Treasury.

86. **Office of Thrift Supervision (OTS):** The OTS charters, examines, regulates and supervises federally-chartered savings associations and state-chartered savings associations belonging to the Savings Insurance Fund, and provides for the registration, examination and regulation of savings association affiliates and holding companies. The OTS is a bureau of the Treasury.

87. **National Credit Union Administration (NCUA):** The NCUA charters, supervises, regulates and examines federally-chartered and certain state-chartered credit unions and insures deposits for federal and state credit unions. The NCUA is an independent agency created by the U.S. Congress.

88. **Federal Banking Agencies (FBA):** Under the Federal Deposit Insurance Act (FDI Act), the "Federal Banking Agencies" include the Federal Reserve, the OCC, the FDIC and the OTS. However, for the purposes of this report, the term also includes the NCUA.

89. **State Banking Regulators:** Each state charters banks and shares supervisory responsibility over such banks through Joint Supervisory Agreements with the Federal Reserve, FDIC, and OTS. Most states also charter and examine credit unions and share supervision with the NCUA.

Securities sector supervisors/regulators

90. **Securities and Exchange Commission (SEC):** The SEC is the federal regulator of the securities markets and administers the federal securities laws (including the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940, the Investment Advisers Act

of 1940, and the Trust Indenture Act of 1939). It has direct regulatory responsibilities and also oversees key participants in the securities industry, including securities exchanges, securities brokers and dealers, investment advisers and investment companies, and the Self-Regulatory Organizations' (SROs) compliance with their statutory obligations under the Securities Exchange Act. The SEC is an independent agency created by the U.S. Congress.

91. **Commodity Futures Trading Commission (CFTC):** The CFTC is the federal regulator of U.S. commodity futures and options markets in the U.S. and it administers and enforces the federal futures and options laws as set forth in the Commodity Exchange Act (CEA) and the accompanying regulations. It also oversees the operations of the industry SRO. The CFTC is an independent agency created by the U.S. Congress.

92. **NASD:** NASD is an SRO for broker-dealers. Securities broker-dealers that effect securities transactions other than on a national securities exchange of which they are a member are required to be NASD members. NASD and the other securities SROs have a statutory obligation to enforce their members' compliance with their own rules, as well as with the U.S. securities laws and SEC rules. NASD oversees the activities of approximately 5,300 brokerage firms, 116,000 branch offices and more than 657,000 registered securities representatives.

93. **National Futures Association (NFA):** The NFA is the SRO for the futures market. Membership in the NFA is mandatory for anyone conducting business with the public on the U.S. futures exchanges. Approximately 4,200 firms and 55,000 associates are members of the NFA. The CFTC has delegated some regulatory responsibilities to the NFA.

94. **New York Stock Exchange (NYSE):** The NYSE is the SRO for exchange member organizations. A member organization is a registered broker-dealer organized as a corporation, a partnership or an LLC, which holds an NYSE trading license or opts for NYSE regulation. A total of 1,272 licenses have been issued and they must be renewed each year. A trading license gives the member organization direct electronic access to the NYSE trading floor and the right to have a member on the floor. Only members are allowed to buy and sell securities on the NYSE trading floor.

Other financial sector and DNFBP supervisors/regulators

95. **IRS Small Business and Self-Employment Division (IRS-SBSE):** The IRS-SBSE has been delegated examination authority for civil compliance with the BSA for all financial institutions that do not have a federal functional regulator as defined in the BSA, including MSBs (as broadly defined), insurance companies, credit card companies, non-federally insured credit unions, casinos (tribal and non-tribal) and dealers in precious metals, stones and jewels. It also has responsibility for auditing compliance with currency transaction reporting requirements that apply to any trade or business.

96. **National Indian Gaming Commission (NIGC):** The NIGC is an independent federal regulatory agency whose primary mission is to regulate gaming activities on Indian lands for the purposes of ensuring that Indian tribes are the primary beneficiaries of gaming revenues, and assuring that gaming is conducted fairly and honestly by both operators and players. The NIGC is authorized to: conduct background investigations of primary management officials and key employees of a gaming operation, conduct audits, review and approve tribal gaming ordinances and management contracts, promulgate federal regulations, investigate violations of these gaming regulations, and undertake enforcement actions (including the assessment of fines and issuance of closure orders. Both Class II gaming (e.g. bingo and certain card games) and Class III gaming (e.g. baccarat, blackjack, slot machines, and electronic or electromechanical facsimiles of any game of chance) are subject to the provisions of the Indian Gaming Regulatory Act (IGRA) and oversight by the NIGC. However, in general, the primary regulator for these activities is the tribal nations themselves.

97. **State-level regulators:** Insurance, MSBs and non-tribal casinos are primarily regulated at the state level, albeit not for BSA purposes. Some states have adopted statutes and regulations that incorporate or parallel the provisions of the BSA.

98. **Tribal-level regulators:** Many tribal gaming commissions have been established by the tribes to oversee tribal gaming. The tribal nations have primary regulatory authority over Class II gaming. Regulation of Class III gaming may be addressed in the Tribal-State compacts (i.e. agreements between a state and a tribe, which are approved by the Secretary of the Interior, concerning the rules to govern the conduct of Class III gaming within the state). Although the terms of Tribal-State compacts vary by state, in most instances, the tribes remain the primary regulator for Class III gaming.

Non-profit sector supervisors/regulators

99. **IRS Tax Exempt and Government Entities Division (IRS-TEGE):** The IRS-TEGE provides federal oversight to all non-profit organizations in the U.S. through the review of applications for tax exempt status and subsequent audits. This division conducts examinations of applications and returns filed to determine if the non-profit organizations are facilitating terrorist financing.

Interagency groups focusing on the development of AML/CFT policy

100. **National Security Council (NSC) Terrorist Financing Policy Coordinating Committee (TF PCC):** The TF PCC is a high-level interagency group that reports directly to the National Security Advisor, who in turn reports directly to the President. Its role is to design and implement and then assess the effectiveness of national CFT policy and to coordinate appropriate adjustments.

101. **Bank Secrecy Act Advisory Group (BSAAG):** The U.S. Congress established the BSAAG to enable the financial services industry and law enforcement to advise the Secretary of the Treasury on ways to enhance the usefulness of BSA reports. The BSAAG serves as the principal forum for industry, regulators and law enforcement to discuss issues relating to the administration of the BSA. The Director of FinCEN chairs the BSAAG. Members include representatives from: law enforcement agencies; federal and state financial regulatory agencies, including SROs; industries subject to the BSA; and trade groups and practitioners representing industries subject to the BSA.

102. **Money Laundering Working Group:** The Money Laundering Working Group (led by the Treasury/TFFC) convenes periodically to coordinate the development and implementation of AML/CFT policy.

103. **National Counterterrorism Center (NCTC):** The NCTC orchestrates an interagency CFT action plan and/or response by coordinating the information flows which are generated by the U.S. intelligence agencies.

Interagency groups and task forces of law enforcement agencies dealing with CFT

104. **Terrorist Financing Operations Section (TFOS):** The TFOS is an inter-agency group that was established by the FBI and operates out of FBI Headquarters as part of the FBI's Counterterrorism Division. A main focus of TFOS is to conduct full financial analysis of terrorist suspects and their financial support structures in the U.S. and abroad.

105. **Joint Terrorism Task Forces (JTTF):** JTTFs are interagency task forces of law enforcement agencies that are lead by the FBI and have primary investigative responsibility for the investigation of terrorism and terrorist financing.

106. **Joint Vetting Unit (JVU):** The JVU reviews ICE and FBI databases to determine whether a nexus to terrorism or terrorism financing exists in a given investigation. Where such a nexus is found to exist, the investigation is conducted under the auspices of the JTTF.

107. **National Joint Terrorism Task Force (NJTTF) and the Foreign Terrorist Asset Targeting Group (FTAT-G):** The NJTTF and FTAT-G are interagency task forces comprised of federal, state and local investigative agencies. They combat terrorist financing by targeting key money laundering professionals and financial mechanisms, such as bulk cash movement and wire transfers.

108. **Antiterrorism Advisory Councils (ATAC):** ATACs promote and ensure proper training and information sharing on terrorism cases and terrorism threats (including terrorist financing) among federal, state and local law enforcement and private sector representatives.[19]

Interagency groups and task forces of law enforcement agencies dealing with AML

109. **High Intensity Financial Crime Areas (HIFCAs):** The statutorily-mandated HIFCA program (spearheaded by the ICE) concentrates the AML efforts of federal, state and local law enforcement agencies in seven designated high-intensity money laundering zones.

110. **Indian Gaming Working Group (IGWG):** The IGWG consists of representatives from the FBI's financial crimes, public corruption and organized crime subprograms as well as representatives from other federal law enforcement agencies. The IGWG meets regularly to address significant criminal violations in the Indian gaming arena.[20]

111. **Organized Crime Drug Enforcement Task Forces (OCDETF):** The primary function of the OCDETFs (which are administered and coordinated by the DOJ) is to target the most significant, high-priority drug trafficking organizations in their region for investigation and prosecution. In particular, this involves following a financial investigative plan for attacking the financial structure of the criminal organization and identifying forfeitable assets.

112. **Money Services Business Working Group (MSB-WG):** The MSB-WG is an interagency working group (comprised of various law enforcement agencies) that focuses on eliminating vulnerabilities posed by unlicensed MSBs.

Interagency groups of financial sector supervisors/regulators

113. **Conference of State Bank Supervisors (CSBS):** The CSBS is a professional association of state officials responsible for chartering, supervising and regulating the U.S.'s 6,000 state-chartered commercial and savings banks and more than 400 state-licensed foreign banking offices.

114. **Federal Financial Institutions Examination Council (FFIEC):** The FFIEC was established by the U.S. Congress as a formal interagency body empowered, among other things, to prescribe uniform federal principles, standards and report forms for the examination of depository institutions by the Federal Banking Agencies, and to make recommendations to promote uniformity in the supervision of those financial institutions,. The FFIEC has established, in accordance with the requirement of the statute, an advisory State Liaison Committee composed of five representatives of state supervisory agencies.

115. **National Association of Insurance Commissioners (NAIC):** The state- and territorial-level regulators in the insurance sector coordinate their regulatory activities through the NAIC. Its Ad Hoc Executive Task Force on USA PATRIOT Act Compliance considers policy issues, develops and

[19] This body was not referenced by the U.S. authorities prior to or during the on-site visit. Consequently, the assessment team did not have the opportunity to meet with this agency or discuss its AML/CFT role.

[20] This body was not referenced by the U.S. authorities prior to or during the on-site visit. Consequently, the assessment team did not have the opportunity to meet with this agency or discuss its AML/CFT role.

coordinates appropriate examination standards, and coordinates with state and federal regulators regarding the USA PATRIOT Act's AML amendments to the BSA.

116. **Money Transmitter Regulators Association (MTRA):** The MTRA is a national non-profit organization that works towards the unifying regulatory practices amongst state-level regulators of money transmitters and check sellers.

Approach concerning risk

Application of AML/CFT obligations to certain sectors

117. The U.S. has followed a risk-based approach in determining which sectors should be subject to various AML requirements. In addition to any risk assessments undertaken by Treasury and FinCEN to apply AML obligations to different types of financial institutions in implementing the requirements of the BSA, federal agencies undertake ongoing assessments of risks, threats and vulnerabilities of industries and activities that are within their purview.

118. The BSA, most recently substantially amended by the USA PATRIOT Act, has a broad definition of "financial institution" (including many sectors not typically considered "financial") and also permits the addition of other activities within the definition by regulation.[21] However, the application of AML/CFT obligations to individual financial activities requires the promulgation of implementing regulations by Treasury. Implementing regulations have been issued for all the categories of financial institutions that the authorities consider present a significant risk of money laundering, and proposed rules have been issued for certain additional types of financial institutions considered to pose a less significant risk of money laundering. Moreover, the order in which Treasury and FinCEN addressed the different sectors was based upon the perceived significance of the risk each presents for potential money laundering and the financing of terrorism.

119. In determining the nature and scope of AML/CFT obligations that should be applied to a particular sector, the BSA authorizes Treasury, in consultation with the federal functional regulators[22], to consider the extent to which these requirements are commensurate with the size, location, and activities of financial institutions, to prescribe minimum requirements for such programs or to exempt financial institutions from these requirements. In practice, the approach to determining whether to issue implementing regulations, how they should be structured and what guidance to provide, is the result of a risk assessment conducted by Treasury and FinCEN, in consultation with the federal functional regulators.

120. Treasury and FinCEN analyzed the actual and potential risks of money laundering and terrorist financing presented by each general category of financial institution, as well as by various subsets within each industry. This typically involved meetings and discussions with any relevant federal regulators, representatives of different sectors of each industry and with their trade associations; a review of money laundering investigations, prosecutions, and convictions in each industry and consideration of law enforcement views; and consideration of international standards (including those of the FATF, European Union and industry-specific associations). Following this analysis, if the sector is deemed of sufficient money laundering risk, FinCEN typically publishes a notice of proposed rulemaking, setting forth its proposal with respect to an AML rule for the industry, and seeking formal public input. However, in three cases FinCEN chose instead to publish advance notices of proposed

[21] Title 31 USC 5312(a)(2)(Y) authorizes the Secretary of the Treasury to include additional types of businesses within the definition of "financial institution" if he/she determines that they engage in any activity similar to any listed business; and subsection (Z) states that the Secretary of the Treasury can include within "financial institution" any other business he/she designates as having cash transactions with a high degree of usefulness in criminal, tax, or regulatory matters.

[22] The Federal functional regulators include the Federal Reserve, FDIC, OCC, OTS, NCUA, SEC, and CFTC.

rulemaking, in order to obtain further public comment with respect to particular types of financial institutions, before deciding whether to proceed to a formal proposed rule.[23]

121. Following the issuance of a proposed rule, public comments are reviewed and considered, as is other relevant information. This deliberative process may extend for a considerable period, it being judged of utmost importance to Treasury and FinCEN to craft their AML/CFT regulations as carefully as possible, in order to achieve the greatest benefit without needlessly imposing burdens on the relevant financial sectors. For example, the public consultation on the proposed rules for the insurance industry started in 2002, resulting in the publication of the final rules in October 2005. These became effective six months after publication. Risk assessments in the future will consider the U.S. Money Laundering Threat Assessment published in January 2006, as well as other relevant information.

Risk-based approach taken by financial institutions

122. Generally, U.S. financial institutions are required to apply a risk-based approach to their AML/CFT obligations. There are, however, certain mandatory prescriptive requirements. For instance, the rules implementing the "customer identification program", mandated for certain financial institutions by the USA PATRIOT Act amendments to the BSA, prescribe the collection of specific minimum information and certain recordkeeping requirements. Similarly, the Secretary of the Treasury has imposed many recordkeeping requirements on wire transfer and other activities by regulation. More generally, the AML Programs required to be implemented by certain financial institutions are very substantially risk-based, providing broad discretion to the institutions to determine the extent of due diligence (both enhanced and reduced) depending on their analysis of the overall risks of their business. This approach to institutional risk management is reinforced within the AML/CFT examination manual that has been developed by the Federal Banking Agencies as the basis for compliance monitoring in the banking sector.

Progress since the last mutual evaluation or assessment

123. Since the last mutual evaluation report (June 1997), the U.S. has implemented a very large number of developments in its AML/CFT regime both in terms of statutory amendments and structural changes. The most high-profile development was the enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), and many other significant improvements derived from it. This report discusses these changes in detail.

2 LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalization of Money Laundering (R.1 & 2)

2.1.1 Description and Analysis

Recommendation 1 (Criminalization of money laundering)

Federal Laws

124. The U.S. criminalized money laundering on 27 October 1986 (Title 18 USC 1956 and 1957, Money Laundering Control Act of 1986, Pub. L. 99-570). Sections 1956 and 1957 criminalize four different types of money laundering: (1) basic money laundering [1956(a)(1)]; (2) international money laundering (where criminal proceeds are moved in or out of the U.S.) [s.1956(a)(2)]; (3) money laundering in the context of an undercover "sting" case (where the money being laundered has been represented by a law enforcement officer as being criminal proceeds) [s.1956(a)(3)]; and

[23] This was done with respect to travel agencies, businesses involved in vehicle sales, and persons involved in real estate closings and settlements.

(4) knowingly spending greater than USD 10,000 in criminal proceeds (s.1957). A five year statute of limitations applies to these offenses (Title 18 USC 3282).

Basic money laundering provision: Laundering of monetary instruments [18 USC 1956(a)(1)]

125. The prosecution must prove the following five elements to obtain a conviction for this offense.

(a) *Knowledge:* The defendant knew that the property was the proceeds of some form of unlawful activity. It is not necessary to establish which particular unlawful activity.[24]

(b) *Intent:* At the time of the transaction, the defendant acted with any one of the following four specific intents:

  (i) The defendant intended to promote the carrying on of a specific unlawful activity (SUA). Most commonly, prosecutors satisfy this element by showing that the defendant reinvested the proceeds of the offense to keep the criminal scheme going ("plowing back") [subsection (a)(1)(A)(i)].

  (ii) The defendant intended to commit tax crimes described in 26 USC 7201 (tax evasion) or 7206 (Fraud and False Statements) of the Internal Revenue Code of 1986) [subsection (a)(1)(A)(ii)].

  (iii) The defendant intended to conceal or disguise the nature, location, source, ownership or control of the proceeds of the SUA. This is the most commonly alleged intent for money laundering [subsection (a)(1)(B)(i)].

  (iv) The defendant intended to avoid a transaction reporting requirement. This includes IRS reporting requirements [subsection (a)(1)(B)(ii)].

(c) *Actus reus:* The defendant conducted or attempted to conduct a financial transaction.

(d) *Factual predicate:* The property does, in fact, "involve" the proceeds of an SUA.

(e) *Factual predicate:* The financial transaction either:

  (i) affected interstate or foreign commerce (in any way or degree) involving the movement of funds, one or more monetary instruments, or the transfer of title to property; or

  (ii) involved the use of a financial institution which is engaged in (or the activities of which affect) interstate or foreign commerce in any way or degree.

126. Sections 1956(a)(1) and1956(a)(3) cover the laundering of the proceeds of specified unlawful activity in certain specified situations. Proof that the defendant simply possessed or concealed the proceeds of a specified unlawful activity is not sufficient for a conviction under section 1956(a)(1), because under U.S. law, in the absence of some sort of financial transaction, no laundering has occurred. In order to constitute a violation of sections 1956(a)(1) or 1956(a)(3) the possession or concealment must involve a financial transaction which in turn must involve a defined type of transaction. It is clear that the prosecution must adduce proof on these two distinct issues (i.e. the prosecution must prove that the defendant conducted a "transaction" and that this transaction constituted a "financial transaction").[25]

127. To qualify as a "financial transaction" for the purposes of section 1956(a)(1) and 1956(3), the transaction must be either:

[24] Senate Report 99-433, 3 September 1986, pages 9-10 makes it clear that the knowledge requirements in s.1956(a)(1) are intended to cover instances of 'willful blindness".

[25] See United States v Leslie 103 F.3d 1093 (where court ruled separately on the 'interstate commerce" element which arises as part of the definition of "financial transaction" and whether conduct was a transaction) and United States v Gallo 927 F.2d 811 (where the court ruled on the "interstate commerce" element but was not asked to determined whether defendant's actions constituted a "transaction").

(a) a transaction that "in any way or degree affects interstate foreign commerce" and either involves the movement of funds by wire or other means; involves one or more monetary instruments (which will cover any transaction involving domestic or foreign currency) or transfers title to land, vehicles, vessels or aircraft; or

(b) a transaction that involves the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree.[26]

128. According to the legislative history of the section, the phrase "affects interstate or foreign commerce" "is intended to reflect the full exercise of Congress's power under the Commerce Clause of the U.S. Constitution".[27] Consequently, the requirement to prove this element provides both sections 1956(a)(1) and 1956(a)(3) with constitutional validity pursuant to the commerce power of the U.S. Constitution.[28] U.S. courts have interpreted this phrase very broadly requiring only a *de minimis* connection to interstate commerce. When interpreting the phrase, U.S. courts can defer to codified Congressional findings and declarations on the relevant predicate offense to establish whether particular conduct affects interstate commerce. For example, 21 USC 801 makes it clear that Congress intended drug trafficking to be interpreted as affecting interstate commerce. Accordingly the court will infer that a transaction involving the proceeds of drug trafficking should also be interpreted as affecting interstate commerce.[29]

129. To qualify as a "transaction" the defendant's conduct must include a purchase, sale, loan, pledge, gift, transfer, delivery or other disposition. This includes making a deposit or withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, using a safe deposit box, or purchasing or selling securities/monetary instruments [s.1956(c)(3)]. It also includes "activities not involving banks, such as the purchase, sale, or other disposition or property of all kinds".[30] The legislative history of the provision indicates that Congress intended this term to cover "those transactions that can be said to constitute the core of money laundering".

130. A key element of the definition of "transaction" is the requirement for a "disposition" of the property. It is clear that the term transaction requires the government to prove that there has been "a placing elsewhere, a giving over to the care or possession of another".[31] The mere possession or

---

[26] The term "financial institution" is also defined very broadly and includes banks, insurance companies, securities brokers and dealers, money remitters, foreign exchange dealers, casinos, persons involved in real estate closing (including lawyers) and settlement, trust companies, pawnbrokers, telegraph companies, travel agencies, the U.S. postal service and vehicle sellers.

[27] See Senate Report No. 99-433 which accompanied Senate Bill No, 2683, page 13.

[28] Both sections also derive constitutional validity from the "currency power" in the U.S. Constitution because this power provides that "Congress can properly regulate the use to which its currency is put, and other activities that affect banks" (United States v Canavan 153 F. Supp. 2d 811).

[29] United States v Gallo 927 F.2d 815.

[30] Senate Report No. 99-433 which accompanied Senate Bill No. 2683 at p.10 and 12, and is also discussed in U.S. v Samour 9 F.3d 531 (6th Cir. 1993), overruled by United States v. Reed, 77 F.3d 139 (6th Cir. 1996).

[31] This point is illustrated by U.S. v Puig-Infante, 19 F. 3d 929 (5th Cir. 1994). In that case, the defendants appealed against a conviction under section 1956(a)(1)(A)(i) on the basis that they did not engage in a financial transaction involving the proceeds of an unlawful activity. The evidence against the appellant was that in a hotel room in Florida she received USD 47 000 cash in exchange for a load of marihuana. The informant and the appellant then drove with the money to Laredo on the border of Texas and Mexico. Although the informant testified that the last time she saw the money it was still in the possession of the appellant, she could not say what happened to the money after that. The court agreed with the appellant's argument that while the money received in payment for marihuana was the proceeds of an unlawful activity, the appellant's subsequent transportation of that money by car from Florida to Laredo did not constitute a "financial transaction" within the meaning of section 1956(a)(1)(A)(i). The court held that: "…(a)lthough it is clear that the transportation of money by car is not a "purchase, sale, loan, pledge, or gift" whether such transportation is a "transfer" or "delivery" is less clear. However the statute makes plain that for something (not involving a financial institution or its facilities), to be a transaction, it must be a "disposition". "Disposition" most commonly means a "placing elsewhere, a giving over to the care of possession of another." Webster's Third New International Dictionary, 654(1961)…(t)he only permissible inference from the government's proof is that Abigail was in possession of the proceeds of unlawful activity. Nowhere is there any evidence that Abigail effected a disposition of those proceeds; i.e. that she "g(ave) over to the care of possession of another' the money she received in exchange for the marihuana. Without such proof, her mere transportation of the proceeds of unlawful activity is not a transaction within the statute

transportation of proceeds will not necessarily meet the definition of "financial transaction". There must be more to the transportation, for example transferring the proceeds of drug trafficking to a courier could constitute a transaction.[32] Similarly, a concealment or disguise of proceeds may not be covered under section 1956(a)(1) if the activity does not involve a transaction (e.g. merely placing money in a shoe box and keeping it).[33]

131. Section 1956 also requires the prosecution to prove the relevant criminal intent in relation to the defendant's conduct namely that the perpetrator engaged in a "financial transaction" that he or she intended would achieve one of the specified outcomes. For example, under subsection 1956(a)(1)(A)(i), the prosecutor must prove that, with the proceeds of an illegal activity, the defendant engaged in a financial transaction that was intended to promote the illegal activity. Under subsection 1956(a)(1)(B)(i), the prosecutor must prove that the defendant engaged in a financial transaction that was intended to conceal or disguise the proceeds of the illegal activity.[34] Most money laundering prosecutions will fall under either subsections 1956(a)(1)(A)(i) or 1956(a)(1)(B)(i).

International money laundering offense [18 USC 1956(a)(2)]

132. This offense will apply to the transportation, transmission or transfer of monetary instruments or funds across, but not within, U.S. borders with one of three possible intents. Section 1956(a)(2)(A) does not require proof that the monetary instrument or funds that are transported, transmitted or transferred are the proceeds of any criminal activity. It merely requires proof that the defendant moved the monetary instrument or funds with the intent to promote an SUA. To prove a violation of 1956(a)(2)(A), the prosecution must prove the following elements:

(a) *Knowledge:* The defendant knew that the funds or monetary instruments were being moved across the U.S. border;

(b) *Actus reus:* The defendant moved (transported, transmitted or transferred) a monetary instrument or funds either to or from the U.S.;

(c) *Intent:* The defendant acted with the intent to promote the carrying on of an SUA.

133. To prove a violation of 1956(a)(2)(B), the prosecution must prove the following three elements to obtain a conviction for the offense.

(a) *Knowledge:* The defendant knew the funds or monetary instruments were the proceeds of some form of unlawful activity. Knowledge may be established by proof that a law enforcement officer represented the funds or monetary instruments to be proceeds and the defendant's subsequent actions indicated that he/she believed that representation to be true.

---

[32] United States v. Reed, 77 F.3d 139 (6th Cir. 1996): Reed was a defense attorney who represented S. M was Reed's neighbour. Reed knew that S and M were involved in the ongoing distribution of marihuana and she conveyed messages back and forth between them. Reed arranged for M and S's wife to meet at her office to transfer some of M's marihuana proceeds to a courier. Two transfers took place. Reed momentarily left her office and M gave S's wife approximately USD 96,000. M left and Reed returned and pursuant to a prearranged plan, Reed and S's wife hid the USD 96,000 in a bag in Reed's office. A few days later a courier arrived and at Reed's direction the office receptionist gave the bag containing the money to the courier. The court was asked to conduct an "en banc" review of the lower court's decision that delivery or transfer of cash, which is the proceeds of unlawful activity, to another person was not a "financial transaction". The court overruled the lower court's decision holding that Reed's conduct in delivering the money to a courier amounted to a financial transaction. The court made it clear that "we do not hold that the mere transportation nof cash meets the definition of 'financial transaction'." Also see United States v Gonzales-Rodriguez, 966 F.2d 918 (5th Cir. 1992) where the court held that carrying cash through the airport was not a transaction in violation of the money laundering statute because there was no evidence that the person carrying the cash intended to conceal or disguise the nature or the source of the money.

[33] United States v Ramirez 954 F.2d 1035 (5th Cir. 1992).

[34] See United States v Jackson 935 F.2d 832 where the U.S. Court observed that the Government will tend to make its case under one or other subsection and only in unusual cases would it be able to prove that a single transaction was intended to both promote an illegal activity and conceal the origin of the funds used in that activity.

(a) *Actus reus:* The defendant moved (transported, transmitted or transferred) a monetary instrument or funds either to or from or through the U.S.

(b) *Intent:* The defendant acted with either of the following intents.

(i) to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the SUA; or

(ii) to avoid a transaction reporting requirement, including IRS reporting requirements.

(c) *Factual predicate:* The property is a monetary instrument or funds

Money laundering in the context of an undercover "sting" case [18 USC 1956(a)(3)]

134. Section 1956(a)(3) makes it possible to prosecute persons who engage in the laundering of "sting money" (i.e. money that is not really criminal proceeds but is represented to be such by a law enforcement officer or a person acting at his/her direction). The prosecution must prove the following three elements to obtain a conviction for laundering sting money:

(a) *Actus reus:* The defendant conducted or attempted to conduct a financial transaction. [The term "financial transaction" has the same meaning as in section 1956(a)(1)].

(b) *Intent:* The defendant acted with any of the following intents.

(i) to promote the carrying on of an SUA;

(ii) to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the SUA; or

(iii) to avoid a transaction reporting requirement, including IRS reporting requirements.

(c) *Factual predicate:* The property involved in the financial transaction conducted or attempted to be conducted is represented to be proceeds of specified unlawful activity.

Engaging in monetary transactions in property derived from SUA: (18 USC 1957)

135. Section 1957 is referred to as the "spending statute" in that it criminalizes the spending of proceeds of crime without the additional requirement (as in section 1956) that this spending be accompanied by the relevant criminal intent.[35] Under this provision it is a criminal offense for a third-party to do business with the wrongdoer or for the wrongdoer to spend the proceeds or engage in a transaction in which he/she was involved. The prosecution must prove the following four elements to obtain a conviction for this offense:

(a) *Actus reus:* The defendant conducted a monetary transaction (i.e. the transaction must be conducted by, to, or through a financial institution).

(b) *Knowledge:* The defendant knows that the monetary transaction is criminally derived property.

(c) *Factual predicate:* The property is, in fact, derived from the proceeds of a SUA.

(d) *Factual predicate:* The monetary transaction must involve more than USD 10,000. Each monetary transaction is a separate offense but it is possible to aggregate separate transactions to reach the USD 10,000 threshold if they are closely related to each other. For example, multiple purchases from the same vendor on the same day, or installment payments on the same item, can constitute a single transaction in some circumstances.

[35] See United States v Allen 129 F.3d 1159 citing United States v Rutgard, 116 F.3d 1270 and describing the statute as having the effect of freezing the proceeds of specific crimes out of the banking system. "As long as the underlying crime has been completed and the defendant "possesses" the funds at the time of deposit, the proceeds cannot enter the banking system without a new crime being committed".

136. The term "monetary transaction" in section 1957 is defined much more narrowly than the term "financial transaction" in section 1956(a)(1) and 1956(3) though there is no separate requirement to prove that the "monetary transaction" involved a "transaction". In proving that the defendant conducted a monetary transaction, the prosecution must prove that the defendant deposited, withdrew, transferred or exchanged funds by, through or to a financial institution. The term "financial institution" includes not only banks and other traditional institutions, but also casinos, persons involved in real estate closing (including lawyers) and settlement, pawnbrokers, telegraph companies, travel agencies, the U.S. postal service and vehicle sellers.

137. Despite the absence of a requirement in section 1957 to prove criminal intent, the DOJ confirmed that prosecutions under section 1957 are generally more difficult than prosecutions under 1956(a)(1) because under section 1957 the prosecution must prove:

(a) that the defendant's conduct must be via the much more narrowly defined "monetary transaction";

(b) that the proceeds were of a value greater than USD 10,000; and

(c) that at least USD 10,000.01 of the property which is the subject of the monetary transaction was "derived" from SUA. (This is only problematic when the transaction involves commingled funds). In contrast, under section 1956(a)(1) the prosecution only has to prove that the financial transaction "involves" proceeds from SUA.)

Other related offenses

138. The U.S. authorities acknowledge that sometimes it can be difficult to secure prosecutions under either of section 1956(a)(1) or section 1957 due to the USD 10,000 threshold requirement in section 1957 and the requirement of proof of specific intent either to promote another offense or to conceal or disguise the criminal proceeds in section 1956. When some elements of the money laundering offenses cannot be proved, the U.S. prosecuting authorities also seem to rely on two other offenses as "fall back" prosecutions. For instance, the prohibition of unlicensed money transmitting business offense (Title 18 USC 1960) contains neither of the above requirements and can be used as a "default charge" to section 1956(a)(1) and section 1957 where the facts permit. The U.S. suggests that these other charges "may prove more potent than either section 1956 or 1957 as a prosecutor's tool". Although the criminal sanction for violation of section 1960 is much lower than for a violation of sections 1956 or 1957, all property involved in a section 1960 offense is subject to civil and/or criminal forfeiture [18 USC 981(a)(1)(A) or 18 USC 982(a)(1)]. Likewise, in appropriate circumstances, the offense of bulk cash smuggling (Title 31 USC 5332) may be pursued. Neither of these provisions creates a money laundering offense. The section 5332 and section 1960 offenses are discussed in more detail in section 2.7 and section 3.11 of this report respectively.

Consistency with the United Nations conventions

139. The Vienna and Palermo conventions require countries to establish as a criminal offense the following intentional acts: conversion or transfer of proceeds; concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to proceeds; and the acquisition, possession or use of proceeds [Article 3(1)(b)(i)-(ii) of Vienna; Article 6(1)(a)(i)-(ii) of Palermo]. This obligation is subject to the fundamental/constitutional principles and basic concepts of the country's legal system [Article 2(1), Vienna convention; Article 6(1), Palermo convention].

140. Section 1956(a)(1) criminalizes money laundering through the conversion, transfer, concealment, disguise or use of proceeds—activities that almost always involve a transaction. However there are a limited number of cases in which there is no "disposition" and, therefore, no "transaction" involved in the concealment or disguise of the proceeds (e.g. concealment in a shoe box). In such situations, there can be no conviction under section 1956(a)(1). Likewise, section 1956(a)(1) does not criminalize ML through the acquisition or possession of proceeds

(including simple transportation within U.S. borders) because these activities do not involve a "transaction". These limitations are therefore inconsistent with the Vienna and Palermo conventions and cannot be justified on the basis of the jurisdictional requirements of the U.S. Constitution.

141. The DOJ has confirmed that facts giving rise to a finding that there will be no "transaction" are extremely rare. In the case of possession by transportation of monetary instruments the federal government does have jurisdiction over activities that cross the national border of the U.S under section 1956(a)(2) but this will not apply to proceeds that are not monetary instruments or funds.

142. The limited number of cases involving the mere concealment or disguise of proceeds and the mere possession of proceeds within the U.S. which are not criminalized by the federal government because of the definition of "transaction" could also be picked up by relevant state legislation. There is the potential for a gap where the conduct occurs within a state that does not have applicable provisions or where the state's provisions also require proof of a transaction. Without analyzing the legislation in each of the 38 States it is difficult to assess the size of this gap. Accordingly the fact that a limited category of conduct in the U.S. may not be criminalized according to all of the requirements of the Vienna and Palermo Conventions will not, of itself, significantly affect the rating on Recommendation 1.

Definition of "proceeds"

143. Neither the term "proceeds" nor the term "property" is defined in section 1956(a)(1). Case law which has developed from litigation surrounding this provision and section 1957 (which also uses these terms) demonstrates that the courts have defined the terms broadly enough to include any type of property that directly or indirectly represents the proceeds of crime. For example, it seems clear that the term "proceeds" can apply to property other than money or cash equivalents. For the same reasons, it would seem clear that the section 1956(a)(3) offense would cover any type of property that is represented to be the proceeds of crime.

144. Although the term "criminally derived property" as used in section 1957 has been interpreted by the U.S. Courts to have the same broad meanings as "proceeds" in section 1956(a)(1), the definition of "property" in section 1957 is restricted in terms of value. The offense only applies to property of a value greater than USD 10,000. Courts have noted that this threshold was imposed by Congress, conscious of the absence of the criminal intent requirement on an offense that can be applied to persons who simply spend dirty money.[36] The threshold in the section 1957 offense would be problematic but for section 1956(a)(1). Where property that might otherwise be the subject of a section 1957 offense is less than USD 10,000 in value, the defendant may be prosecuted under section 1956(a)(1) provided that the conduct involves a "financial transaction" and the relevant criminal intent can be proven.[37] Consequently, the threshold on the definition of "property" in section 1957 does not negatively impact the U.S.'s overall compliance with Recommendation 1.

145. Section 1956(a)(2) does not apply the wider definition of "proceeds". It involves the international transportation of only funds or monetary instruments. Consequently, proceeds in other forms (e.g. precious stones, metals, art or other high value goods) would not be covered.[38] This limitation is ameliorated by the fact that, in instances where there is a transmission or transfer in or out of the U.S. borders that would qualify as a "transaction", prosecutors can use section 1956(a)(1) instead. Nevertheless, for the reasons outlined above, however, section 1956(a)(1) cannot be used to

[36] United States v Brown 186 F.3d 661.

[37] The reverse is not true, since the definition of a monetary transaction is more narrow than the definition of financial transaction.

[38] Official from the DOJ advise that it could be argued that the term "funds" is broader than "currency" and could include anything of value. However, this has not yet been tested.

capture cases involving the simple transportation of proceeds other than funds or monetary instruments. This limitation does not significantly affect the rating on Recommendation 1.

Predicate Offenses

146. Money laundering is an autonomous offense. When proving that property is the proceeds of crime, it is not necessary that a person be convicted of a predicate offense.

147. The U.S. has adopted a list approach to define the scope of predicate offenses. The underlying predicate offenses for money laundering are listed in section 1956(c)(7) and include all of the Racketeer Influenced and Corrupt Organization (RICO) predicates listed in 18 USC 1961(1). There are approximately 250 predicate offenses for money laundering, including a range of offenses in 18 out of the 20 designated categories of offenses set out in the Glossary to the FATF 40 Recommendations (which defines the minimum scope of predicate offenses required). However, two designated categories are not specifically listed by name in sections 1961(1) and 1956(c)(7): insider trading and market manipulation, and piracy.

148. The U.S. authorities have provided citations of cases which demonstrate that unlawful conduct covered by the offenses of insider trading and market manipulation could be captured by relying on other USC offenses such as fraud in the sale of securities.[39]

149. In the same way, conduct constituting piracy could also be covered by other specified unlawful activity despite the fact that sections 1956(c)(7) and 1961(1) do not specifically include an offense called "piracy" in their lists. Section 1956 includes in its list of specified unlawful activities violations of modern U.S. statutes that reach piracy-type activities: violence against maritime navigation (in violation of 18 USC 2280), and violence against fixed platforms (in violation of 18 USC 2281). Furthermore, U.S. authorities pointed out that piracy activities could form the basis of money laundering charges relying on other predicate offenses such as 18 USC 659 (relating to theft from interstate shipment); section 1201(relating to kidnapping); section 1203 (relating to hostage taking); section 1363 (relating to destruction of property within the special maritime and territorial jurisdiction); and could also be covered by indictments relying on drug trafficking.[40]

150. Only some of the predicate offenses contained in the SUA list are predicate offenses for money laundering if they occurred in another country [18 USC 1956(c)(7)(B)]. Eight out of the 20 categories of designated offenses are not included as foreign predicates offenses under U.S. legislation: (1) participation in an organized criminal group and racketeering; (2) illicit trafficking in stolen and other goods; (3) fraud which is not fraud against a foreign bank; (4) counterfeiting currency; (5 counterfeiting and piracy of products; (6) environmental crime; (7) forgery; (8) piracy; and (9) insider trading and market manipulation. Officials from the DOJ indicated that the most critical omission from the SUA list in relation to prosecuting offenses is where the predicate offense in the foreign country is simple fraud. The DOJ points out that while they may not be able to prosecute for money laundering where the predicate offense is simple fraud outside the U.S., they can sometimes prosecute individuals and entities using several domestic statutes, such as the Interstate Transportation of Stolen Property Act (involving property valued at more than USD 5,000 taken by theft, fraud, or

[39] SEC v. O'Hagan, 901 F.Supp. 1461 (D. Minnesota 1995) where the defendant was charged with securities fraud under SEC Rule 10b-5. The court drew a link between insider trading and securities fraud on the facts of that case by explaining that the offense of insider trading requires proof of the use of a fraudulent "device" in the sale of securities. The court noted that O'Hagan's conduct in using information he acquired as a member of a law firm representing the tender offeror to purchase stock in the target corporation prior to tender constituted the use of a fraudulent device. Other cases include United States v. Newman, 74 Fed.Appx. 126 (2d Cir. 2003) (describing the defendant's pump and dump market manipulation scheme as a securities fraud scheme); United States v. Scop, 846 F.2d 135 (2d Cir. 1988) (describing market manipulation as securities fraud).

[40] U.S. v. Monaco, 194 F.3d 381 (2d Cir. 1999) dealt with an assertion that the prosecution was time barred. The court indicated that the defendants continued to conceal the proceeds of their specified unlawful activities, "viz., drug trafficking and piracy" until that time. United States v. La Spina, 299 F.3d. 175 [quoting 18 USC 1956(a)(1)(B)(I)].

conversion), and the mail and wire fraud statutes.[41] The DOJ also attempts to capture as much fraudulent activity as it can under the heading "fraud by or against a foreign bank." Nonetheless, the fact that an offense like simple fraud is not covered is potentially troublesome. It is noted that the U.S. is recognized as a global financial center. In this context, the U.S., in criminalizing money laundering, should seek to ensure that as many foreign predicate offenses as possible are covered.

151. Officials from the DOJ also indicated that prosecuting offenses under sections 1956 and 1957 would be much easier if a threshold approach to categorizing predicate offenses (rather than the current list approach) was adopted.[42]

Self-laundering and ancillary offenses

152. Self-laundering is a crime (i.e. a person who may have committed the underlying predicate offense may also be charged with money laundering the proceeds of that predicate).

153. There are ancillary offenses to all of the money laundering offenses, including conspiracy to commit money laundering [18 USC 1956(h), which applies to both section 1956 and 1957 offenses] and attempt to commit money laundering [18 USC 1956(a)(1)-(3) and 1957(a)]. Additionally, anyone who aids and abets, counsels, commands, induces, procures or willfully causes a money laundering offense can be prosecuted and punished as a principal (18 USC 2).

Additional elements

154. Generally, the U.S. cannot prosecute someone for money laundering if the proceeds of crime are derived from conduct that occurred in another country, which is not an offense in that country but would have constituted a predicate offense had it occurred in the U.S.

State laws

155. The general elements of the federal money laundering offenses described above apply throughout the U.S. Additionally, 38 of the 50 states and three U.S. territories have enacted money laundering statutes. Georgia, Vermont and the Virgin Islands only regulate money laundering in the sense of requiring reports of certain activity. The remaining states have statutes that create an offense of money laundering; however, the state-level money laundering offenses of Kansas, North Dakota and Oklahoma relate to a limited category of predicate offense (i.e. certain drug offenses). The other states have broader money laundering statutes.[43] The assessment team did not visit or consider the situation in any of the 12 states that have not criminalized money laundering. For the purposes of this evaluation, the assessment team examined the state legislation of New York and Arizona.

[41] Examples included the Mizuno case in which Japanese citizen Ken Mizuno defrauded hundreds of victims of millions of dollars in Japan. He transferred the money to the U.S. where he invested in property. The defendant was successfully prosecuted for violation of the Interstate Transportation of Stolen Property Act and Section 1956. Likewise, Pavel Lazarenko, the former Prime Minister of Ukraine, was successfully prosecuted for money laundering in the U.S. when he moved stolen monies to and through the U.S. Both of these cases were prosecuted in the U.S. because the "home" jurisdictions were unable to do so.)

[42] On 13 March 2006, the Combating Money Laundering and Terrorist Financing Act of 2006 bill was introduced in the U.S. Senate (S 2402). The bill provides for both domestic and foreign "all crimes" money laundering. If this bill becomes law, it will simplify and expand the definition of "specified unlawful activity" to mean "(A) any act or activity constituting an offense in violation of the laws of the United States or any Sate punishable by imprisonment for a term exceeding 1 year; and (B) any act or activity occurring outside of the United Sate that would constitute an offense covered under subparagraph (A) if the act or activity had occurred within the jurisdiction of the United States or any State."

[43] Arizona, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Guam, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Virgin Islands and Washington.

Case study – New York

New York's money laundering statutes are set out in Article 470 of Part Four, Title X of the New York Penal Code. The language of the provision largely mirrors that of the basic money laundering federal statute section 1956(a)(1). There are separate offenses depending on the total value of the property involved in the financial transaction.[44]

The predicate offenses for the New York statutes are referred to as "specified criminal conduct". These include as predicate offenses all the offenses under the federal racketeering laws. The statute of limitations for prosecutions under Article 470 is five years.

Discussions with prosecutors from the District Attorney's office in New York demonstrate that while a particular money laundering offense could fall within either state or federal jurisdiction, the state and federal prosecuting authorities work well together to ensure crimes are prosecuted by the most appropriate authority. Federal prosecutions might be preferred where there are assets eligible for confiscation as the federal laws permit greater recoveries.

[44] Section 470.20 "Money laundering in the first degree" applies where the total value of the property exceeds USD 500,000; s.470.15 "Money laundering in the second degree" applies where the total value of the property exceeds USD 50,000; s.470.10 "Money laundering in the third degree" applies where the total value of the property exceeds USD 10,000; and s.470.21 "Money laundering in the fourth degree" applies where the total value of the property exceeds USD 1,000.

Case study – Arizona

Arizona's money laundering statutes can be found at section 13—2317 in Title 13, Chapter 23 of the Criminal Code in the Arizona Revised Statutes. Arizona's laws are seemingly more far reaching than the federal laws and extend beyond what would be considered the mere laundering of proceeds of crime. Apart from a basic money laundering provision similar to section 1956(a)(1), the statute picks up conduct pertaining to AML measures that are set out in other parts of the statute and deems failures in these requirements to also be money laundering. For example, intentionally making a false statement or representation in any financial statement or report that must be maintained or filed under the AML laws, or intentionally knowingly failing to disclose information is all deemed to be money laundering in the second degree [sections 13-2317(B)(4), (5) and (6)].

Arizona's money laundering statute has a strong focus on money transmitters who will also be guilty of money laundering in the second degree if they intentionally or knowingly accept false personal identifying information from any person or otherwise knowingly incorporate false personal identifying information in any report which is required. The statute also captures the customers of money transmitters who will be guilty of money laundering in the third degree if they seek to bribe a money transmitter to not comply with any reporting or identification requirement. Any money transmitter or employee thereof who accepts anything of value and agrees to not comply with any reporting or identification requirement will also be guilty of money laundering in the third degree.

The predicate offenses for Arizona's money laundering statutes are defined extremely broadly to include "conduct for which a sentence to a term of incarceration is provided by any law of the United States". Arizona also creates a specific tier of offenses for money laundering where racketeering proceeds are involved. There is a "king pin" style of money laundering offense whereby a person will be found guilty of money laundering in the first degree if the person:

(a) knowingly organizes, plans, finances, directs, manages, supervises or is in the business of money laundering involving racketeering proceeds [section 13-2317(A)(1)]; or

(b) acquires or maintains an interest in, transacts, transfers, transports, receives or conceals that existence of racketeering proceeds or makes racketeering proceeds available for the purposes of facilitating terrorism or murder [section 13-2317(B)(1)].

Recommendation 2 (Criminalization of money laundering)

Scope of liability

156. The offense of money laundering applies to natural persons who knowingly engage in money laundering activity (1 USC 1). The law permits the intentional element of the money laundering offense to be inferred from objective factual circumstances. Proof of the intentional elements of the offense can occur either from direct evidence or from circumstantial evidence. The case law provides many examples of circumstantial evidence being successfully used to prove this element of the offense.[45]

[45] For instance, in U.S. v. Golb, 69 F.3d 1417 (9th Cir.1995), the court held that the jury could infer that the defendant, who brokered an airplane sale, (1) knew that the purchase money was illegally derived because the money came as multiple, anonymous wire transfers and bundles of checks, (2) made statements about the purchaser's involvement in drug trafficking, and (3) made threats of violence, showing he/she knew he/she was not representing a legitimate business person. For additional examples, see: U.S. v. Otis, 127 F.3d 829 (9th Cir. 1997) (defendant's "pager contacts, associations, and criminal history" sufficient to show that defendant knew that the USD 60 000 he/she turned over to a third-party in a parking lot was criminal proceeds); U.S. v. Hurley, 63 F.3d 1 (1st Cir. 1995) (even underlings who never dealt with drug dealers knew that money they were laundering was drug proceeds because no other cash-generating business would require the laundering of such huge quantities of cash); U.S. v. Campbell, 977 F.2d 854 (4th Cir. 1992) (real estate agent willfully blind to client's use

157. Criminal liability for money laundering also extends to legal persons. Title 1 USC 1 Provides that in all statutes enacted by Congress the words "person" and "whoever" shall include corporations, companies, associations, firms, partnerships, societies, and joint stock companies as well as individuals. Congress may stipulate that a corporation can acquire criminal intent and thus criminal liability through its employees or agents pursuant to the doctrine of vicarious liability/*respondeat superior*. A legal person can therefore be criminally liable for the illegal acts of its employees and agents if they are acting within the scope of their authority and their conduct is intended to benefit the legal person.

Sanctions for money laundering

158. Making natural and legal persons subject to criminal liability for money laundering does not preclude the possibility of parallel civil or administrative proceedings. Persons who commit a criminal offense of money laundering are also liable to a civil penalty [section 1956(b)] or, in the case of a legal person, having their license revoked.

159. Both natural and legal persons are subject to effective, proportionate and dissuasive criminal, civil and administrative sanctions for money laundering. Criminal sanctions for violating section 1956 are a fine of not more than USD 500,000 or twice the value of the property involved in the transaction (whichever is greater) or imprisonment for not more than 20 years or both. Criminal sanctions for violating section 1957 are a fine and/or imprisonment for not more than 10 years "or an alternate fine of not more than twice the amount of criminally derived property and/or imprisonment for not more than 10 years. These enhanced fines may be utilized by sentencing tribunals in the instances of egregious conduct. The DOJ confirmed that enhanced fines have been imposed on corporations.

160. Criminal sanctions are imposed with regard to the federal sentencing guidelines which were implemented in 1987. In January 2005, the U.S. Supreme Court held that, although federal courts must consult the sentencing guidelines, they are not bound to apply them. Based on the severity of the offense, the guidelines assign most federal crimes to one of 43 "offense levels." Each offender is also assigned to one of six "criminal history categories" based upon past misconduct. The point at which the offense level and criminal history category intersect on the Commission's sentencing table determines an offender's guideline range. Judges can then choose a sentence from within the guideline range.

161. Civil sanctions for violating both sections 1956 and 1957 are imposed by way of civil penalty the maximum amounts of which are prescribed by section 1956(b) as being either the value of the property, funds, or monetary instruments involved in the transaction or USD 10,000 (whichever is greater).

162. Persons who attempt or conspire to commit one of these offenses, or commit any of the other ancillary offenses to money laundering are subject to the same criminal and civil sanctions as the principals to the offense.

163. If a financial institution or any officer, director or employee of a financial institution is found guilty of a money laundering offense pursuant to sections 1956 or 1957, the Attorney General must provide a written notice of conviction to the financial institution's regulatory agency [section 1956(g)]. Parallel civil and administrative actions are also applicable as discussed in section 3 of this report.

Effectiveness of the money laundering offenses (Recommendations 1 & 2)

164. The U.S. takes a robust approach to dealing with money laundering prosecutions and has achieved a significant number of convictions. The number of convictions per year is substantially higher than it was at the time of the second mutual evaluation of the U.S. The following statistics show the number of defendants sentenced in fiscal years 2002 to 2004 where money laundering was at least one of the counts of conviction.

---

of drug proceeds to purchase house); and U.S. v. Long, 977 F.2d 1264, 1270-71 (8th Cir. 1992) (car dealer willfully blind to use of drug proceeds to purchase car).

Fiscal year	Number of Defendants convicted of 18 USC 1956	Number of Defendants convicted of 18 USC 1957	TOTALS
2002	1,034	217	1,251
2003	955	163	1,118
2004	970	178	1,148
2005	749	326	1,075

165. Additionally, money laundering convictions have been obtained at the state level; however, no overall statistics are available.

166. Information from officials of the DOJ and the U.S. Attorney's Office suggests that money laundering offenses are being aggressively prosecuted. However, officials were candid about technical difficulties in securing successful prosecutions for money laundering and the tendency to pursue the easier option of prosecuting the predicate offense (and consequential forfeiture applications) rather than the money laundering offense. Nevertheless, the information provided (including copies of pending indictments and a large body of reported case law on these offenses) demonstrates no apparent lack of will in prosecuting money laundering offenses and creativity in getting around these difficulties.

167. The U.S. proactively investigates and prosecutes money laundering cases and has a record of successful prosecutions and convictions over a number of years. While there are a few deficiencies in the criminalization of money laundering, this record demonstrates that the system is working effectively overall.

2.1.2 Recommendations and Comments

168. The U.S. federal anti-money laundering laws are largely comprehensive. Some state legislation, particularly that of Arizona, also comprehensively addresses a range of criminal conduct relating to money laundering. The following comments relate to the federal legislation.

169. The U.S. should take legislative measures to ensure that the definition of "transaction" is broadened to cover all conduct as required by the Vienna and Palermo Conventions.

170. The U.S. should take legislative measures to ensure that the scope of the section 1956(a)(2) offense is broadened include proceeds other than funds or monetary instruments.

171. The list of SUA does not fully cover two of the 20 designated categories of offenses required by the FATF Recommendations. It is recommended that the list of SUA be amended to include the offenses of piracy, market manipulation and insider trading. Discussions with securities organizations and the SEC indicated that there was no particular view from industry or supervisors as to why market manipulation and insider trading were not included in the list of SUA.

172. In 1997, the second mutual evaluation report of the U.S. recommended that the U.S. review its list of foreign predicate offenses. At that stage, it was indicated that there were current legislative proposals to this effect. This should be reviewed as soon as possible. In particular, the U.S. should expand the list of foreign predicate offenses to include all of the domestic predicate offenses (including piracy, market manipulation and insider trading). It is noted that the limited number of foreign predicate offenses also results in limitations on the U.S. system for freezing, seizing and forfeiting assets based only on violations of the money laundering statutes as noted in section 2.3 of this report below.

2.1.3 Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
R.1	LC	• The list of domestic predicate offenses does not fully cover 2 out of the 20 designated categories of offenses specifically (insider trading and market manipulation, and piracy). • The list of foreign predicate offenses does not cover 8 out of the 20 designated categories of offenses. • The definition of "transaction" in s.1956(a)(1) means that mere possession as well as concealment of proceeds of crime , does not constitute the laundering of proceeds. • The definition of "property" in relation to the section 1956(a)(2) offense (international money laundering) only includes monetary instruments or funds.
R.2	C	• The Recommendation is fully observed.

2.2 Criminalization of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

Special Recommendation II (Criminalization of terrorist financing)

Federal laws

173. There are four federal offenses which deal directly with financing of terrorism or terrorist organizations:[46]

(a) 18 USC 2339A (enacted in September 1994 and came into effect in April 1996)–providing material support for commission of certain offenses;

(b) 18 USC 2339B (enacted by Congress and signed by the President in April 1996, and implemented with State Department designations of FTOs on 8 October 1997)–providing material support or resources to designated FTOs; and

(c) 18 USC 2339C(a) (enacted 25 June 2002)–providing or collecting terrorist funds

(d) 18 USC 2339C(c) (enacted 25 June 2002)–concealing or disguising either material support to FTOs or funds used or to be used for terrorist acts.

174. These offenses are subject to an eight year limitation period, but 18 USC 3286 provides for an extension of this limitation period for certain terrorism offenses, including no limitation period where the act results in death.

175. Additionally, Executive Orders made by the U.S. President pursuant to the International Emergency Economic Powers Act (IEEPA) prohibit the contribution of funds to certain designated persons and organizations. In the case of EO 13224, the designated persons and organizations are "Specially Designated Global Terrorists" (SDGTs). Consequently, violations of EO 13224 are de facto terrorist financing offenses. Prosecutions pursuant to EO 13224 operate as alternatives to prosecutions under sections 2339A, 2339B and 2339C. U.S. authorities reported that, to date, "most defendants" have preferred to plead guilty to "IEEPA offenses" under EO 13224.

Providing material support to terrorists (18 USC 2339A)

176. Although the heading of section 2339A refers to providing material support to a "terrorist" this term is not used in the provision. Instead, the provision makes it an offense to provide material support

[46] 18 USC section 2339D was added to the federal criminal code in December 2004 to directly criminalize the act of receiving military-type training from a foreign terrorist organization. While the offense is related to the other terrorist support statutes, it does not by itself directly affect the financing of terrorism or terrorist organizations, and so is not discussed here more fully.

or resources intending that such material support be used to carry out violations of listed offense provisions. To obtain a conviction, the prosecution must prove the following.

(a) *Actus reus:* The defendant either provided or concealed or disguised material support or resources .

(b) *Intent:* The defendant knew or intended that the material support or resources were to be used to prepare for or carry out:

  (i) violations of certain offense provisions;

  (ii) the concealment of an escape from committing any such violations; or

  (iii) an attempt or conspiracy to commit such violations.

177. There is no definition of "terrorist act" as this phrase is not actually used in the provision. Rather the prosecution must prove that the defendant knew that the funds were to be used in preparation for or in the carrying out of a violation of any one of 37 federal offenses. There does not need to be a prior conviction for these specified offenses. Included in the 37 listed offenses, (for which material support must have been provided), is the "Federal Crime of Terrorism" [31 USC 2332(b)(g)(5)(B)] which requires proof of the following two elements:

(a) the act was calculated to influence the conduct of the U.S. government or to retaliate against the conduct of the U.S. government; and

(b) the act is a violation of another lengthy list of specified offenses. This list repeats all of those offense provisions in section 2339A(a) and includes several more offense provisions. These offense provisions generally relate to the conduct specified in the Treaties as required by Article 2(1) of the United Nations International Convention for the Suppression of the Financing of Terrorism (1999) (Terrorist Financing Convention).

178. Rather than providing funds, a conviction under this section requires provision of "material support or resources". This term is broadly defined to encompass virtually all tangible and intangible property (including currency, monetary instruments or financial securities) and services (including financial services), except for medicine or religious materials. The definition also extends beyond pure funding support to include lodging, training, expert advice or assistance, personnel (one or more individuals who may be or include oneself), transportation, weapons, false documentation etc. [18 USC 2339A(b)(1)].

Providing material support or resources to designated foreign terrorist organizations (18 USC 2339B)

179. Title 18 USC 2339B makes it an offense to provide material support or resources to a foreign terrorist organization (as opposed to the perpetrators of terrorist acts under section 2339A). To obtain a conviction, the prosecution must prove the following.

(a) *Actus reus:* The defendant provided material support or resources to a foreign terrorist organization. The term "material support or resources" has the same meaning as it does in section 2339A. The term "terrorist organization" means an organization that has been designated as such by the Secretary of State pursuant to section 219 of the Immigration and Nationality Act and section 302 of the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) [s.2339B(g)(6)]. As of May 2006, there were 41 organizations that had been listed by the U.S. as FTOs pursuant to the AEDPA. A list of the current FTOs and the legal criteria used to identify and publish additions to the list can be found on the State Department's website. All FTOs currently on the AEDPA list have also been designated pursuant to EO 13224 which list is administered by OFAC. Consequently, a violation of section 2339B will usually also give rise to a violation of IEEPA which is discussed below.

(b) *Knowledge:* The defendant acted with the knowledge that:

  (i) the organization is a designated terrorist organization; and

(ii) the organization has engaged or engages in terrorist activity or the organization engages in terrorism.

180. The term "engage in terrorist activity" is defined by reference to other legislation namely section 212(a)(3)(B) of the Immigration and Nationality Act [Title 8 USC 1182(a)(3)(B)(iv)]. This lengthy definition relies on a further definition of "terrorist activity" which is defined in Title 8 USC 1182(a)(3)(B)(iii) and includes the following:

(a) the highjacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle);

(b) the seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained;

(c) a violent attack upon an internationally protected person or upon the liberty of such a person;

(d) an assassination;

(e) the use of any (1) biological agent, chemical agent, or nuclear weapon or device, or (2) explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property; or

(f) a threat, attempt, or conspiracy to do any of the foregoing.

181. The term "terrorism" is defined in section 140(d)(2) of the Foreign Relations Authorization Act [see also 22 USC 2656f(d)(2)] as meaning "premeditated, politically motivated violence perpetrated against noncombatants by subnational groups or clandestine agents".

Terrorist financing—Provision or collection [18 USC 2339C(a)]

182. Section 2339C(a) tracks the language of Article 2(1) of the Terrorist Financing Convention and criminalizes the provision or collection of funds for terrorist financing. Under section 2339C(a), the prosecution must prove the following.

(a) *Knowledge:* The defendant acted willfully.

(b) *Intent:* The defendant knew or intended the funds to be used, in full or in part, to carry out specified acts. These are defined in sections 2339C(a)(1)(A) and 2339C(a)(1)(B) which mirror the definitions in the Terrorist Financing Convention except in the following respect. Section 2330C(a)(1)(B) defines "terrorist act" to be an act which constitutes an offense within the scope of all of the treaties listed in the Annex to the Terrorist Financing Convention [reproduced at section 2339C(e)(7)], to the extent that these treaties have been implemented by the U.S. All of the listed treaties have entered into force in the U.S.

(c) *Actus reus:* The defendant provided or collected funds, directly or indirectly, by any means. The term "funds" is defined in similar terms to that in the Terrorist Financing Convention.

(d) *Factual predicate:* There must be jurisdiction [set out in section 2339C(b)]. This is further discussed below.

183. There is no requirement under section 2339C(a)(1) for the prosecution to prove that the funds were actually used to carry out a terrorist act.

Terrorist financing—Concealment or disguise of material support or funds [18 USC 2339C(c)]

184. Section 2339C(c) makes it an offense to knowingly conceal or disguise terrorist assets.

(a) *Actus reus:* The defendant concealed or disguised the nature, location, source, ownership or control of any material support or resources, funds or proceeds.

(b) *Knowledge:* The defendant acted knowingly.

(c) *Intent:* The defendant knew or intended that the concealed property was (or would be) provided to a designated foreign terrorist organization (in violation of s.2339B) or were (or would be) provided/collected [in violation of § 2339C(a)].

(d) *Factual predicate:* The defendant was either:

  (i) inside the U.S.; or

  (ii) outside the U.S. and is a U.S. national or legal entity.

185. Sections 2339C(a) and 2339A cover the same sort of criminal conduct and could be used interchangeably. To date there have been no successful prosecutions under section 2339C. The DOJ has confirmed that prosecutions under section 2339A would be much easier than those under section 2339C. The definition of "material support and resources" under section 2339A covers a much broader range of activity than the definition of "funds" under section 2339C. Section 2339A does not require proof of specific jurisdiction as is required in section 2339C. Prosecution under both provisions does, however, require the prosecution to prove that the funds or material support were or are to be used to carry out an act that is not clearly defined and requires reference to other legislation or treaties.

Violation of Executive Order 13224

186. On 23 September 2001, pursuant to powers and authorities under the IEEPA (50 USC 1702 and 1702), the U.S. President issued EO 13224 "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism". Although EO 13224 is principally directed towards the blocking of various transactions involving designated persons and organizations [known as SDGTs)–discussed further in Section 2.4.1 and Section 6], EO 13224 also prohibits U.S. persons (including U.S. legal entities, their branches worldwide, and in some circumstances, foreign subsidiaries of U.S. companies) from making or receiving any contribution of funds, goods, or services to or from those persons listed in the Annex to the Executive Order or subsequently designated by the Secretaries of the Treasury and State under the terms of the Executive Order. Persons who violate the prohibition under EO 13224 can be prosecuted which makes it a de facto terrorist financing offense. EO 13224 is discussed in more detail in section 2.4 of this report.

Ancillary offenses

187. It is also an offense to attempt or conspire to commit any of the above-noted terrorist financing offenses [s.2339A(a); s.2339B(d)(1)(F); s.2339C(a)(2); s.1705, IEEPA; s.2, EO 13224]. Additionally, it is an offense to aid and abet, counsel, command, induce, procure or willfully cause any of these terrorist financing offenses. Persons who commit these ancillary offenses may be prosecuted as principals (18 USC 2).

Predicate offenses for money laundering

188. Section 2339A, Section 2339B, and Section 2339C are predicate offenses for money laundering [see 18 USC 1956(c)(7)(D)]. Section 2339C was recently added to the list of money laundering predicates by section 409 of the USA PATRIOT Improvement and Reauthorization Act of 2005, enacted on 9 March 2006 as Public Law No. 109-177.

Scope of liability

189. Sections 2339A, 2339B and 2339C all apply to "whoever" and, as discussed below, this is interpreted to include legal persons. Making legal persons subject to criminal liability for terrorist

financing does not preclude the possibility of parallel civil liability under section 2339C(f) for violations under section 2339C(a).

190. There are no specific jurisdictional limits to prosecutions under Section 2339A. Section 2339B (the offense of providing material support to designated FTOs) defines those liable for these offenses as anyone within the U.S. or subject to its jurisdiction. The crime also expressly provides for extraterritorial federal jurisdiction [18 USC 2339B(a)(1) and (d)]. The U.S. terrorist financing enforcement program uses these provisions to allow for the prosecution of U.S. citizens and U.S. persons for conduct they commit overseas, or non-U.S. persons whose criminal conduct occurs within the U.S. Non-U.S. persons, including persons who have never been in the U.S., have been charged with a section 2339B conspiracy, as long as overt acts of the conspiracy have occurred within the territory of the U.S.

191. The jurisdictional limitations for prosecutions under section 2339C(a) are somewhat confusing. Essentially where the offense takes place in the U.S. there either needs to be some physical connection to another country or otherwise the prosecution must prove: (1) that the offense was directed towards a predicate act committed in an attempt to compel the U.S. to do or abstain from doing anything [2339C(b)(5)]; or (2) that either the offense or the predicate act affects interstate or foreign commerce. The broad interpretation of the "interstate or foreign commerce" requirement by the courts has been previously noted.

192. Section 2 of EO 13224 states that any U.S. person or person within the U.S. may be found liable for violating the order. The term "person" is defined as being any natural or legal person, including a partnership, association, corporation or other organization, group or subgroup (s.3, EO 13224).

193. The law permits the intentional element of the terrorist financing offense to be inferred from objective factual circumstances. There is however very little case law on any of these offenses to assess this issue properly. The small amount of litigation surrounding sections 2339A and 2339B revolves around the constitutional validity of the provisions as well as whether allegations under these provisions can form the basis of civil compensation claims by the victims.

Sanctions for terrorist financing offenses

194. The penalty for criminal violations of 18 USC 2339A and 2339B are fines and/or imprisonment for a period of up to 15 years for each violation, and if death of any person results, for any term of years or for life. The penalty for criminal violations of 18 USC 2339C is a fine and/or imprisonment for a period up to 20 years for each violation. The penalty for criminal violations of 18 USC 2339C(c) is a fine or imprisonment for up to 10 years. The penalty for criminal violations of EO 13224 (IEEPA) (50 USC 1701) include substantial fines (up to USD 50,000) and/or imprisonment for up to 20 years.[47]

195. There are no civil penalty provisions relating to violations of sections 2339A or 2339C(c), however legal entities (not individuals) either located in the U.S. or organized pursuant to U.S. law who violate subsection 2339C(a) are subject to civil penalties of at least USD 10,000, if a person responsible for the management or control of that legal person has, in that capacity, committed an offense [2339C(f)].

196. Financial institutions (as that term is broadly defined in the BSA) above which become aware that they have possession of or control over any funds in which a foreign terrorist organization or agent has an interest have a positive duty to retain possession or maintain control of these funds and report the existence of such funds. Financial institutions will be subject to civil penalties where they violate this subsection [2339B(a)(2)].

[47] The maximum penalty for a violation of a provision of the IEEPA was recently enhanced from ten to twenty years by section 402 of the USA PATRIOT Improvement and Reauthorization Act of 2005, enacted on 9 March 2006 as Public Law No. 109-177.

State laws

197. At least two states have enacted terrorist financing offenses—Arizona and New York. No information was provided concerning whether other states have terrorist financing offenses.

Effectiveness of the terrorist financing offenses

198. The U.S. provided materials showing that it has charged 126 individuals with criminal violations of the specific terrorist financing offenses discussed above (i.e. 18 USC 2339A, 2339B, and 2339C). Of those 126 so charged, 54 so far have either pleaded guilty or been convicted of either 18 USC 2339A or 2339B.

2.2.2 Recommendations and Comments

199. While the terrorist financing provisions cover conduct as required by the Terrorist Financing Convention it is very difficult legislation to follow and in some aspects seemingly unnecessarily complicated. For example, given that both provisions have the same constitutional limitations, it is not clear why the prosecution is required to work through a series of options to prove a jurisdictional requirement in section 2339C(a) when there are no such jurisdictional requirements for prosecutions under section 2339A. The main difficulty with the U.S. terrorist financing provisions is that they are not self contained, in that many key terms such as "terrorist act", "terrorist activity" and "foreign terrorist organization" are defined by reference to other legislation. The need for cross referencing to other legislation makes it quite difficult to understand the elements of the offenses. More importantly prosecutors have confirmed that this adds to difficulties in prosecutions as judges and juries have to be guided through what seems to be an unnecessarily complex legislative chain. Even the newest and clearest terrorist financing provision (2339C) is not wholly self-contained with the key element of the terrorist act being defined by reference to a series of treaties as implemented by the U.S. Prosecutors have to therefore firstly prove that the defendant's conduct falls within that prohibited by one of these nine international treaties and then prove that that part of the treaty has been implemented by the U.S. These comments do not, however, affect the rating.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	C	• This Recommendation is fully observed.

2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)

2.3.1 Description and Analysis

Recommendation 3 (Freezing, seizing and confiscation)

Federal laws

Forfeiture

200. The U.S. has parallel civil (*in rem*) and criminal (*in personam*) forfeiture systems, which provide for the forfeiture of both the instrumentalities and proceeds of crime. Administrative forfeiture can also be applied under certain conditions.

201. Criminal forfeiture (18 USC 982) is dependant on the conviction of the defendant and is imposed concurrently. The burden of proof in money laundering cases requires that both the government and claimants (persons contesting the forfeiture) establish their respective claims by a preponderance of the evidence. In addition to the specific and express penal provisions of 18 USC 982, property is subject to criminal forfeiture in all cases where civil forfeiture is provided for [Civil Asset Forfeiture Reform Act 2000 (CAFRA), 28 USC 2461(c)].

202. Civil forfeiture actions (18 USC 981) are not conviction-related and are instituted against the offense-generated or related property itself on a preponderance of evidence standard, as opposed to the reversed onus of proof before the CAFRA. The legal controversy about the concurrent use of civil forfeiture actions and criminal proceedings, which in the past affected the use of civil forfeiture, was solved by a Supreme Court ruling confirming that this did not constitute "double jeopardy".

203. Administrative forfeiture (or "nonjudicial civil forfeiture") through the seizing law enforcement authority is possible if no claims contesting the forfeiture are timely filed. The procedures are detailed in 18 USC 983(a)(1) & (2), and 19 USC 1602. The availability of administrative forfeiture is limited to four categories of property:

(a) where the value does not exceed USD 500,000 per individual item;

(b) where its importation is illegal;

(c) where it is a means of transportation used in moving or storing controlled substances; or

(d) where it is currency or monetary instrument of any value.

204. As long as the forfeiture remains uncontested, the judiciary authorities are not involved. As the statistics show, most forfeitures are dealt with this way.

205. There is no general provision imposing forfeiture for instrumentalities used in or proceeds from all crime. Forfeiture of property is only possible when provided in a specific statute and when related to a large number of offenses specified in 18 USC 981 and 982, including ML and TF:

(a) Title 18 USC 981(a)(1)(A) and 982(a)(1) provide for civil or criminal confiscation in a money laundering context (18 USC 1956, 1957 and 1960), in addition to the predicates constituting SUA [18 USC 981(a)(1)(C)].

(b) In terrorist financing cases forfeiture (both civil and criminal) is made possible by:

  (i) Title 18 USC 981(a)(1)(C) which provides for the forfeiture of the proceeds of all specified unlawful activities (including supporting and financing terrorism as in 18 USC 2339A, 2339B and 2339C);

  (ii) Title 18 USC 981(a)(1)(G) for terrorism activities; and

  (iii) Title 18 USC 981(a)(1)(H) for collecting or providing funds for terrorist purposes [18 USC 2339C(a)].

206. Confiscation is mandatory in a criminal case whenever the court considers the facts established.

207. The statute of limitations for criminal forfeiture proceedings follows that of the money laundering and terrorist financing offenses, namely five years (for money laundering) or eight years (for terrorist financing) counting from discovery of the facts or termination of the criminal activity. The statute of limitations for civil forfeiture is five years from the date of the discovery of the offense or two years from the discovery of the involvement of the property in the offense whichever is later (19 USC 1621).

208. The law provides for the forfeiture of "any property, real or personal, involved" in particular offenses, "or any property traceable to such offense" (18 USC 981 and 982). The term "property" is not strictly defined, but jurisprudence has held that the term "property involved" should be read broadly to include: the money or other property being laundered (the *corpus* or "subject matter" of the money laundering offense); any commissions and fees paid to the money launderer; and any property used to facilitate the money laundering offense. Applying this definition, the property subject to forfeiture in a money laundering case falls into the following categories:

(a) the proceeds of the SUA being laundered and consequently becoming the *corpu*s or the subject matter of the money laundering offense (i.e. property part of, or integral to, the money laundering transaction). Moreover jurisprudence in conspiracy and attempt cases has established that the proceeds the defendant conspired or attempted to launder could be forfeited, even if the offense was not completed;

(b) property other than the SUA proceeds which is also part of the subject matter of the money laundering offense (commingled property). This may include "clean" money being used to commit a criminal offense and property that is the subject of a purchase, sale or exchange constituting a money laundering offense. Thus any time that a money laundering offense is committed through a financial transaction, the assets purchased or sold or obtained are "involved" in the offense and constitute part of the subject matter of the crime that can be forfeited (i.e. property used to facilitate the money laundering offense or so-called "instrumentalities"). It can be deduced from the very broad notion of "involvement" that instrumentalities used or intended for use in the commission of an offense are also subject to confiscation. Such confiscation is expressly provided in the context of the criminal forfeiture procedure under 21 USC 853(a)(2) on condition of the "property used or intended to be used" belonging to the defendant;

(c) property (other than the proceeds) used to facilitate the money laundering offense; and

(d) substitute assets, investment yields and other benefits of the proceeds of crime. The import of the wording "involved" and "traceable" is indeed broad enough to encompass all direct and indirect derivatives of the proceeds of crime. In the same reasoning, any other asset or valuable, material or immaterial (such as licenses), can be forfeited if in any way linked to or resulting from an offense.

209. In the terrorism financing offense context of 18 USC 2339C(a), legitimate assets, used to that purpose, are to be forfeited pursuant to 18 USC 981(a)(1)(H). *Mutatis mutandis* the other categories applicable to the ML also apply here. No confiscation is however specifically provided in connection with the terrorism support offenses of 18 USC 2339A and 2339B. This may arguably be covered by 18 USC 981(a)(1)(C) forfeiting the proceeds of SUA offenses (including sections 2339A and 2339B) where the term "proceeds" is then considered broad enough to include the *corpus* of the offense. Any controversy over this apparent lacuna however is now being pre-empted by draft legislation expressly stipulating forfeiture for these specific offenses.

210. Equivalent value forfeiture is only possible in a criminal procedure, as then confiscation is always compulsory. Since the forfeiture is directed against the defendant personally and not at particular items of property, the court can enter a money judgment against the defendant for the value of the property, to be executed against the defendant's personal assets, or can order the forfeiture of substitute assets if the property has been dissipated or cannot be found. This concept is primarily based on Rule 32.2 of the Federal Rules of Criminal Procedure and is firmly embedded in case law.

211. All property constituting the subject matter of a money laundering offense being subject to forfeiture, the forfeiture is not limited to the net profits realized from a sale or exchange, but includes any property that was involved in the offense. Also, when money laundering activity relates to commingled funds, forfeiture applies to the commingled funds as "property involved" in the offense.

212. Only property belonging to the defendant can be forfeited in a criminal case considering the *in personam* character of the procedure. Consequently property that belongs to third parties cannot be forfeited criminally, even if the defendants used it to commit the offenses for which they were convicted, except if the third party itself is charged and convicted for (aiding and abetting or conspiracy to) money laundering. However, property held by nominees, delegates and persons who did not acquire their interest until after the crime was committed can be forfeited as property of the defendant.

213. To forfeit property belonging to third parties at the time the crime was committed (for instance in the case of money seized in the hands of couriers), or that was derived from or used to commit crimes other than the one for which the defendant has been convicted, the government must use the civil *in rem* forfeiture. This obviously requires the presence of an object (*res*) upon which the forfeiture can be applied, together with a causal link between that object and the originating offense ("involved" or "traceable").

214. The combination of both confiscation proceedings gives the system a versatility that enhances effective asset recovery. The Supreme Court's rejection of the double jeopardy challenge between the criminal and civil forfeiture proceedings has ended the dispute over this issue and enables the prosecution to switch from criminal to civil forfeiture whenever the need arises (e.g. in the event that the defendant dies before a final conviction could be secured).

Seizure:

215. Property subject to forfeiture can be seized, frozen (restrained), or otherwise preserved prior to trial in order to ensure that it remains available, provided that there is probable cause to believe that the property is subject to confiscation. The court in a criminal case is permitted to issue both pre-indictment and post-indictment restraining orders under 21 USC 853(e). The property can also be seized with a criminal seizure warrant [s.853(f)] if it is demonstrated that a restraining order would not be adequate to preserve the property. Similarly, federal courts have broad authority in forfeiture proceedings *in rem* to "take any...action to seize, secure, maintain, or preserve the availability of property subject to...forfeiture," pursuant to 18 USC 983(j), as well as authority to issue a seizure warrant pursuant to 18 USC 981(b).

216. However, only property "involved in" or "traceable to" the offense can be seized. Consequently the seizure of unrelated property aimed at securing assets for the execution of a money judgment is not covered, nor provided for by any statute, except in one very specific circumstance. A special seizure/confiscation regime is provided by section 319 of the USA PATRIOT Act allowing the government to seize funds subject to forfeiture which are located in a foreign bank account, by authorizing the seizure of the foreign bank's funds that are held in a correspondent U.S. account, regardless of whether or not the money in the correspondent account is directly traceable to the money held in the foreign bank account. The funds in the U.S. account are then seized as a substitute for the foreign deposit. This provision enhances the ability of prosecutors to obtain the criminal proceeds that have been placed offshore. The provision has already been used in 11 cases.

217. Nevertheless, the equivalent value confiscation and seizure regime is problematic. Equivalent value confiscation is not possible in civil forfeiture proceedings because of its strict *in rem* nature and the condition of the assets having some relation to the offense. In the criminal confiscation regime, money judgments against the (assets of the) defendant may be considered to have the effect of an equivalent value forfeiture, but in that case no statute provides for the restraint/seizure of property that is unrelated to any offense for the purpose of avoiding dissipation of the assets and enabling effective execution of the money judgment against untainted property. Jurisprudence is apparently quite divided on this issue, with the majority rulings going against the possibility of such seizure. This shortcoming in the confiscation regime should be remedied (preferably through legislative action) to allow for equivalent value seizure.[48]

218. The initial application to restrain or seize property subject to confiscation can be made *ex-parte* and without prior notice. No pre-restraint hearing is required for either a pre-indictment or post-indictment order or a civil seizure warrant [21 USC 853(e)].

[48] Draft legislation is pending before Congress which will allow for equivalent value seizure.

219. The power to identify and trace property that is subject to forfeiture under the relevant statutes is a basic investigative tool for all law enforcement agencies. Those powers include the use of grand jury subpoenas and/or administrative subpoenas as well as search warrants. Through the reporting obligations—SAR, Currency Transaction Reports (CTR), and Forms 8300, among others—FinCEN is also in a position to identify and discover potential forfeitable assets, and to make that information available to the law enforcement agencies.

Third party protection

220. Civil forfeiture: To protect the interests of innocent property owners who were unaware that their property was used for illegal purposes or of true bona fide purchasers for value, there is the possibility of a "uniform innocent owner" defense. If somebody claims he/she is a bona fide purchaser, he/she must be a "purchaser" in the commercial sense, but he/she must also show that at the time of the purchase he/she "did not know and was reasonably without cause to believe that the property was subject to forfeiture." Under that statute, persons contesting the forfeiture must establish their ownership interests and their innocence by a preponderance of the evidence [18 USC 983(d)].

221. Criminal forfeiture: Only property belonging to the defendant can be criminally forfeited. Criminal proceeds and property owned by the defendant at the time of the offense, but later transferred to a third party are considered property of the defendant for purposes of criminal forfeiture. Ownership issues are not addressed in the forfeiture phase of the criminal procedure. Third party interests are dealt with in an ancillary proceeding set forth in 21 USC 853(c) and (n), and Rule 32.2(c) of the Federal Rules of Criminal Procedure to determine the ownership of the property. If the ownership of the defendant is established, the forfeiture becomes valid and final, otherwise it is declared void and the property must be restored to the third party concerned.

222. It is interesting to note that, according to some law enforcement authorities, the reinforcement of third parties' rights with the introduction of the CAFRA has given rise to abusive practices and generated an increase of disruptive actions, where numerous claims are being filed against the property by family members of the defendant or other proclaimed interested parties in an attempt to negate the forfeiture action and recover the assets. The circumstance that the government is liable for payment of the defendant's lawyer fee if it loses the case is also considered a restraining factor.

223. In preventing or voiding actions taken to avoid the consequences of forfeiture, the "relation back" doctrine applies [21 USC 853(c) and (n)(6)(B) for criminal forfeiture and 18 USC 981(f) and 983(d)(3) for civil forfeiture]. Pursuant to this doctrine, once the government obtains a judgment of forfeiture, title vests as of the time that the commission of the act giving rise to the forfeiture occurs. Therefore, unless subsequent transferees are bona fide purchasers, those subsequent transfers can be invalidated.

Additional elements

224. The property of organizations that are primarily criminal in nature are subject to forfeiture. The RICO statute authorizes the forfeiture of all assets of an "enterprise," or any property affording a defendant a "source of influence" over the enterprise [18 USC 1963(a)]. Additionally, all assets (foreign or domestic) of a domestic or international terrorist or terrorist organization are subject to civil and criminal forfeiture [18 USC 981(a)(1)(G)] if directed against the U.S., its citizens and residents, or their property. As noted above, the U.S. has also effectively implemented a system of civil forfeiture.

225. U.S. forfeiture law generally does not allow reversal of the burden of proof. In fact civil forfeiture has lost some of its appeal since the CAFRA did away with the burden of proof reversal to the defendant. Now, in most *in rem* forfeiture cases, the government must establish by a preponderance of the evidence that the property is subject to forfeiture [some exceptions to this rule are possible is in the context of terrorism cases under 18 USC 981(a)(1)(g), see 18 USC 987, and some cases under U.S. customs laws]. In criminal forfeiture cases, the prosecution must first prove the

defendant's guilt beyond a reasonable doubt and then establish the extent of the forfeiture by a preponderance of the evidence standard.

State laws

226. Forfeiture provisions at the state level typically relate to "racketeering" offenses. They generally follow the line of the federal forfeiture laws and predominantly have a complementary character. Seizure/confiscation measures in a specific money laundering context obviously only exist in the 38 States that have promulgated anti-money laundering statutes. Of the samples reviewed by the evaluation team, Arizona's *in rem* and *in personam* forfeiture system was of particular interest for its protection of the innocent third party or victim, its broad scope and its versatility.

Effectiveness of the freezing, seizing and confiscation measures

227. It is clear from the available relevant data that the U.S. has made a priority of the recovery of criminal assets and is systematically and vigorously pursuing seizure and confiscation. To achieve that goal law enforcement can count on a comprehensive and solid legal basis, and on the support of specialists. The forfeiture system is quite flexible to offer the possibility to use the most effective and adequate procedure: civil, criminal or administrative. If the money laundering statutes are not applicable or suitable for any reason, there are a series of related penal provisions the authorities can and do use frequently to recover the criminal assets (such as bulk cash smuggling, structuring and other BSA offenses, IEEPA violations, bank fraud offenses, etc).

228. To enhance the asset seizure and forfeiture effort, law enforcement can rely on the support of specialized prosecutors, offices and agents, such as the attorneys involved in the Justice and Treasury Asset Forfeiture Funds, the IRS-CI field offices known as Asset Forfeiture Coordinators (AFCs), and US ICE Asset Identification and Removal Groups (AIRG). These specialists are responsible for providing expert advice to the field agents when they are conducting a money laundering or terrorist financing investigation about the viability to seize and forfeit assets, and track the assets until final disposition.

229. The figures on amounts seized and forfeited are quite substantial, even taking into account the proportionality with the size of the country. The statistics show that the U.S. freezing, seizing and confiscation regime is performing. Significant (and steadily increasing) amounts of proceeds have been forfeited in recent years: USD 564.5 million in 2003, USD 614.4 million in 2004 and USD 767.4 million in 2005. The following statistics (which were provided by the DOJ) concern the amount of property that was seized and confiscated relating to criminal proceeds and terrorist financing by law enforcement agencies during fiscal years 2004 to 2005.

JUSTICE ASSET SEIZURES AND FORFEITURES BY AGENCY FOR FISCAL YEAR 2004					
AGENCY	FORFEITURE TYPE	SEIZED ASSETS	SEIZED VALUE	FORFEITED ASSETS	FORFEITED AMOUNT
DEA	Administrative	11,639	USD 260,669,786.50	10,699	USD 216,235,774.96
	Civil/Judicial	2,001	USD 122,250,783.24	1,147	USD 79,957,319.37
	Criminal	1,590	USD 76,602,535.23	1,146	USD 66,485,824.53
DEA TOTALS		15,230	USD 459,523,104.97	12,992	USD 362,678,918.86
FBI	Administrative	1,387	USD 62,803,379.11	1,104	USD 55,834,952.99
	Civil/Judicial	774	USD 102,658,679.48	579	USD 86,484,310.09
	Criminal	1,686	USD 113,793,994.87	1,190	USD 55,561,737.25
FBI TOTALS		3,847	USD 279,256,053.46	2,873	USD 197,881,000.33
FDA	Civil/Judicial	18	USD 2,508,102.12	4	USD 775,822.92
	Criminal	8	USD 1,556,739.00	2	USD 1,255,000.00

FDA TOTALS		26	USD 4,064,841.12	6	USD 2,030,822.92
DHS[49]	Administrative	0	USD 0	3,899	USD 8,098,066.23
	Civil/Judicial	4	USD 1,457,599.84	22	USD 2,029,897.82
	Criminal	1	USD 1	20	USD 557,747.37
DHS TOTALS		5	USD 1,457,600.84	3,941	USD 10,685,711.42
USMS	Civil/Judicial	22	33,101,708.76	24	USD 30,872,594.21
	Criminal	49	USD 1,281,103.81	44	USD 1,679,262.62
USMS TOTALS		71	USD 34,382,812.57	68	USD 32,551,856.83
USPS	Civil/Judicial	117	6,261,092.81	77	USD 3,654,475.65
	Criminal	218	USD 19,622,549.82	166	USD 4,927,405.58
USPS TOTALS		335	USD 25,883,642.63	243	USD 8,581,881.23
FY 2004 TOTALS		19,514	USD 804,568,055.59	20,123	USD 614,410,191.59

JUSTICE ASSET SEIZURES AND FORFEITURES BY AGENCY FOR FISCAL YEAR 2005					
AGENCY	FORFEITURE TYPE	SEIZED ASSETS	SEIZED VALUE	FORFEITED ASSETS	FORFEITED AMOUNT
DEA	Administrative	10,903	USD 321,358,941.29	10,957	USD 295,265,225.97
	Civil/Judicial	2,106	USD 119,286,467.87	1,214	USD 51,911,270.68
	Criminal	1,380	USD 107,318,909.36	1,122	USD 49,196,100.56
DEA TOTALS		14,389	USD 547,964,318.52	13,293	USD 396,372,597.21
FBI	Administrative	1,504	USD 52,050,695.67	1,191	USD 46,372,723.73
	Civil/Judicial	824	USD 266,200,272.30	594	USD 197,789,177.76
	Criminal	1,715	USD 310,745,786.13	1,289	USD 93,402,716.81
FBI TOTALS		4,043	USD 628,996,754.10	3,074	USD 337,564,618.30
FDA	Civil/Judicial	24	USD 5,799,790.77	4	USD 905,845.00
	Criminal	58	USD 6,150,357.94	41	USD 4,839,648.35
FDA TOTALS		82	USD 11,950,148.71	45	USD 5,745,493.35
DHS	Civil/Judicial	20	USD 1,832,018.10	24	USD 2,770,588.33
	Criminal	0	USD 0	6	USD 92,819.96
DHS TOTALS		20	USD 1,832,018.10	30	USD 2,863,408.29
USMS	Civil/Judicial	24	USD 10,321,100.47	29	USD 8,082,023.08
	Criminal	33	USD 1,513,288.99	52	USD 349,444.15
USMS TOTALS		57	USD 11,834,389.46	81	USD 8,431,467.23
USPS	Civil/Judicial	193	USD 43,158,507.65	70	USD 6,633,797.95
	Criminal	187	USD 10,977,524.37	220	USD 9,742,585.49
USPS TOTALS		380	USD 54,136,032.02	290	USD 16,376,383.44
FY 2005 TOTALS		18,971	USD 1,256,713,660.91	16,813	USD 767,353,967.82

230. The following statistics (which were provided by the Treasury) concerning the amount of property that was confiscated by various Treasury agencies for the years 2002 to 2005.

AGENCY	2002	2003	2004	2005
ATF	USD 2,780,132	USD 3,208,977	USD 7,783,347	USD 4,225,119
USSS	USD 5,968,707	USD 14,407,909	USD 9,762,931	USD 3,707,194
IRS	USD 54,246,330	USD 64,013,754	USD 78,202,183	USD 132,048,861
ICE & CBP[50]	USD 92,359,804	USD 152,444,062	USD 194,785,019	USD 145,608,128

[49] Note – INS no longer exists as an agency. The functions performed by INS are now performed by ICE and CBP.

[50] ICE and CBP are part of DHS, not Treasury. However, assets forfeited by ICE and CBP are placed in the Treasury Asset Forfeiture Fund (prior to the creation of DHS, legacy U.S. Customs was part of the Treasury Department).

TOTAL	USD 152,354,973	USD 234,047,702	USD 290,533,480	USD 285,649,302

2.3.2 Recommendations and Comments

231. Overall, the U.S. system for freezing, seizing and forfeiture is quite robust and is achieving good results. There are, however, some weaker areas. For instance, as a consequence of the limitation of the money laundering offense in respect of foreign predicate criminal activity, confiscation is equally restricted. Even though U.S. Attorneys will then endeavor to seek conviction and confiscation based on offenses other than money laundering, or based on domestic specified unlawful activities by virtue of the fact that the proceeds or other objects of the offense traveled through foreign commerce and were laundered in the U.S., the restriction represents a deficiency that needs to be addressed. Likewise, insofar as the money laundering offense does not cover all designated categories of predicate offenses as SUA (insider trading, market manipulation and, to a certain extent, piracy are not predicate offenses for money laundering), confiscation is similarly affected. (For a more detailed discussion of the gap in predicate offenses, see section 2.1 above). As well, the inability to freeze or seize assets of equivalent value is problematic.

232. The U.S. should therefore extend domestic and foreign predicates to fully cover all 20 categories of predicate offenses listed in the Glossary to the FATF 40 Recommendations. It should also take measures to ensure that property which may be subject to equivalent value confiscation may be seized/restrained to prevent its being dissipated.

2.3.3 Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	LC	• Where the proceeds are derived from one of the designated categories of offenses that are not domestic or foreign predicate offenses for ML, a freezing/seizing or confiscation action cannot be based on the money laundering offense. • Property of equivalent value which may be subject to confiscation cannot be seized/restrained.

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and Analysis

Special Recommendation III (Freezing and confiscating terrorist assets)

Freezing

233. The U.S. implements its obligations relating to financial sanctions under both United Nations Security Council Resolution S/RES/1267(1999) and S/RES/1373(2001) through Executive Order 13224 "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism" (EO 13224) issued by the U.S. President on 23 September 2001, in response to the terrorist attacks of 11 September 2001.

234. EO 13224, as amended, authorizes the Secretaries of the Treasury and State, in consultation with the DOJ and the DHS, to implement the President's authority to combat terrorists, terrorist organizations and terrorist support networks systemically and strategically. EO 13224 prohibits any U.S. person or entity from transacting or dealing with individuals and entities owned or controlled by, acting for or on behalf of, financially, technologically, or materially assisting or supporting, or otherwise associated with SDGTs, namely, persons listed in the Executive Order or subsequently designated by the Secretaries of the Treasury and State under the terms of the Executive Order. The Executive Order also blocks all property or interests in property of designated persons in the United States. The designation is done *ex parte* without notifying the involved party.

235. The OFAC list (which is administered by the Treasury) also comprises FTOs that are named under section 219 of the Immigration and Nationality Act and section 302 of the Antiterrorism and Effective Death Penalty Act (AEDPA). These designations only apply to terrorist organizations. The FTO list is administered by the State Department.

236. OFAC administers and enforces the EO 13224 sanctions against terrorists and terrorist organizations, as well as the U.S. economic and trade sanctions against designated foreign countries, international drug traffickers and persons involved in weapons of mass destruction proliferation. It has 125 staff and currently administers 30 economic sanctions programs against foreign governments, entities and individuals.

237. EO 13224 gives the government authority to:

(a) identify and designate terrorists and support structures related to terrorist organizations (not limited to, but also including those parties designated by the UN 1267 Committee and related to Al-Qaida, Usama bin Laden, and the Taliban);

(b) prohibit U.S. persons from having dealings with these designated parties; and

(c) demand that U.S. persons freeze assets related to these designated parties and report these actions to the OFAC.

238. EO 13224 thus targets not only Al-Qaida and the Taliban, but includes terrorist groups such as Hamas, Hizballah, the FARC, the Real IRA, and associated individuals and entities. A designation puts U.S. persons on notice that they are prohibited from having dealings with those specific persons and must block their assets.

239. The designation makes it unlawful for a person in the United States or subject to the jurisdiction of the U.S. to have dealings with the designated person, called an SDGT. Any U.S. financial institution that becomes aware that it has possession of or control over funds in which a SDGT or its agent has an interest must retain possession of or control over the funds and report the funds to OFAC. Generally, U.S. financial institutions must block or freeze funds that are remitted by or on behalf of a blocked individual or entity, are remitted to or through a blocked entity, or are remitted in connection with a transaction in which a blocked entity has an interest. Additionally, OFAC enforcement officers may serve blocking orders on designated persons within the U.S. These actions may involve the complete shutdown of the entity and the placement of blocked non-financial property in permanent storage. Once funds are blocked, they may be released only by specific authorization from the Treasury. As of July 2005, 438 persons had been designated since the beginning of the terrorism program under EO 13224. Approximately 330 of the designations have been bilateral and/or through the UN.

240. Whenever an individual or entity is proposed for inclusion on the UN 1267 consolidated list by another country through the UN or is proposed to the U.S. bilaterally, OFAC or the State Department is responsible for preparing an administrative record or "evidentiary" in support of a U.S. domestic designation under EO 13224. This process may require continued discussions with the initiating party and further coordination through the UN or with other countries in order to obtain sufficient information to meet domestic legal criteria. These procedures apply in cases in which:

(a) new designations are being proposed; or

(b) there is a request to introduce a new name or alias (a.k.a.) to an existing designation.

241. Not all persons and entities designated in the context of S/RES/1267(1999) and S/RES/1373(2001) were accepted by the U.S. to be included in the EO 13224, because the U.S. considered them not to contain sufficient identifying information to make the listing of these names operationally constructive. Consequently, only one of the 143 Taliban names has been placed on the OFAC list for fear of the counterproductive effects as a result of the confusion and uncertainty such a list would create leading to unjustified blockings. The Taliban was designated as an entity as a whole,

whereby all individuals involved in that organization are deemed to be included. In this system, OFAC takes on the responsibility of organizing the information supply and appropriate support to the relevant sectors. However, this raises an issue: although domestic designation in the context of S/RES/1373(2001) is indeed largely dependant on the acceptance of the adequacy of the information supplied by the requesting jurisdiction, S/RES/1267(1999) is fully mandatory and apparently does not allow (nor does SRIII) any free interpretation.[51]

242. Blocking actions pursuant to EO 13224 extend to all property and "interests in property" that come within the U.S. or that thereafter come within the U.S., or that thereafter come within the possession or control of U.S. persons. The term "interests in property" means an interest of any nature whatsoever, direct or indirect, in whole or in part (CFR 594.306). The broad definition of "assets and property" and "property interests" can affect most products and services provided by financial institutions located in the U.S. or organized under the laws of the U.S., including their overseas branches. Blocked property may not be transferred, withdrawn, exported, paid, or otherwise dealt in without prior authorization from OFAC.

Communicating actions taken under freezing mechanisms and guidance

243. To give effect to the sanctions programs, OFAC publishes, updates and maintains an integrated list of designated parties that U.S. persons cannot deal with and whose assets must be frozen and reported. Parties designated under EO 13224 are included on this integrated list. Designations are subsequently published in the U.S. Government's Federal Register. The OFAC list is continually being revised.

244. The U.S. authorities advised that every regulatory agency (both at the federal and state level) receives priority electronic notice of all of OFAC's designations and other actions affecting the financial community. The regulators assist in disseminating that information to their examiners and the institutions under their supervision. Furthermore, OFAC maintains an Internet list on its website that informs all its subscribers of any update of its information. OFAC also uses a fax broadcast system as well as a separate e-Alert system to reach financial and securities associations, which in turn are expected to transmit the notice to their members. When an institution identifies an entity that is an exact match, or has many similarities to a subject listed on the Specially Designated Nationals (SDN) and Blocked Persons List, the institution can call OFAC's Compliance Hotline for verification.

245. The functional regulators issue guidelines for banks and other entities, and their examiners ensure compliance with sanctions administered by OFAC. OFAC provides assistance in developing such guidance. OFAC has issued general guidance which is applicable to any person or entity. It has also issued industry-specific guidance to the following sectors: banking, securities, insurance, MSB, real estate settlement, corporate registration and NPO sectors, among others. Nevertheless, these communications do not seem to be working effectively outside of the banking, securities and MSB sectors. Indeed, some representatives from the private sector that the assessment team met with were not aware of their responsibilities pursuant to the OFAC list. This seemed particularly the case with the state-regulated sectors. OFAC might benefit from additional resources to continue to increase its outreach efforts further to various industries.

Delisting and unfreezing requests

246. There are policies and procedures in place to consider de-listing requests and to allow for the "unfreezing" of funds belonging to a de-listed individual or entity. A blocked person may seek administrative reconsideration of its designation or assert that the circumstances resulting in the designation no longer apply, and thus seek to have the designation rescinded (31 CFR 594.201 and 501.807). The procedures apply to persons blocked pursuant to any of the U.S. government sanctions programs administered by OFAC, including the terrorism program established pursuant to EO 13224.

[51] As of 22 February 2006, S/RES/1267(1999) listed 492 designated persons and entities, of which 143 (about one third) are persons or entities belonging to or associated with the Taliban.

247. A de-listing request must be made by the blocked person and addressed to the Director of OFAC. If upon review it is established that there is no longer a sufficient basis for the designation or it is demonstrated that the circumstances resulting in the designation no longer exist, OFAC proposes removal. The U.S. government then takes appropriate administrative actions, including removing the person as an SDGT from the SDN List on the OFAC website, and, if appropriate, working with the UN to remove the person from the UN's 1267 Consolidated List. Pursuant to these procedures, OFAC has de-listed 10 individuals and entities initially designated under EO 13224.

248. Furthermore, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) provides that a FTO may file a petition for revocation two years after its designation date or two years after the determination date on its most recent petition for revocation. Finally, the Secretary of State may at any time revoke a designation upon a finding that the circumstances forming the basis for the designation have changed in such a manner as to warrant revocation, or that the national security of the United States warrants a revocation. A designation may also be revoked by an Act of Congress, or set aside by a Court order.

249. Although there is an administrative procedure for seeking de-listing, there is always the possibility to challenge SDGT designations and other OFAC decisions in court. Furthermore by law an organization designated as an FTO may seek judicial review of the designation in the United States Court of Appeals for the District of Columbia Circuit not later than 30 days after the designation is published in the Federal Register.

250. Legal challenge of the *ex parte* designation procedure as "undue process" has already been rejected by the Courts. Several other approaches have been used, such as seeking a preliminary injunction or arguing violation of the APA on the grounds that the decisions are arbitrary and capricious, and an abuse of discretion or otherwise not in accordance with the law. Other challenges were based on an alleged violation of constitutional protections such as the First Amendment right to free speech and association or the Fifth Amendment right not to be deprived of property without due process of law. The courts have rejected all these challenges. The USA PATRIOT Act, enacted in October 2001, has enhanced OFAC's ability to implement sanctions and to co-ordinate with other agencies by clarifying OFAC's authority to block assets of suspect entities prior to a formal designation in "aid of an investigation" to prevent the disappearance or deterioration of assets.

251. Similarly, in cases a party to a transaction believes funds have been blocked due to mistaken identity, that party may seek to have funds unblocked through administrative procedures published in the CFR. Any person who is a party to the transaction that resulted in blocked funds pursuant to OFAC regulations may address OFAC for the release of funds. In the event the Director of OFAC determines that the funds should be released, OFAC will direct the financial institution to return the funds to the appropriate party. OFAC may also issue letters to innocent parties that share a similar name to that of a designated party informing any concerned party of the distinction between the innocent bearer party and a designated party sharing a similar name (31 CFR 501.806).

252. Requests to unfreeze assets blocked in the context of an OFAC designation can also be brought before a U.S. Federal Court. The Civil Division of the DOJ is charged with the responsibility for litigating such cases.

Authorizing access to frozen funds or other assets

253. There are procedures in place for authorizing access to funds or other assets that were frozen pursuant to either S/RES/1267(1999) or S/RES/1373(2001) and that have been determined to be necessary for the payment of certain types of expenses. OFAC can license or authorize access to blocked property or accounts on a case-by-case basis to ameliorate the effects of the designation. It may permit access by a designated person to his assets to the extent necessary for basic or even extraordinary expenses OFAC can also authorize the transfer into the U.S. of non-blocked assets, which prevents the assets from being blocked upon receipt by a U.S. person. OFAC, across its 30 sanctions programs,

processes approximately 42,000 specific license applications and requests for interpretive rulings each year, and receives approximately 15,000 telephone calls involving license queries each year.

Seizure and Confiscation

254. In contexts other than a designation pursuant to S/RES/1267(1999) and S/RES/1373(2001), funds or other assets provided or used in violation of 18 USC 2339A, 2339B and 2339C are subject to seizure and forfeiture when:

(a) involved in a transaction or attempted transaction in violation of 18 USC 1956-1957 (laundering of terrorist related assets);

(b) they represent the proceeds of a 18 USC 2339A or 2339B offense (supporting and resourcing terrorists or terrorist organizations); or

(c) they represent funds involved in a violation of section 2339C (financing of terrorism) (see also section 2.2 above).

255. More generally, 18 USC 981(a)(1)(G) and 18 USC 2331 make subject to forfeiture—all foreign or domestic assets

(a) of any individual, entity or organization engaged in planning or perpetrating any act of domestic terrorism or international terrorism and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization, acquired or maintained by any person with the intent and for the purpose of supporting, planning, conducting, or concealing an act of domestic terrorism or international terrorism, or

(b) derived from, involved in, or used or intended to be used to commit any act of domestic terrorism or international terrorism.

256. Until recently this provision only applied when U.S. interests were implicated. With the enactment of the USA PATRIOT Improvements and Reauthorization Act of 2006 of 9 March 2006, however, 18 USC 981(a)(1)(G) was expanded to include individuals, entities and organizations that plan or perpetrate acts of international terrorism against international organizations (such as the UN) or foreign governments.

257. As with all other forfeitures covered by 18 USC 981, the rights of innocent third parties are protected (see section 2.3 above).

Compliance

258. Measures to ensure compliance with SR III are based on the IEEPA and the AEDPA that place the burden for effecting compliance on the affected financial institution or other affected entity. Both statutes impose civil money penalties on financial institutions that fail to comply with its obligations. Moreover, a knowing violation of the obligation by the financial institution or entity could lead to a criminal charge of providing material support or resources to a designated foreign terrorist organization or of engaging in a transaction with a blocked person or entity [18 USC 2339B(a), and 50 USC 1705].

259. For the regulated financial sector compliance monitoring is mainly the responsibility of the regulators and supervisors, such as the U.S. federal bank regulatory agencies — the Federal Reserve, the FDIC, the NCUA, the OCC and the OTS. The regulators review OFAC compliance policies and procedures under their general safety and soundness supervisory authority. They generally focus their attention on the quality of the compliance program in place, commensurate with the risk profile of the supervised entity. Occasionally examiners proceed to case sampling on the basis of the OFAC list.

260. OFAC also works with other U.S. government agencies to enforce its regulations, especially in other high-risk industries such as export-import and travel, and receives operational support from law

enforcement agencies. Treasury also conducts outreach to educate and inform the financial sector, high risk industries and the general public about the economic and financial sanction programs administered by OFAC.

261. OFAC's enforcement process relies heavily on the examination of the blocked transaction reports that are reviewed and maintained for investigative and compliance purposes. Relevant information is shared with law enforcement agencies. Serious indications of inadequate compliance, also from other sources (such as law enforcement and regulators) are investigated by sending an administrative subpoena to the suspected violator requesting an explanation from the suspected violator. OFAC may refer the case to ICE, the FBI, IRS-CI or another law enforcement agency for further investigation. If OFAC believes a U.S. person has or may have violated the law, one of several possible actions may result: the issuance of a cease-and-desist order, warning letter, or cautionary letter; the assessment or settlement of a civil penalty; or the suspension or even revocation of a specific license. A willful or egregious violation may lead to more severe action such as a referral to the DOJ for criminal charges.

262. OFAC has civil monetary penalty authority. The office retains discretion in determining whether to administer a civil penalty and if so, the appropriate amount. Penalties range from USD 50,000 to USD 1.075 million. Since 1993, OFAC has collected nearly USD 30 million in civil penalties for sanctions violations and has processed more than 8,000 matters across all its sanctions programs. OFAC collected USD 2,925 in penalties for terrorism violations in 2003, and none in 2004 and 2005.

263. Compliance is also enforced through criminal sanctions in cases where persons willfully engage in unlicensed transactions involving blocked property or a designated person or entity. Criminal investigations of IEEPA violations are accomplished by federal law enforcement agencies, principally the FBI in terrorist financing cases. Responsibility for criminal prosecution rests with the DOJ, often represented by the U.S. Attorney for the respective federal district. OFAC may provide technical advice and assistance during the criminal investigation and prosecution phase.

264. Nevertheless, the effectiveness of the compliance measures is not consistent across all sectors. As indicated above, knowledge among the financial sector and, indeed, the regulatory agencies was patchy, particularly within the state-regulated sectors. For instance, a state insurance regulator that the assessment team visited confirmed that it was not checking for compliance with EO 13224.

Additional elements

265. In addition and in support of the above described measures the U.S. has also implemented other recommendations that are set out in the FATF Best Practices Paper for Special Recommendation III, such as:

(a) ***Drafting a packet of identification information for each designation:*** When a determination has been made to proceed with a designation action, the Department of the Treasury and/or the State Department work with the interagency community to produce an unclassified Statement of the Case (SOC). The SOC serves as an unclassified summary of the factual basis for the public announcement of a designation and includes identifier information for use in implementing blocking and freezing actions.

(b) ***Addressing concerns about the use of sensitive information:*** Although the administrative record may contain classified information underlying a designation, effort is made to declassify the information. In most cases, however, there are sensitivities that prevent full disclosure. This may raise an issue in respect of the sharing of information with foreign jurisdictions (see section 6.5.1)

(c) ***Prohibitions against publishing sensitive information:*** The USA PATRIOT Act explicitly authorizes submission of classified information to a court, in camera and *ex parte*, upon a legal challenge to a designation.

(d) ***Consultation with other governments during designation process:*** Countries that are pre-consulted are encouraged and welcomed to contribute additional identifier or factual information they may have available, such as information available in public records that is not readily accessible within the U.S.

(e) ***Pre-notification of pending designations to other governments:*** The U.S. has developed a system for early and rapid pre-notification of pending designations to other jurisdictions, inviting those jurisdictions to join in a designation or freeze funds / other assets simultaneously across jurisdictions. When the U.S. government decides to designate individuals and entities in accordance with S/RES/1373(2001), the State Department, through its embassies and missions, and other U.S. agencies engage their international counterparts on a bilateral basis in order to encourage support for the designation and to facilitate implementation. Background information is shared in the form of an unclassified "statement of case". Some FATF members indicated that they experienced difficulties with their requests for additional information. Although OFAC maintains that they satisfy these queries whenever possible. However, they are bound by the classified status of the data and are totally dependant from their sources for declassification.

(f) ***Guidance for financial institutions:*** OFAC works with the regulators to provide guidance for the development of effective compliance programs. Most recently, OFAC has worked with the federal banking regulators to develop written guidance for banks and their examiners to promote compliance with sanctions administered by OFAC. The FFIEC Examination Manual includes a section on assessing OFAC compliance programs in financial institutions.

(g) ***Sharing information with other jurisdictions:*** OFAC submits requests to FinCEN to work through its bilateral FIU-to-FIU channels and/or through the Egmont Group of FIUs to request and share additional financial intelligence relating to designated parties. FinCEN offers reciprocity for similar requests from foreign FIUs.

(h) ***Integrate, publish and update lists without delay:*** Newly named SDGTs are immediately incorporated into OFAC's SDN List and posted on OFAC's website. In cases involving technical amendments to designations that already appear on the UN 1267 list (i.e. spelling changes, ordering names, or new identifying information —other than new names and "also know as" (aka's), the U.S. accepts this information on its face from a submitting country in relation to the submitting country's own nationals in conjunction with the 1267 Monitoring Team's vetting of the information.

(i) ***Process for responding to inquiries concerning potential identification mismatches:*** When an institution identifies an entity that is an exact match, or has many similarities to a subject listed on the SDN and Blocked Persons List, the institution may contact OFAC by telephone for verification. Unless a transaction involves an exact match, it is recommended that the institution contact OFAC before blocking assets.

Effectiveness of the measures for freezing and confiscating terrorist assets

266. As of 26 March 2006, the U.S. has designated 438 individuals and entities for terrorist and terrorist financing-related activities pursuant to EO 13224. Over 300 of these entities are associated with Usama bin Laden, Al-Qaida or the Taliban, which has provided the basis to propose these names to the UN Al-Qaida and Taliban Sanctions Committee for inclusion on its consolidated list of individuals and entities. The remainder of parties designated under EO 13224 represents terrorist and terrorist financing-related threats independent of those presented by Al-Qaida or the Taliban.

267. The following statistics concerning the number of persons or entities and the amounts of property frozen pursuant to the UN Resolutions relating to terrorist financing were submitted. As of 19 August 2005, the U.S. has frozen/blocked a total of USD 281,372,910 worth of assets as follows:

- 24 Taliban-related individuals/entities totaling USD 264,935,075;
- 258 Al-Qaida-related individuals/entities totaling USD 9,322,159; and

- 21 other terrorist individuals/entities totaling USD 7,115,676

268. Of the USD 281,372,910, USD 12,488,924 remains blocked by OFAC as of 19 August 2005. The USD 264,935,075 blocked under the Taliban program was unblocked upon removal of Taliban control. In addition, other funds were unblocked due to licensing actions, delisting actions, and account maintenance/management fees.

269. As of 19 August 2005, assets seized pursuant to U.S. investigations with possible terrorist links totaled USD 37,314,379.

270. No statistical details were submitted on the number and amount of TF related confiscations.

2.4.2 Recommendations and Comments

271. Overall, the U.S. has built a solid, well-structured system aimed at effectively implementing the UN sanctions under S/RES/1267(1999) and S/RES/1373(2001). The statistics on the frozen terrorist related assets speak for themselves. Indeed, the measures in place correspond to most recommendations set out in the FATF Best Practices Paper for SR III. Combating terrorism in all its facets and targeting particularly the financial aspects obviously being a prime concern in U.S. policy, it has engaged substantive resources to cut off the financial basis from terrorist entities and activities. The OFAC plays a central role in this process. This authority has powerful means, both legal and structural, at its disposal to fulfill its mission and it uses them quite adequately, as the figures show. Although the information supporting the designation process is not always fully accessible to the designated parties, the process is balanced by the possibility for these parties to challenge the designation and defend their rights through legal or administrative means, and by the ability of an independent federal judge to fully review, in camera, the evidence submitted in support of a designation that is challenged in federal court.

272. The implementation by the U.S. of the obligations resulting from S/RES/1267(1999) raises the question if countries can deviate from a formal transposition obligation of the name list into their national preventive system and, if so, to what extent. A strong argument for the U.S. approach is the effectiveness of their system, which is shown abundantly by the figures. Indeed, a literal copying of the list without effective implementation serves no purpose and does not meet the obligations under the UN resolution. Also such a purely formal approach based on incomplete, vague or unreliable identification carries a serious risk of acting counterproductively. On the other hand the obligation under S/RES/1267(1999) to transpose the complete list is quite clear and gives little latitude to the countries for divergent interpretations. In addition, the reliability of the names on the UN list has been improved through successive rounds of corrections and additions of identifiers, year after year. It continues to evolve into a much more accurate and reliable document, so a radical refusal to place all of the Taliban names on the OFAC list does not seem to be wholly justified. Moreover, it deprives the industry of a practical tool that may help them in their evaluation of the situation in respect of EO 13224. Publication of the UN 1267 list through the OFAC list would obviously not be sufficient in itself without accompanying support measures, such as the assistance role that OFAC now fulfills. This being said, the assessment team takes the view that this formal deficiency in transposing the 1267 list is to a large extent counterbalanced by the substantive quality and the undeniable effectiveness of the approach adopted by the U.S. which has been translated in a large amount of frozen assets. Therefore, this deficiency only has a limited impact on the rating.

273. A real challenge for OFAC lies in the effectiveness of the compliance monitoring process. The sheer number of financial institutions and other entities/persons affected by the designations defies even the substantial organizational resources that are meant to ensure full compliance. The system predominantly relies on examination by the regulators and supervisors, but they focus mainly on the quality of the compliance program in place and occasional checking of name samples. In particular, monitoring of the less or non-federally regulated sectors (such as insurance or DNFBPs) is

problematic. OFAC has too limited resources to monitor such a large number of entities (138 employees, of which two dozen are dedicated to monitoring and outreach, to administer all 29 of OFAC's sanctions programs). Of course the system checks itself to a certain extent as somewhere along the line some subjected entity may pick up indications of non-compliance and will report those deficient links in the chain. Overall, further efforts will have to be made to improve compliance monitoring of all targeted entities, particularly the state-regulated sectors and DNFBPs.

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	LC	• Compliance monitoring in non-federally regulated sectors (e.g. insurance, MSBs) is ineffective. • Not all S/RES/1267(1999) designations are transposed in the OFAC list.

2.5 The Financial Intelligence Unit and its functions (R.26)

2.5.1 Description and Analysis

Recommendation 26 (FIU)

274. FinCEN (which was created in 1990) is the financial intelligence unit of the U.S. The USA PATRIOT Act of 2001 re-established FinCEN as a bureau within the Treasury. The authority of the Secretary of the Treasury to administer Title III of the BSA (codified at 31 USC 5311-et. seq. with implementing regulations at 31 CFR Part 103) has been delegated to the Director of FinCEN.

275. The mission of FinCEN is to fulfill the duties and powers assigned to the Director by the USA PATRIOT Act [codified in relevant part at 31 USC 310(b)], support law enforcement efforts, foster interagency and global co-operation against domestic and international financial crimes, and provide U.S. policy makers with strategic analysis of domestic and worldwide trends and patterns (Treasury Order 180-01 dated 26 September 2002). FinCEN works toward those ends through information collection, analysis and sharing, as well as technological assistance and innovative, cost-effective implementation of the BSA and other Treasury authorities that have been assigned to it. FinCEN is considered to be a law enforcement support agency, although it has no criminal investigative or arrest authority. As the sole administrator of the BSA, FinCEN retains a high-degree of operational independence.

276. FinCEN fulfils three main roles. Its role as an FIU is discussed in this section. Its role as a regulator is discussed in section 3 of this report. Finally, its role as an information network is discussed in section 6.1 of this report.

Functions and responsibilities of the FIU

277. FinCEN is responsible for collecting, housing, analyzing and disseminating financial information that is collected under the BSA and other authorities, and which relates to investigations of illicit finance (including money laundering). The duties and powers of FinCEN expressly include "analyz(ing) and disseminat(ing) the available data...to...determine emerging trends and methods in money laundering and other financial crimes" [31 USC 310(b)(2)(C)], among other things, and to gain an increased understanding of methodologies, typologies, geographic patterns of activity and systemic vulnerabilities relating to terrorist financing.

278. FinCEN receives the following types of suspicious transaction reports that must be filed by various types of financial institutions pursuant to the BSA: SAR; SAR by a Money Services Business (SAR-MSB); SAR by Casinos & Card Clubs (SAR-C); and SAR by Securities & Futures Industries (SAR-SF). Beginning in May, 2006, FinCEN will begin receiving SARs from insurance companies, and effective October 2006, FinCEN will begin receiving SARs from mutual funds.

279. FinCEN also receives the following other types of reports: CTRs; CTR by a Casino (CTR-C); CTR by a Casino-Nevada; Foreign Bank Account Report (FBAR); CTR Filing Exemption Form (Designation of Exempt Persons); Report of International Transportation of Currency or Monetary Instruments (CMIR); Report of Cash Payments over USD 10,000 Received in a Trade or Business (Form 8300); and Registration of Money Services Business.

280. In general, SARs are filed with FinCEN (electronically or in paper form) within 30 to 60 days of the suspicious activity being detected by the reporting entity, which is a long period of time. SARs may also be reported through a telephone hotline; however, in such cases an electronic or paper SAR must still be filed. Only about 30% of the reports are received electronically; approximately 70% are filed in paper form. Pursuant to an agreement with FinCEN, the IRS is responsible for entering reports into the database. The agreement stipulates that all reports must be entered in the database within 10 days of being received by the Detroit computing center. FinCEN reports that, over the years, its checks have confirmed that this obligation is mostly being met.

281. Given the very large number of reports being received by FinCEN annually (over 14 million in 2004, including over 600,000 SARs), FinCEN is not able to perform a comprehensive analysis of each SAR, but instead devotes its analytical resources to those SARs considered most valuable to law enforcement, in accordance with the following parameters.

282. At the strategic level, FinCEN assigns analysts to study BSA data and all other available information for trends and patterns based on the needs of FinCEN's law enforcement, regulatory, and policy customers. Such analysis includes identifying geographic and systemic "hot spots," identifying new and emerging phenomena, and providing detailed lead information to law enforcement and the intelligence community.

283. FinCEN also provides operational analysis and case support to a broad range of federal, state and local law enforcement agencies, and international law enforcement agencies in ongoing CFT investigations. FinCEN refers proactive lead information, case studies, and analysis to U.S. and international law enforcement agencies. This analysis is increasingly geared toward complex cases in which law enforcement agencies need assistance in identifying multiple subjects, mapping criminal financial activity over large geographic areas and establishing international linkages that are not apparent in initial investigative activity. Through the use of sophisticated technology and information extracted from the numerous data sources to which FinCEN has access, intelligence analysts link together various aspects of a case and add value to what is already known by investigators. FinCEN's analysts also develop threat assessments, industry reports, and technical guides to financial transaction mechanisms.

284. The single most important stated operational and tactical priority for FinCEN is providing counter-terrorism support to law enforcement and the intelligence community. To emphasize the importance of this work, FinCEN has implemented a comprehensive counter-terrorism strategy that draws resources and expertise from FinCEN's analytical support to law enforcement, regulatory tools and international networking capabilities. Elements of this strategy include reviewing, for both tactical and strategic value, virtually all SARs filed where the filer has indicated suspected terrorism financing activity. After reviewing those terrorist financing-related SARs, FinCEN performs additional, more complex analysis on those SARs determined by FinCEN through its review as most likely to be indicative of terrorism financing. The products of these reviews are intelligence reports on individuals and businesses potentially providing financial support to terrorist groups or objectives. FinCEN allocates considerable operational resources in support of law enforcement and intelligence counter-terrorism efforts.

285. FinCEN has adopted an alternative operational approach in its work in relation to anti-money laundering cases. FinCEN continues to develop (from the BSA information in its database) proactive lead information, and to forward these cases to the appropriate law enforcement agencies. FinCEN reports that recent feedback from customers of FinCEN's proactive products on money laundering and terrorism shows a high level of satisfaction. However, FinCEN reports are not always welcomed by

law enforcement, some law enforcement agencies hold the position that they are more able to make their own analysis of BSA data and that their analysis are more in concert with their ongoing investigations because they are in a better position to judge the relevant information. For instance, during the on-site visit, the assessment team was advised that not all local FBI agents use the FinCEN database for their work, but rather pursue more traditional methods of information gathering.

286. FinCEN indicated that it understands the law enforcement position with regards to straight-forward investigations which can be approached in a more linear fashion. To respond to this view, FinCEN has enhanced its role as a network by providing broader access to its databases by law enforcement agencies working both on and off of FinCEN's premises. By enhancing its role as a network, FinCEN plays an important role in facilitating domestic coordination and cooperation (as is discussed in more detail in section 6.1 of this report). Having given direct access to its database, there is a concern that FinCEN does not receive adequate feedback from the authorized agencies. This could ultimately impede FinCEN's analytical functions and its own ability to give guidance regarding the manner of reporting and to develop its expertise about ML/FT methods, trends and typologies.

287. It is therefore essential that FinCEN maintains its key role within the AML/CTF chain and does not become a FIU with solely a database to be explored by others. The added value of FinCEN is its prominent role within the AML/CTF chain and the ability to make broader linkages and bring a more 'macro' perspective to an investigation thanks to the massive amount of domestic and international data stored in its databases. Moreover, FinCEN's expertise in trends and typologies (which have been developed through its strategic analysis) can further facilitate an investigation.

288. Although FinCEN's stated mission and operational priority has shifted towards supporting the law enforcement and the intelligence communities as far as counter terrorism is concerned, the methods used by organized crime to launder money do not differ substantially from the methods used by terrorist financiers. Consequently, a similar operational approach in relation to SARs which may be related to money laundering would be appropriate. One would not like to see that experience gained at other agencies when analyzing transaction information gets lost.

289. Given the large number of SARs received annually by FinCEN, appropriately sophisticated filters are needed to facilitate and target this work. It would be worthwhile for FinCEN to work closely together with law enforcement, to know in what kind of e.g. transaction-information they are interested, what are the crime areas of interest, what kind of analysis are needed, etc.. Additionally, although it will be a challenge, it is important that FinCEN and the law enforcement agencies themselves work to change perceptions in the law enforcement community and promote FinCEN's strategic and operational products as having added value in both expertise and scope of information. During the development of new systems or products within FinCEN, such work should include FinCEN devoting sufficient time to match the new products with the needs of its customers. At the case level, such work should include FinCEN receiving specific feedback from the law enforcement agencies on its products, so that it can better use its database, develop appropriate products for law enforcement and provide adequate feedback to reporting entities.

Access to information

290. The information that FinCEN collects under the BSA and the ability to link this data with a variety of law enforcement and commercial databases makes FinCEN one of the largest repositories of information available to law enforcement in the country. FinCEN's information sources fall into three categories, all of which can be accessed by FinCEN in a timely manner: (1) direct access to its financial database; (2) direct access to commercial databases; and (3) indirect access to law enforcement data.

291. The financial database is comprised of the reports that must be filed under the BSA, such as data on large currency transactions conducted at financial institutions or casinos, suspicious transactions and international movements of currency or negotiable monetary instruments. The scope

of information contained in this database will expand as the obligation to report SARs is extended to additional sectors that FinCEN/Treasury determines should be subject to these requirements.

292. Commercial databases contain information from commercially available sources such as state corporation records, property records, and people locator records, as well as professional licenses and vehicle registrations.

293. Finally, FinCEN is able to access (indirectly) various law enforcement databases through written agreements with each agency. Additionally, the fact that law enforcement liaisons work within FinCEN provides–within the limits of the existing laws and regulations—the possibility for FinCEN to explore the data of these agencies in a timely fashion. The allocation of FinCEN liaisons to the HIFCAs also presents opportunities for information exchange with law enforcement agencies.

294. FinCEN also has the authority to go to reporting parties for additional information (such as for original supporting documentation for filing a suspicious transaction report that may be needed to properly undertake its functions) directly or through law enforcement. The regulations governing the filing of SARs enable FinCEN and appropriate law enforcement and financial institution supervisory agencies to request all supporting documentation related to the filing of the SAR [31 CFR 103.18(d) and (e)(affecting banks); 31 CFR 103.19(d) and (e) (affecting brokers or dealers in securities); 31 CFR 103.20(c) and (d) (affecting MSBs); and 31 CFR 103.21(d) and (e) (affecting casinos) and 103.16(e), governing insurance company SARs, as of 2 May 2006]. Under these provisions, supporting documentation is "deemed" to have been filed with the SAR and is therefore available to FinCEN, law enforcement or supervisory agencies, without a subpoena or court order.

Dissemination of information

295. FinCEN disseminates financial information to domestic authorities for investigation in a number of ways. In 2001, FinCEN put in operation a hotline encouraging financial institutions to report suspicious transactions that may relate to terrorist activity by calling FinCEN's HOTLINE which is operational 7 days a week, 24 hours a day. The purpose of the HOTLINE is to facilitate the immediate transmittal of this information to law enforcement. This HOTLINE provides law enforcement and other authorized recipients of SAR information with details of the suspicious activity in an expedited fashion. Using the HOTLINE is voluntary and is not a substitute for an institution's responsibility to file a SAR in accordance with applicable regulations.

296. Additionally, FinCEN refers intelligence reports (that it develops based on its review of SARs which identify terrorist financing as the alleged violation) to appropriate law enforcement and intelligence agencies. FinCEN also shares the strategic and financial information and resources with its federal law enforcement partners and provides analytical support to complex investigations of all types. As well, in its role as a network, FinCEN disseminates information to law enforcement agencies via the Gateway, Platform and, in the future, through BSA Direct programs, as well as through the processes implemented pursuant to section 314(a) of the USA PATRIOT Act. For a more detailed description of these programs, see section 6.1 of this report. FinCEN publishes (in "The SAR Activity Review-Trends, Tips & Issues") statistics relating to the section 314(a) process, broken down by the number of new accounts and transactions identified by industry responses to 314(a) requests, as well as the number of subpoenas, search warrants, arrests, and indictments resulting from 314(a) information.

Secure protection of information

297. In its role as the administrator of the BSA, FinCEN is the central point of dissemination of BSA information. FinCEN's authority to share BSA report information is set forth in 31 USC 5319 and 31 CFR 103.53. Such sharing must be consistent with one or more of the purposes contained in 31 USC 5311 (including the support of a law enforcement investigation or proceeding). The manner in which BSA report information is shared (e.g. on an individual subject query basis or in a bulk download to facilitate data mining) is left to the discretion of FinCEN. However, by sharing the

BSA reports with law enforcement (or "so many agencies"), FinCEN runs the risk of leakage of this valuable and (sometimes) sensitive information. In June 2004, FinCEN issued "Re-dissemination Guidelines for Bank Secrecy Act Information" which elaborates these principles.

298. Additionally, FinCEN imposes strict procedural safeguards on all reports filed under the BSA, including reports of the cross-border transportation of monetary instruments, and CTRs. All persons with electronic access to the computerized database in which such reports are maintained must have successfully completed a background investigation. Moreover, all state and local agency personnel, and all federal personnel outside the Treasury with electronic access must have successfully completed appropriate training. FinCEN employs passwords and access controls, and all non-Treasury agencies are required to enter into signed agreements outlining usage and dissemination rules before electronic access is authorized.

299. Procedural and physical safeguards include the logging of all queries and periodic review of such query logs, compartmentalization of information to restrict access to authorized personnel, physical protection of sensitive hard copy documents and magnetic tapes, encryption of electronic communications, intruder alarms and other security devices, and 24-hour building guards. FinCEN does not provide BSA records to members of the general public.

300. Reports and records of reports filed under the BSA are exempt from access under the Freedom of Information Act (31 USC 5319). In addition, FinCEN has exempted the system of records in which BSA reports are maintained from the access and amendment provisions of the Privacy Act [31 CFR 1.36(c), 1.36(g), and 31 CFR Part 1, Subpart C, Appendix N]. FinCEN also authorizes Gateway users, trains them, and monitors their use to ensure that the data, which are considered law enforcement sensitive, are properly used, disseminated, and kept secure.

301. In general, a federal, state, or local government agency may not re-disseminate BSA information to another government agency or to any other person without first obtaining FinCEN's approval (which may be obtained on an expedited basis in the extremely rare case where the information is required on an urgent basis). However, there are a few exceptions.

302. For instance, a federal, state or local government agency may disclose BSA information to another federal, state or local government agency that is working on the same (or related) investigation or prosecution. Likewise, federal, state or local government agencies may also disclose BSA information to each other, provided that they are members of the same joint task force and the sharing of the information is in furtherance of the joint task force's common objectives. In both cases, the information sharing is subject to a number of conditions, including: (1) the receiving agency must sign in advance a written acknowledgement which reflects its understanding that no further dissemination of the information may be made without the prior approval of FinCEN; (2) each BSA Report or item of BSA information being shared must contain the warning statement pertaining to its use and further re-dissemination; (3) copies of the acknowledgment form must be maintained by the federal, state or local government agency; and (4) in the case of joint task forces, a record of each disclosure of BSA information to task force participants shall be kept. Such records must be provided to FinCEN upon its request. FinCEN made 48 such requests in fiscal year 2004. See below for a further discussion of this issue.

303. In very limited circumstances, a federal prosecutor may disclose BSA information in the course of a judicial proceeding without first obtaining the approval of FinCEN. However, such disclosures (particularly of a SAR) should only be made when "necessary to fulfill the official duties of such officer or employee" [31 USC 5318(g)(2)]. A government official may not disclose a SAR to the subject of such report except in cases where a prosecutor believes that disclosure of the SAR is compelled by constitutional, statutory or regulatory authority. FinCEN and the DOJ have issued guidance to federal prosecutors on the limited circumstances in which it is appropriate to disclose SARs in a judicial proceeding. Disclosure of a SAR or the information in a SAR that might reveal its existence, should be distinguished from disclosure of records constituting the transactions discussed in

a SAR, such as a wire transfer record, which can be treated as ordinary evidence. Because the underlying documents prove the transaction, and the SAR does not, it should rarely be necessary to use a SAR in the prosecution's case.

304. Additionally, FinCEN and the Federal Banking Agencies each have a concurrent authority to re-disseminate a SAR (including any information that might reveal its existence) that is filed with FinCEN by a bank or banking organization, under rules issued under the authority of 31 USC and the SAR rules issued by each of the Federal Banking Agencies [31 USC 5318(g)(2)]. Such disclosure authority must be exercised in accordance with other federal law or regulation (e.g. consistent with BSA purposes, Privacy Act routine use, etc.).

305. FinCEN also has safeguards in place to ensure that the information which it disseminates in accordance with its network functions is only distributed in appropriate cases. For instance, requests made pursuant to section 314(a) of the USA PATRIOT Act are made via a secure website. Additionally, FinCEN requires federal law enforcement to provide assurances that the request has been subject to appropriate scrutiny at the agency level and that the matter under investigation satisfies FinCEN's standards for processing a formal Section 314(a) inquiry. This includes submitting a form certifying that the investigation is based upon credible evidence of terrorist financing or significant money laundering.

Guidance concerning the obligation to report

306. FinCEN provides various types of guidance and general feedback to domestic financial institutions and DNFBPs regarding the detection and reporting of suspicious activity. Much of this guidance and feedback is posted on FinCEN's website. FinCEN's guidance materials include the following:

(a) letter rulings explaining how SAR requirements apply to specific facts and circumstances;

(b) answers to frequently asked questions about SAR requirements;

(c) a document entitled "Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative";

(d) a document entitled "Suspicious Activity Reporting Guidance for Casinos"; and

(e) SAR Bulletins on specific issues, like automatic teller machines, phone cards, indicators of the financing of terrorism, and SARs filed by casinos;

(f) the annual "SAR Activity Review—Trends, Tips & Issues and its companion publication "SARs by the Numbers". These publications are discussed in more detail in section 3.7 below.

307. However, financial institutions indicated that they also prefer case-specific feedback.

Periodic reports

308. FinCEN produces reference materials that provide law enforcement and intelligence agencies with a better understanding of financial transactions. These reference manuals are developed in close consultation with representatives of the relevant industries and assist investigative officials in explaining the intricate operations of financial systems, record retrieval procedures, and audit trail identification and analysis.

309. In addition, in 2004 FinCEN published its first Annual Report which highlights the operations of FinCEN's various units.

Egmont Group

310. FinCEN is one of the founding members of the Egmont Group. FinCEN's Deputy Director serves as the Chairman of the Egmont Committee and FinCEN is represented on all five of the Egmont working groups. On behalf of the Egmont Group, FinCEN maintains the Egmont Secure

Web, which permits members of the group to communicate with one another via secure email about ongoing case investigations, requests for financial information, posting and accessing information regarding trends, analytical tools, and technological developments.

311. As a member of the Egmont Group of FIUs, FinCEN representatives were actively involved in helping to draft and revise the Statement of Purpose and Principles of Information Exchange between Financial Intelligence Units for Money Laundering Cases. FinCEN's memoranda of understanding (MOUs) are all based on Egmont's Principles of Information Exchange. FinCEN handles the information/requests of foreign FIUs with great care. With the exception of terrorism-related requests, information contained in requests from foreign FIUs is shared with law enforcement only if the requesting FIU grants authorization for networking. FinCEN's ability to cooperate with foreign FIUs is discussed in more detail in section 6.5 of this report. The fact that terrorism-related information in requests from foreign FIUs is shared with law enforcement without, as is mentioned by the U.S. authorities, the foreign FIU's authorization for networking is—though it is a highly sensitive issue—not in line with the international principles of information exchange (among others, the Egmont Principles).

Effectiveness of the FIU

312. FinCEN receives over 14 million reports (including about 600,000 SARs) annually, of which only about 11% of the total number of reports (and 30% of SARs) are filed electronically. The U.S. authorities advised that SARs are entered into the database no later than 10 days after being received. However, increasing the amount of electronic filing would be much more efficient and timely—particularly given the importance of making SAR information available to law enforcement as quickly as possible. This would also ensure that FinCEN becomes more independent of the administrative process in Detroit. The chart below shows the number of reports received by FinCEN in 2003 and 2004.

TYPE OF REPORT	FY 2003	FY 2004
Suspicious Activity Reports (SARs)	413,052	663,655
Currency Transaction Reports (CTRs)	13,341,699	13,674,114
Reports of Foreign Bank and Financial Accounts	199,738	218,667
Reports for Cash Payments over USD 10,000 received in a trade or business (Form 8300)	129,824	151,998
TOTALS	14,084,313	14,708,434

313. Since FinCEN receives such a huge amount of reports, through a mixture of a rule- and risk-based system, one should be constantly aware of whether all the CTRs have the same added value (periodic review of CTR obligations could be worthwhile). The suggestion to invest more in a risk-based approach (without neglecting the need for rule-based reporting) is that reporting institutions are better able to judge whether a transaction is unusual/suspicious. It is also a FIUs (FinCEN) role to support the reporting institution on this issue, by giving advice to them based on their gained experience either by working together with law enforcement and/or foreign FIUs.

314. According to FinCEN, the quality of SARs varied substantially from institution to institution. In order to improve the quality of filings by reporting institutions FinCEN should improve its feedback and guidance to reporting institutions.

315. Over the five-year period 2000 through 2004, FinCEN conducted research on a yearly average of 29,246 individuals or businesses, each of which would have been checked for SAR filing histories. On average another 6,500 individuals or businesses were checked for SAR filing histories by federal law enforcement agencies using FinCEN facilities and another 47,000 checks were conducted by state and local government law enforcement agencies. All of the state and local government law enforcement agency checks were conducted for SAR filing histories. SAR analysis was conducted on 314 strategic projects causing the analysis of thousands of SARs. No exact count is maintained on this analysis. Additionally, FinCEN's Annual Report for 2004 provides the following indicia of its performance.

Analytic products produced by FinCEN	FY 2003	FY 2004
Analytic products completed by FinCEN employees and contractors to support law enforcement investigations	4,403	2,913
Subjects researched by FinCEN employees and contractors	30,429	19,304
Analytical products to support intelligence community	175	79
Proactive analysis initiated by FinCEN and referred to law enforcement	249	266
Analytical products related to geographic threat assessments, money laundering, illicit financing methodologies and/or analysis of BSA compliance patterns	79	56
Law enforcement cases supported through information exchanges with foreign jurisdictions	724	844

316. Dissemination of SARs is tracked and over the five-year period 2000-2004 a total of 3,417 SARs were disseminated to foreign FIUs and 237,095 to domestic agencies. FinCEN disseminates SARs to domestic law enforcement (state and federal) and regulatory clients and foreign requesters routinely and records this data in an in-house database. Statistics are not gathered on the dissemination of CTRs and CMIRs. SAR dissemination statistics for 2000 through 2004 are reflected below.

Suspicious Activity Reports Disseminated from 2000-2004				
Year	To Foreign Requestors		To Domestic Requestors	
	# Cases	# SARs	# Cases	# SARs
2000	31	1,718	677	7,423
2001	50	172	735	5,335
2002	77	674	1,177	20,658
2003	132	957	1,316	105,835
2004	169	1,512	1,156	98,844

2.5.2 Recommendations and Comments

317. Overall, FinCEN substantially meets the requirements of Recommendation 26. However, there are a few issues that should be addressed to improve its effectiveness and strengthen its role in the AML/CTF chain. First, FinCEN should invest in a faster and more efficient reporting system with a preference to: (1) mandatory e-filing for all reporting institutions, and (2) the use of a single form for all reporting institutions.

318. The position of FinCEN, within the AML/CTF chain, could be influenced by BSA-direct, if the access and feedback it is not well regulated.

319. FinCEN should improve its guidance and feedback to reporting entities with a view to improving the quality of reports filed by these entities. FinCEN should also ensure that its information and guidance for reporting entities is combined and/or coordinated with the law enforcement agencies and regulators that issue similar or related material.

320. FinCEN should focus on promoting the added-value of its analytical products to law enforcement. In turn, the law enforcement agencies should work at the operational level to change their perceptions concerning the value of FinCEN's products (i.e. by promoting within their agencies a broader use of FinCEN's ability to produce operational and/or strategic analysis).

321. Since the U.S. shares terrorism-related information in requests from foreign FIUs with law enforcement in the U.S. without the authorization of the foreign FIU, it does not act in accordance with international principles of information exchange between FIUs that were established by the Egmont Group. The US authorities are advised to act in this matter with caution and only on the basis of mutual agreement between the concerning FIUs.

2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	LC	• The effectiveness of FinCEN, is impeded by: - perceptions concerning the value of its products and the risk that over-emphasis on FinCEN's network function will weaken its place in the AML/CFT chain; - the handling of the huge amount of 14 million reports of which 70% are still filed in a paper format; - the fact that SAR filing is only done in 30-60 days after detection; and - insufficient adequate/timely feedback to reporting institutions. • Since terrorism-related information in requests from foreign FIUs is shared with law enforcement—for networking—without the prior authorization of the foreign FIU, the U.S. does not act in accordance with international principles of information exchange established by the Egmont Group.

2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offenses, and for confiscation and freezing (R.27 & 28)

2.6.1 Description and Analysis

Recommendation 27 (Law enforcement and prosecution authorities)

Designated law enforcement authorities

322. The U.S. Constitution places responsibility for the investigation and prosecution of federal crimes in the executive branch. Investigatory jurisdiction for the crime of money laundering rests by statute with the Treasury, the DOJ, DHS, and the Postal Service.

323. Department of Justice (DOJ): The DOJ is the central authority for the investigation and prosecution of federal laws in the U.S., including the federal money laundering and terrorist financing offenses. The vast majority of federal criminal prosecutions are handled by the U.S. Attorney's Office in the district where the offense occurred. Money laundering and terrorist financing cases, however, routinely raise unique problems, cross judicial districts, or require particular expertise. Therefore, if the U.S. Attorney's Office does not have the expertise or resources to handle a complicated money laundering or financing terrorism case, the matter is referred to the DOJ headquarters in Washington, D.C., where specialized sections investigate and, if appropriate, prosecute the matter.

324. Federal Bureau of Investigation (FBI): Primary investigative responsibility for the investigation of terrorism and terrorist financing rests with the FBI-led multi agency JTTF. The FBI has specialized units located at their Headquarters in Washington DC for investigating terrorist financing. Additionally, the FBI promotes the investigation and prosecution of money laundering across all investigative programs in which it participates. To do this, the FBI utilizes a two pronged investigative approach. Prong one targets the underlying criminal activity, while prong two follows the money to discover the financial infrastructure of the criminal or terrorist organization.

325. Drug Enforcement Administration Office of Financial Operations (FO): The FO is the primary office responsible for the monitoring of money laundering/financial investigations within DEA. It provides the field with guidance on how to best utilize approved money laundering operations and plans initiatives to include the evaluation, auditing, and monitoring of all financial investigations and approved money laundering operations. The FO provides guidance, assistance and coordination for the implementation of specialized money laundering groups in DEA's 21 domestic field divisions. The FO also assists the Sensitive Undercover Operations Unit with on-site reviews to ensure compliance with manual and policy requirements. FO also provides oversight, coordination and support to each of DEA's Sensitive Activity Review Committee-approved proactive money laundering operations and to the priority target investigations under its supervision. Additionally, FO provides

the majority of all of DEA's money laundering/financial investigations training. The following chart shows investigative statistics for the FO for the fiscal years 2003 to 2005.

YEAR	INVESTIGATIONS	ARRESTS
2003	236	76
2004	253	112
2005	319	156

326. Department of Homeland Security, Immigration and Customs Enforcement (ICE): ICE is responsible for deterring, interdicting, and investigating threats arising from the movement of people and goods into and out of the U.S. This includes investigating bulk cash smuggling, drug smuggling, alien trafficking and commercial fraud. ICE targets the financial component of all investigations within its areas of jurisdiction. ICE has made it a priority to target the financial component to all investigations of criminal activity within its areas of jurisdiction, including narcotics smuggling, alien trafficking and commercial fraud. The ICE Financial and Trade Investigations Division (FTID) applies a systems-based approach to "follow the money" (i.e. identify, disrupt and dismantle organizations that potentially serve as sources of terrorists funding). The following chart shows investigative statistics for ICE for the fiscal years 2003 to 2005.

YEAR	Money laundering offense (s.1956)			Money laundering offense (s.1957)		
	Arrests	Indictments	Convictions	Arrests	Indictments	Convictions
2003	260	274	204	28	39	11
2004	312	335	183	67	56	38
2005	228	170	100	20	28	10

327. Department of Homeland Security, Customs and Border Protection (CBP): The CBP was created with the consolidation of legacy U.S. Customs inspection functions, the Border Patrol and the inspection functions of the Immigration and Naturalization Service and the Agriculture and Plant Health Inspection Service. The role of CBP is to control and protect the nation's borders, at and between the official points of entry.

328. Internal Revenue Service Criminal Investigation (IRS-CI): The IRS-CI (which is part of the Treasury) has primary investigative jurisdiction for money laundering crimes involving banks and other financial institutions and for currency reporting violations under Titles 31 (the BSA) and 26 (the Tax Code). IRS-CI also has joint investigative jurisdiction of money laundering violations and asset forfeiture provisions contained in the criminal code of Title 18. This authority is often shared between IRS-CI and the federal law enforcement agency with the investigative authority over the predicate crime, if such crime is outside the investigative jurisdiction of IRS-CI. Finally, IRS-CI is involved with terrorist financing investigations as an active member of the JTTFs. IRS-CI has formed at each of its field offices SAR Review Teams with other federal law enforcement personnel to review all SARs filed in the U.S. for possible money laundering and terrorist financing activity. For the past five years, IRS-CI special agents have investigated about 1,600 money laundering investigations each year of which 86% resulted in recommendations for prosecution. Eighty-nine percent of the cases that were forwarded for prosecution resulted in a plea agreement (information) or an indictment.

329. Internal Revenue Service Lead Developmental Centers (LDC): Since the last mutual evaluation, the IRS-CI has implemented specialized centers—the LDC—to develop cases for investigations. In the U.S. context, it is very difficult for law authorities to obtain valuable tax information. The analytical work of the LDC involves searching for the same information (i.e. the information that is reported on a tax form, for instance) in a publicly available source (such as a company or property registry) and then bringing all of that publicly available information together (so-called "parallel construction" techniques). The package of publicly available information can then be made available to law enforcement agencies. The LDC in Garden City, New York (started in

January 2003) is devoted solely to identifying terrorist financing investigations. Since the Garden City LDC began operations, it has received approximately 1,300 leads to evaluate. It has completed research of 531 leads (involving 1,161 targets and associates), of which 15 referrals were sent to the field for further investigation. In addition, to researching leads, the Garden City LDC initiated the Individual Tax Identification Number (ITIN) Project in May 2005. Under this project all requests for ITINs made to the IRS are matched against the OFAC's SDN list to identify any suspected terrorists making this request. Since, May 2005, 4,477 ITIN requests have been received, of which 761 applications have been researched due to an apparent match to the OFAC list. This work has resulted in two probable matches to the OFAC SDN list, both of which are being investigated further. The LDC in Tampa, Florida (started in October 2004) focuses on money laundering investigations and works closely with the SAR Review Teams. Since it began operations, the Tampa LDC has evaluated 470 leads for possible money laundering violations. Twenty of these leads were developed through its own proactive data mining.

330. U.S. Postal Service: Title 18 USC 3061, cites the investigative powers of Postal Service personnel and grants investigative authority to the Postal Inspection Service. Where appropriate, the Postal Service is able to use this power in the context of money laundering or terrorist financing investigations. In particular, U.S. postal inspectors work with JTTFs across the country to investigate domestic and international terrorism.

Waiver or postponement of arrest or seizure

331. There are no legislative or regulatory provisions in place allowing for or regulating the use of the technique of postponing or waiving the arrest of suspects. However, in practice, during the course of long term financial investigations or undercover operations, in many cases, arrests will be deferred for substantial periods of time until sufficient evidence has been obtained to prosecute the full extent of the unlawful scheme and all of the significant participants. Once a suspect is arrested, he or she has a right to a finding of probable cause, to a speedy trial, and to the disclosure of the government's evidence against him. Therefore, unless exigent circumstances exist, such as the possibility of harm to victims or the flight of the defendant, the government is usually best served by making arrests according to its own timetable as determined by the coordinated decisions of the prosecutor and the investigators.

Additional elements

332. During the onsite visit, it was clear that law enforcement agencies are of the opinion that all the measures are in place that provide law enforcement or prosecution authorities with an adequate legal basis to use of a wide range of special investigative techniques when conducting ML/FT investigations. For instance, each law enforcement agency has guidelines that govern controlled deliveries of contraband, such as drugs or weapons, and cash. With respect to contraband, the policy is that the government will not allow drugs or weapons to be released outside of the government agents' control. Thus, in such cases, seizure cannot be postponed for any significant period of time. With respect to controlled deliveries of money, these are allowed according to the guidelines of each law enforcement agency and are closely monitored by the law enforcement agencies and the DOJ. Law enforcement agencies also have the ability to use wiretap and undercover operations in AML/CFT investigations.

333. Additionally, many of the law enforcement agencies have units that specialize in investigating the proceeds of crime and are staffed with trained financial investigators. For example, the DEA's FO focuses on the financial component of drug investigations. Numerous interagency working groups and task forces also specialize in money laundering and terrorist financing investigations, such as the HIFCAs (for ML) and the JTTFs (for FT). Other interagency working groups focus on intelligence sharing. All of these groups are discussed in more detail in section 6.1 of this report. Additionally, special units, such as the AFMLS, have been established to focus on the seizure, freezing and confiscation of the proceeds of crime.

334. As well, cooperative investigations sometimes take place with appropriate competent authorities in other countries. Such investigations may include the use of special investigative techniques.

335. At the information and intelligence gathering stage, the USA PATRIOT Act provides valuable tools, including roving wiretaps and nationwide search warrants, which allow a U.S. federal judge, with adequate predication, to issue warrants for searches to be conducted outside that judge's judicial district. Many such provisions would have expired at the end of calendar 2005 as a result of "sunset" provisions on many of the most useful provisions of the USA PATRIOT Act. However, Congress took interim steps to extend these provisions of the USA PATRIOT Act long enough to enable them to pass a more permanent extension of those provisions. On 9 March 2006, the President of the United States signed into law the USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109-177) and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (S. 2271).

Recommendation 28 (Law enforcement powers)

Powers to compel production, search and seize

336. Although there is a legal basis for secrecy between banks and their account holders,—the Right to Financial Privacy Act (RFPA), enacted in 1978 (12 USC 3401-22)—law enforcement and other competent authorities have the power to compel production of financial records through the issuance of administrative, grand jury or civil subpoenas. Law enforcement authorities can conduct searches of persons or premises to obtain evidence of money laundering or other financial crimes, including the seizure of financial documents, if a search warrant is obtained from an appropriate judicial authority or where there are exigent circumstances which negate the necessity of obtaining a search warrant. The documents obtained through the issuance of subpoenas or obtained through searches can be used in the investigation and prosecution of money laundering or terrorist financing or in a forfeiture action.

337. The RFPA generally prohibits disclosure of information to federal government authorities without notice to the customer and an opportunity for the customer to challenge the request. However, exceptions exist in the context of administrative, grand jury or civil subpoenas. Criminal and civil penalties exist for making certain disclosures involving offenses regarding the subpoena: criminal fines and prison terms of up to five years [18 USC 1510(b)] and RFPA civil penalties for disclosure [12 USC 3420(b)]. See section 3.4 below for a more detailed discussion of the RFPA.

338. The DOJ is able to apply for grand jury subpoenas and search and seizure warrants on behalf of U.S. federal law enforcement agencies from the U.S. judiciary system in order to compel production of, search persons or premises for, and seize and obtain transaction records, etc., to be used in conducting investigations and prosecutions of money laundering, terrorist financing, and the underlying predicate offenses and related actions such as asset seizure and forfeiture. A similar system is in place at the state and local level. Representatives from the DOJ confirmed that a subpoena can be obtained quickly. See section 5.1 below for a description of the process for obtaining a grand jury subpoena.

339. U.S. law enforcement authorities also have additional powers, including the use of Geographic Targeting Orders (GTO). A GTO gives Treasury the authority to require a financial institution or a group of financial institutions in a geographic area to file additional reports or maintain additional records above and beyond the ordinary requirements imposed by BSA regulations. Pursuant to 31 USC 5326, as implemented by 31 CFR 103.26, the Secretary of the Treasury, upon a finding that reasonable grounds exist for concluding that additional recordkeeping and reporting requirements are necessary to carry out the purposes of this subtitle, may target specified financial institutions in a geographic area to submit reports for currency transactions of USD 10,000 or less, for up to 60 days (subject to renewal).

340. A GTO has at least two important and complementary functions. First, it serves as an information gathering device that enables law enforcement authorities to gain greater knowledge of

patterns of money laundering. The information gathered helps to establish better estimates of the volume of illicit funds laundered, and assists in more effective targeting of illegal activities by law enforcement. Second, a GTO helps to prevent evasion of the BSA regulations by disturbing established patterns of money laundering through the introduction of uncertainty and heightened risk into the cost-benefit and other calculations of illicit money movers who would circumvent the standard BSA reporting and record keeping requirements.

Powers to take witness statements

341. As part of their investigatory powers, the relevant law enforcement authorities have the power to interview and take witness' statements for use in a criminal investigation and prosecution, as well as in civil litigation.

2.6.2 Recommendations and Comments

342. The U.S. has designated law enforcement authorities that have responsibility for ensuring that ML/FT offenses are properly investigated. These authorities have adequate powers, are producing good results and seem to be working effectively.

2.6.3 Compliance with Recommendation 27 and 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	C	• The Recommendation is fully observed.
R.28	C	• The Recommendation is fully observed.

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis

Special Recommendation IX (Cash couriers)

343. Cash can be smuggled out of the U.S. through the 317 official U.S. land, sea, and air ports of entry (POE), and any number of unofficial routes out of the country along the Canadian and Mexican borders. The northern border recorded 77 million individual crossings and 37 million vehicle crossings in 2004. The southern border has five times more traffic than the northern border. There are 35 official POE on the U.S. border with Mexico and some 1 million individuals who cross over daily.[52] Canada and Mexico are the two largest U.S. trading partners with USD 446 billion and USD 267 billion in merchandise trade last year, creating ample opportunity to smuggle cash out of the country in shipping containers. The 2006 "U.S. Money Laundering Threat Assessment" confirms that the nature of money laundering in the U.S. has reverted from using the financial system back to more "basic" methods of simply moving cash. This assessment is supported by anecdotal evidence received from state and federal prosecutorial authorities throughout the onsite visit.

344. The two primary agencies responsible for the seizure and investigation of cash smuggling in the U.S. are CBP and ICE. Both fall under the DHS. ICE targets key debarkation ports that are most likely to be used by international couriers, including the perceived threat of currency smuggling at particular ports.

Implementation of a declaration system

345. The U.S. has implemented a declaration system that applies to incoming or outgoing physical transportations of cash and monetary instruments—Reports of International Transportation of

[52] Fisk, Daniel W., Deputy Assistant Secretary of State for Western Hemisphere Affairs, Statement Before the Senate Committee on Foreign Relations, 6 April 2005.

Currency or Monetary Instruments (CMIR) [31 CFR 103.23(a) and 31 USC 5316 and 5317]. The bearer is obligated to declare to the CBP the total amount of currency, coins or other monetary instruments being brought into the U.S. ICE has primary investigative jurisdiction for violations of this reporting requirement. A definition of "monetary instruments" is included in the instructions of the CMIR and meets the definition of "bearer negotiable instruments" as that term is used in Special Recommendation IX.

346. The obligation to make a truthful written declaration is triggered when a person physically transports, mails, ships, or causes to be physically transported, mailed or shipped, currency (U.S. or foreign) or other monetary instruments in an aggregate amount exceeding USD 10,000 on any one occasion to or from the U.S. In addition, 31 CFR 103.23(b) states that each person in the U.S. who receives currency or other monetary instruments in excess of USD 10,000, from a place outside the U.S., must report the amount, the date of receipt, the form of monetary instruments, and the person from whom the currency or monetary instruments were received.

347. It should be noted that the CMIR requirement does not apply to certain types of financial institutions/entities, including the Federal Reserve, a bank or an SEC-registered securities broker dealer with respect to currency or other monetary instruments which are mailed or shipped through the Postal Service or by a common carrier [31 CFR 103.23(c)]. In addition, with respect to overland shipments, commercial banks and trust companies are exempt from reporting currency shipped to or received from the account of an established customer who maintains a deposit relationship with the bank, provided the item amounts are commensurate with the customary conduct of business of the customer concerned. However, such entities would still be obligated to make a truthful disclosure if asked by customs authorities.

348. With respect to incoming transportation of cash or monetary instruments, all travelers entering into the U.S. must complete CBP Form 6059B, Customs Declaration for Passengers. At different stages people are informed that they are obliged to report the transport or transfer of USD 10,000 or more, either by signs along the road towards the border and/or through an interview by the CBP-officer. The CBP Form 6059B is provided either on an airplane, vessel or at the border crossing. Question 13 of the form asks if the traveler is entering with USD 10,000 or more or its equivalent in currency or monetary instruments and advises the traveler that this money or monetary instruments must be declared upon entry. If the answer is "yes", then the traveler must fill out FinCEN Form 105, which is the CMIR form described above. In addition, CBP Form 1304 Customs Declaration is specifically used for crewmembers (and also asks if the traveler is entering with USD 10,000 or more or its equivalent in currency or monetary instruments and advising the traveler that this money or monetary instruments must be declared upon entry). Within approximately three weeks this form is filed in a database and by then accessible for further analysis and/or investigation purposes.

349. The system described above is enforced through intelligence-driven targeting, inbound and outbound blitzes and increased scrutiny of courier hubs. CBP and ICE emphasized that they, at this moment, place greater emphasis on stringent preliminary and intensified inbound examinations. Inbound roving operations take place at airports during which inspectors in plain clothes act as spotters and uniformed inspectors conduct field interviews of suspicious travelers as they wait for their luggage.

Implementation of a disclosure system

350. The U.S. has also implemented a disclosure system in relation to outgoing physical transportations of cash and monetary instruments. Random and target-specific outbound operations take place with cash leaving the U.S. Notification of the reporting requirements for passengers departing the U.S. is accomplished through the placement of posters in the departure lounges and border crossings, entrances to the jet way and inside the jet way. In addition, announcements of the currency reporting requirements are made over the public address system before initiating any inspections. Interviews are conducted on those individuals who merit further examination and a number of questions are asked to determine if the declaration, disclosure, or both, are truthful.

351. These obligations also apply to containers and the mail. Individuals who are shipping goods through containerized cargo are notified of the requirements in the Shippers Export Declaration form (SED). With respect to transportations effected through the mail, first class mail (including Express Mail and mail destined for delivery in foreign countries) is sealed against inspection under U.S. law. This means that mail cannot be opened by law enforcement personnel without a court order granting authority to open mail. There is no legal provision for a person to claim the value of any cash that may be included in mail pieces. That notwithstanding, the Postal Inspection Service aggressively investigates proceeds from illicit activities being sent through the mail. The Inspection Service has seized, pursuant to court-ordered search and seizure warrants, millions of dollars of illicit proceeds from the mail. In addition, Postal Inspectors initiated 1,534 investigations involving the illegal mailing of controlled substances in FY 2005. Inspectors made 1,855 arrests and reported 1,279 convictions for mail-related violations.

Powers of competent authorities upon discovery of a false declaration/disclosure or suspicion of ML/FT

352. Upon discovery of a false declaration/disclosure of currency or monetary instruments or a failure to declare/disclose them, the funds are subject to seizure/forfeiture and the subject is subject to arrest and prosecution. When a subject is placed under arrest, an attempt is made to interview him concerning the source of the funds. In concert with this interview, an investigation is initiated to determine what, if any, connection the funds have to criminal or terrorist activity. These actions are implemented by CBP officers using procedures established by the former U.S. Customs Service. Officers perform thorough inspections of passengers, conveyances and cargo when it is suspected that currency and bearer-negotiable instruments may be falsely declared or disclosed or that they may be related to terrorist financing or money laundering.

353. Furthermore, CBP, ICE and other competent authorities have the authority to obtain subpoenas and search warrants for the purpose of gaining additional information and evidence. Border authorities also have the authority to demand production of witnesses and records. Additional ICE/CBP authorities to request and obtain further information include:

(a) Title 19 USC 482: Authority to search persons and conveyances;

(b) Title 19 USC 1486: Authority to administer oaths;

(c) Title 19 USC 1581: Authority to search and seize;

(d) Title 19 USC 1582: Authority to detain persons; and

(e) Title 19 USC 1589: Authority to carry weapons, make arrests, execute warrants.

354. In addition to the above, Customs authorities under Title 19, ICE and CBP have the authority to conduct searches without a warrant pursuant to border search authority under 19 USC 1595. Under Title 19 (Customs Duties), ICE and CBP are the designated competent authorities vested with the authority to stop, search, seize, forfeit and arrest for cross-border crimes. ICE and CBP have the authority through a number of statutes (31 USC 5316, 31 USC 5317 and 31 USC 5332) to stop or restrain currency for a reasonable time that is unreported or falsely reported.

355. For purposes of ensuring compliance with the CMIR requirements or any other suspected violation of law, a customs officer may stop, search and seize, at the border without a search warrant, any vehicle, vessel, aircraft, or other conveyance, any envelope or other container, and any person entering or departing the U.S. (31 USC 5316 and 31 USC 5317). Additionally, under 31 USC 5317, a search warrant may be executed when law enforcement reasonably believes that a monetary instrument is being transported and a CMIR has not been filed or contains a material omission or misstatement.

356. Detailed procedures exist for CBP and ICE officers who are initially involved in restraining persons and currency at the border. In addition to interviews to determine suspicion of money laundering and terrorist financing, a document review is conducted including a review of passports,

tickets and other evidence to scrutinize frequency of travel to source countries, or other indicators of suspicious travel. If suspicion is developed that indicates there is evidence of money laundering or terrorist financing involved, the funds will be detained by CBP or ICE as the competent authority during cross-border encounters. Additionally, a money laundering or terrorist financing investigation is initiated by ICE or other competent authority pursuant to 18 USC 1956 and 18 USC 2339, money laundering and terrorist financing, respectively. When there is suspicion that the funds may be related to money laundering or terrorist financing, or when there is a false declaration, these funds can be restrained through both criminal and civil procedures.

Information collected and retained

357. When currency or monetary instruments are declared, the type and amount of currency and monetary instrument as well as the bearer's identification data is recorded on the CMIR and retained. In addition, if the cash is not U.S. currency, the name and country of the currency must also be recorded. Disclosure of the social security number is mandatory as this number is used as a means to identify the individual who files the report [31 USC 5316(b) and 31 CFR 103.27(d)].

358. Additionally, when currency or monetary instruments are detected (either through false declaration or suspicion of money laundering or terrorist financing), the amount and bearer's identification data are recorded electronically in a seizure report and retained for use by the appropriate authorities. The amount, type, and denomination of currency information is retained electronically in a seizure report available for all competent authorities. Identification of an individual or company making outbound transportation of currency, as well as amount, type, and denomination of declared currency is retained electronically as well as identification of all individuals, planes, or vessels leaving the U.S. via air or sea, and all cargo containers. When operations on land borders of outbound traffic are conducted information is recorded and retained.

359. The data collected via CMIR and seizure reports are maintained in the computerized database known as the Treasury Enforcement Communications System (TECS) which is available to all competent authorities involved in AML/CFT enforcement. Additionally, the information derived from the completed CMIR, as well as any intelligence derived from currency seizures, is forwarded by CBP to FinCEN via electronic database. In July 2003, the CMIR became a FinCEN form like other BSA reporting forms. CBP and ICE seizure and arrest data is also captured in the Treasury Enforcement Communications System II (TECS II). TECS II is one of the world's largest databases containing over a decade of data related to domestic and international financial crimes. All relevant U.S. law enforcement agencies have access to this data through FinCEN.

360. The principal purpose for collecting the information contained on the CMIR is to assure maintenance of reports or records having a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings. The information collected may be provided to those officers and employees of CBP, ICE and any other constituent unit of the DHS that has a need for the records in the performance of their duties. The records may be referred to any other department or agency of the federal government upon the request of the head of such department or agency. The information collected may also be provided to appropriate state, local, and foreign criminal law enforcement and regulatory personnel in the performance of their official duties.

Coordination among domestic competent authorities

361. Following 9/11, the Homeland Security Act of 2002 created the DHS to secure the nation against terrorist attacks, ensure a coordinated response to threats, crises, and disasters, and execute the border security and immigration missions of the legacy Customs Service and Immigration and Naturalization Service, into one entity. DHS is responsible for, among other things, securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the U.S., including managing and coordinating those functions transferred to DHS at ports of entry.

362. The Task Force concept, which combines representatives from federal, state and local agencies, is also widely employed in the implementation of SR IX. For example, to supplement the CBP/ICE staffing at borders, cash interdiction task forces have been established at key border entry points on the southwest border with Mexico. In addition, CBP has developed an Outbound Currency Interdiction Training (OCIT) program. The training includes instruction and practical exercises to provide specialized knowledge in currency interdiction, and has an anti-terrorism component. This training is provided to a variety of federal, state and local inspectors and border officials.

363. Additionally, the DEA FO, has implemented a "bulk" currency initiative that is aimed at assisting in the development of new investigations pertaining to seizures of large amounts of U.S. currency as well as linking these seizures to ongoing drug investigations. This initiative endeavors to bring together all of the information and intelligence from existing interdiction programs through cooperative and collaborative sharing of information between federal, state, and local initiatives, and will include currency seizures made on U.S. highways through the highly successful "Operation Pipeline" program, currency seizures made at various U.S. commercial airports through "Operation Jetway" and seizures made by DEA-led investigations. The EPIC acts as the central repository for all information related to "bulk" currency seizures.

364. To complement the ICE Bulk Cash initiatives being conducted primarily at the U.S. borders, the IRS-CI is studying interceptions of bulk cash by state and local law enforcement in the interior of the U.S. IRS-CI is planning to concentrate resources on the intra-country routes identified by this analysis to provide resources to uncover and dismantle the money laundering organizations using these routes.

International cooperation and assistance

365. The U.S. accomplishes the exchange of customs information both bilaterally and multilaterally through the following mechanisms: DHS (ICE and CBP) Attachés posted in U.S. Embassies and Consulates throughout the world; EUROPOL, INTERPOL and World Customs Organization Liaison Officers; the International Bulk Currency Smuggling Training Initiative; the International Law Enforcement Academies (ILEA); Passenger Pre-Clearance Programs; customs mutual assistance agreements; and mutual legal assistance treaties.

366. In an effort to enlist and expand support on the Mexican side of the border for currency interdiction, the U.S.-Mexico Border Partnership was signed in March 2002. In addition to sharing data on the physical cross-border movement of cash, the initial bilateral efforts have focused on the following five major programs (these programs are not exclusive to the U.S. Mexico partnership).

(a) **Vehicle and Cargo Inspection System (VACIS):** The U.S. has 10 permanent devices capable of scanning (x-ray or gamma ray) sealed containers, including vehicles as large as a railroad car. Additionally, it has three mobile VACIS (for moveable truck or car inspection) and three portable x-ray scanners (for inspecting luggage) at seven border crossing sites, international airports, and rail stations. The U.S. plans to install the VACIS machines along the southern border this year.

(b) **Advanced Passenger Information System (APIS):** APIS (which became operational in 2004) enables the Mexican authorities to screen passenger manifests of incoming commercial air flights against law enforcement, terrorism and immigration data banks in both Mexico and the U.S.

(c) **Secure Electronic Network for Travelers Rapid Inspection (SENTRI):** SENTRI are special land border crossing lanes for expedited inspection of pre-registered, low risk, frequent travelers to reduce inspection loads. CBP now has fully-funded projects underway coordinated on both sides of the border at six principal crossing sites.

(d) **Border Wizard:** Border Wizard is software the U.S. uses that creates a simulated model of a border crossing and inspection site as a management tool to analyze traffic flow and resource use. The software is being adapted for Mexico.

(e) **Safety and Training courses** are conducted for Mexican border law enforcement personnel.

367. The ICE Attaché in Mexico City, in coordination with Mexican authorities, conducts investigations into the smuggling of U.S. bulk cash into Mexico and onward to Central and South America. Three separate outbound operations conducted at Benito Juarez International Airport in Mexico City resulted in the seizure of over USD 33 million and the arrest of over 50 individuals.

Sanctions for making a false declaration or disclosure

368. Depending on the severity of the offense, a number of different judicial, law enforcement and regulatory authorities (e.g. U.S. Attorney, CBP, ICE, and FinCEN) have the power to impose criminal penalties, civil penalties or administrative fines.

369. With respect to the CMIR declaration obligations, persons who make false disclosures or declarations are subject to a wide range of criminal, civil and administrative sanctions. Civil and criminal penalties, including under certain circumstances an administrative fine of not more than USD 500,000 and imprisonment of not more than ten years, are provided for failure to file a report, filing a report containing a material omission or misstatement, or filing a false or fraudulent report. Examples of criminal penalties include, under the CMIR Statute (31 USC 5317), incarceration of up to 6 months for smuggling USD 350,000.

370. If currency or monetary instruments are not declared, it is considered a false declaration and they are subject to seizure and forfeiture by the relevant competent authority (CBP/ICE). When unreported currency is found, it is turned over to a Seized Property Custodian for storage or an ICE Special Agent for further investigation. If the officers determine that an individual is in violation of the reporting requirements during their examinations, the individual is detained and the local office of the U.S. Attorney is contacted to determine the likelihood the case will be prosecuted and what action to take. If the U.S Attorney declines to prosecute (e.g., extensive caseload or higher priority offenses), ICE can still seize the currency and seek civil forfeiture of the funds. In addition, if the amount in question is less than USD 500,000, the forfeiture may be pursued administratively.

371. These sanctions can be applied to all persons required to file a CMIR which includes: an individual, corporation, partnership, trust or estate, joint stock company, association, syndicate, joint venture or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities. As far as the institutions are concerned which the Federal Banking Agencies supervise, any failure to comply with BSA-related regulatory requirements, the Federal Banking Agencies have a range of supervisory tools available to them in order to encourage corrective action by the institutions and their institution affiliated parties (see section 3.10).

Sanctions for bulk cash smuggling

372. In addition, the Bulk Cash Smuggling Statute (31 USC 5332) also dramatically increased the criminal penalties for currency smuggling. The criminal sanctions for violating section 5332 are a term of imprisonment for not more than five years as well as the forfeiture of all property, real or personal, involved in the offense. Under the Bulk Cash Smuggling Statute, sentencing guidelines call for a sentence of 15 to 21 months for smuggling USD 30,000.

373. Section 5332(b) provides for criminal forfeiture of the property, real or personal, involved in the offense, and any property traceable to such property. This includes a personal money judgment if the directly forfeitable property cannot be found and the defendant does not have sufficient substitute assets to satisfy the forfeiture judgment. The statute therefore targets individuals, criminal organizations, and terrorists smuggling currency or monetary instruments in excess of the reporting requirement. One of the main purposes of this statute is to authorize forfeiture of any cash or instruments of the smuggling offense. Prior to this statute being enacted, the Supreme Court had

denied the Government's right to forfeit the entire amount of currency that was not reported in violation of a cash transaction reporting statute (Title 31 USC 5316). The court held that forfeiture was grossly disproportionate sanction to the gravity of the cash transaction reporting offense.[53] Prosecutors under the bulk cash smuggling statute must prove that the defendant intended to avoid the currency and monetary instrument reporting requirement. The U.S. authorities have anticipated legal challenges suggesting that the new statute is nothing more than a re-codification of the existing penalties for violating the currency reporting requirements which is why Congressional findings as to the purpose of the statute have been included in the provision. The findings emphasize the seriousness of currency smuggling and the importance of authorizing confiscation of the smuggled money. In particular, the findings state that the intentional transportation of currency into or out of the U.S. "in a manner designed to circumvent the mandatory reporting (requirements) is the equivalent of, and creates the same harm as, smuggling goods." Moreover, the findings state that "only the confiscation of smuggled bulk cash can effectively break the cycle of criminal activity of which the laundering of bulk cash is a critical part." Section 5332(c) authorizes civil forfeiture for the same offense.

374. Section 5332 makes it a crime for anyone with the intent to evade the CMIR requirement to knowingly conceal more than USD 10,000 in currency or monetary instruments and to transport or transfer or attempt to transport or transfer such currency or monetary instruments into or out of the U.S. This offense focuses on the intent to evade the reporting requirement rather than the source or destination of the funds. To obtain a conviction under the section 5332 offense, the prosecution must prove the following elements:

(a) *Actus Reus:*

  (i) The defendant transports or transfers or attempts to transport or transfer from or to the United States

  (ii) The defendant transports more than USD 10,000 in currency or other monetary instruments.

  (iii) The defendant conceals the transferred or transported cash. Concealed is defined to include either on the defendant's person (including concealment in any article of clothing worn or in any luggage carried) or in any conveyance, luggage, merchandise or other container. The DOJ has confirmed that if the target entering or leaving the U.S. makes no attempt to conceal the money, this offense cannot be proved;

(b) *Knowledge*: The defendant must have knowingly concealed the money.

(c) *Intent*: The defendant must have intended to evade the CMIR reporting requirement under 31 USC 5316 which requires reporting of monetary instruments transported into and out of the U.S.

Sanctions for making a cross-border transportation related to ML/FT

375. Sanctions also apply to persons who are conducting cross-border transportation of cash that may be related to money laundering or terrorist financing. Persons who try to launder funds or monetary instruments by transporting it across the U.S. border can be prosecuted criminally pursuant to section 1956(a)(2) (the international money laundering offense). This offense is described in more detail above in section 2.1. Criminal sanctions for violating section 1956 are a fine of not more than USD 500,000 or twice the value of the property involved in the transaction (whichever is greater) or imprisonment for not more than 20 years or both.

376. Additionally, persons found with currency or monetary instruments that is related to terrorist financing can also be charged under 18 USC 2339C (Prohibitions Against Terrorist Financing) and sentencing guidelines for this charge can be up to 20 years. The powers available to U.S. authorities

[53] United States v Bajakajian, 524 U.S. 321 (1998).

are both broad and proportionate to the severity of the situation. For example, if the amount in question is less than USD 500,000, the forfeiture may be pursued administratively.

Seizing, freezing and confiscation

377. Many asset forfeiture provisions apply to persons who are smuggling cash or monetary instruments that are related to terrorist financing or money laundering. These include the following:

(a) Title 31 USC 5321 and 31 CFR 103.57 (Civil penalties for not filing or filing a false report);

(b) Title 31 USC 5322 and 31 CFR 103.59 (Criminal penalties for concealed transportation with the intention of evading reporting requirements);

(c) Title 31 USC 5317 and 31 CFR 103.58 (Search and forfeiture of monetary instruments);

(d) Title 31 USC 5324(c) (Criminal penalties for not filing or filing a false CMIR); and

(e) Title 18 USC 981(a)(1) and 18 USC 982(a)(1) (Civil and criminal forfeiture for violations of 18 USC 1956).

378. Persons who are conducting cross-border transportation of cash that are related to terrorist financing are also subject to the following two statutes: Material Support to Terrorism and Terrorist Financing (18 USC 2339A) and Prohibitions Against the Financing of Terrorism (18 USC 2339C), both of which focus on the movement of currency and monetary instruments in support of terrorist financing. In terms of implementation, when targeting individuals, names are checked against the OFAC list and UN terrorist watch lists. Systems are in place to freeze assets consistent with the travel ban requirements contained in S/RES/1267(1999) and S/RES/1373(2001).

Unusual cross-border movements of gold, precious metals or precious stones

379. If the U.S. discovers an unusual cross-border movement of gold, precious metals or precious stones, notification of the appropriate customs service or other competent authorities of the countries from which these items originated and/or to which they are destined is accomplished via the corresponding ICE Attaché. For instance, ICE has cooperated with foreign customs authorities and notified them when unusual shipments of gold are discovered.

Safeguards to ensure the proper use of information reported or recorded

380. The systems for reporting cross border transactions are subject to strict safeguards to ensure proper use of the information or data that is reported or recorded. In addition, data of this type is protected by the BSA of 1970 and the Privacy Act of 1974—both of which provide substantial penalties for any misuse or abuse.

Other measures

381. Additionally, the U.S. has implemented some of the measures set out in the Best Practices Paper for SR IX. For instance, civil penalties impose a reverse burden of proof on the person carrying currency or bearer negotiable instruments. In other words, if the person is unable to demonstrate the legitimate origin and destination of the currency or bear negotiable instruments, those funds can be stopped or restrained.

Effectiveness of the measures relating to cash couriers

382. Since 1970, the U.S. has been collecting information relative to the international movement of currency and monetary instruments through the use of the CMIR form. A table of the filings over the past four years follows.

Reports of International Transportation of Currency and Monetary Instruments Filed (2001-2004)	
2001	298,483
2002	276,513
2003	232,665
2004	229,131
TOTAL	1,036,792

383. The assessment team met with ICE officers in New York, Miami, Phoenix and Washington DC. Both groups do excellent work, especially in consideration of the significant volume of people and cargo that cross the border annually. From 2001 through February 2005, ICE agents have arrested more than 260 individuals for bulk cash smuggling violations. Approximately 20% of the arrests resulted from seizures not at a border or port of entry but within the interior of the U.S. In addition, ICE and CBP have seized a combined total of more than USD 107 million in cases where bulk cash smuggling was charged. A preliminary review of these records indicates approximately 16% of seizures were from Mexican nationals, 18% were inbound seizures from Mexico, and 18% of the seizures were believed to be destined to Mexico. The following statistics show how many arrests, indictments and convictions for bulk cash smuggling resulted from ICE investigations for the fiscal years 2003 to 2005.

Prosecutions for bulk cash smuggling offense (31 USC 5332)

Number of...	Fiscal year 2003	Fiscal year 2004	Fiscal year 2005 (first 9 months)
Cases	-	124	124
Defendants	58	133	140
Convictions	32	75	100

384. The following statistics show how many cases arose for not filing reports on the exportation and importation of monetary instruments for the fiscal year 2004.

Prosecutions relating to reports on exporting and importing monetary instruments (31 USC 5316)

Number of...	Fiscal year 2004
Cases	99
Defendants	109
Successful charges	108
Terminated defendant count	96
Guilty	67

385. The following statistics show how many forfeiture cases arose during fiscal year 2004 in relation to violations of sections 5313 (failing to file a report on domestic coins and currency transactions), 5316 (failing to file a report relating to the exportation or importation of monetary instruments) and 5324 (structuring transactions to avoid the reporting requirement).

Prosecutions relating to the search and forfeiture of monetary instruments (31 USC 5317)

Number of...	Fiscal year 2004
Cases	27
Defendants	39
Successful charges	19
Terminated defendant count	19
Guilty	6

386. ICE has been involved in various law enforcement projects that have focused successfully on specific aspects of bulk cash smuggling. Operation Pipeline records seizures made from private cars and trucks. Operation Convoy records highway seizures involving commercial vehicles. Operation Jetway records seizures from airports, train and bus stations, package shipment facilities (e.g. FedEx and UPS), U.S. Post Offices, and airport hotels/motels.

387. In 2003, ICE made a total of 575 cash seizures totaling over USD 62 million. In 2004, ICE made a total of 311 cash seizures totaling over USD 18 million. All of these seizures were made pursuant to 31 USC 5316, 31 USC 5317 and 31 USC 5332. Over half of these seizures made in 2003-2004 resulted in a criminal conviction. The following table sets out the top ten origins and number of recorded seizures of cash and monetary instruments from 2001 to 2003.[54]

2001		2002		2003	
Texas	140	Texas	130	Texas	128
California	122	California	126	California	115
New York	122	New York	81	New York	78
Illinois	113	Illinois	71	Illinois	77
Georgia	76	Georgia	56	Georgia	59
Ohio	60	Ohio	48	Florida	45
Michigan	57	Florida	44	Ohio	45
Florida	48	Michigan	43	Tennessee	39
Missouri	48	Tennessee	32	Michigan	37
North Carolina	47	Missouri	31	Arizona	36
No State ID	527	No State ID	338	No State ID	331

2.7.2 Recommendations and Comments

388. The law enforcement authorities have a clear understanding of the procedures that are in place in the U.S. for implementing Special Recommendation IX. Overall, the measures for implementing Special Recommendation IX are working effectively. There are, however, a number of comments—none of which affects the rating.

389. Since drugs are imported in the U.S. by international criminal organizations, for instance by organizations located and operating out of/from Mexico and South America, the earnings of these operations are smuggled out of the country via different means. This may include, alone or in combination, using cash couriers, bulk smuggling (for instance via vehicles) and/or wire transfers. Especially in a state like Arizona, close to the Mexican border, it was indicated that the money flow coming into the State greatly exceeds the money leaving the state. However, the CBP and ICE emphasized that they, at this moment, place greater emphasis on stringent preliminary and intensified inbound examinations. The competent authorities should, however, ensure that they do not lose sight of the fact that money and other bearer negotiable instruments which leave the country and is related to ML/FT may return to the U.S. when it is placed, layered and finally integrated into the financial system. The U.S. authorities are therefore advised to further invest in the detection and investigation as well as the resources, techniques and methods to counter outgoing cross-border transportations of cash or any negotiable bearer instrument.

390. Additionally, the authorities should focus on conducting thorough border checks of people, vehicles, trains, cargo, etc., without allowing the level of thoroughness to be dictated by the volume of traffic waiting to cross the border.

[54] The decrease in reported seizures by ICE for 2004 is attributable to the fact that the 2003 figure represents the aggregate totals reported by ICE, CBP, and the legacy U.S. Customs Service. Starting in 2004, seizure data is reported separately by ICE and CBP.

2.7.3 Compliance with Special Recommendation IX & Recommendation 32

	Rating	Summary of factors relevant to s.2.7 underlying overall rating
SR.IX	C	• The Recommendation is fully observed.

3. PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

Preamble: Guidance as "other enforceable means"

391. Throughout this section of the report extensive reference is made to various types of guidance issued by the regulatory agencies with respect to the financial sector's AML/CFT obligations and the regulators' approach to compliance. The assessment team considers such guidance to be "other enforceable means" if the following elements are met:

(a) the guidance was issued by a competent authority, including securities SROs, or its existence otherwise has a clear basis in law;

(b) the guidance specifically addresses the issues required to be in place in accordance with the methodology;

(c) there is a clear means by which the guidance is legally enforceable (i.e. it underpins a legal obligation) by criminal, civil or administrative means, either through powers directly available under the BSA, or through the use of the regulators' own authority, including to ensure "safety and soundness" within a financial institution;

(d) there are effective, proportionate and dissuasive sanctions for persons that fail to comply with the obligation; and

(e) there is clear evidence or precedent for the guidance being cited as a basis for enforcement action that has actually been taken or remedial action required.

392. The extent to which such guidance can be deemed to be "other enforceable means" is central to the evaluation of the financial sector preventive measures, and the position taken on the main forms of guidance is as follows, unless otherwise stated in a specific context.

a) **Interpretive guidance published in the Federal Register:** This typically takes the form either of a preamble to the published regulations, or responses to informal enquiries on the application of the regulations. Such guidance does not have direct force of law, but, according to recent notice published by FinCEN, is considered by the authorities to have "persuasive precedential effect". To the extent that the authorities may cite non-compliance with such guidance in the general context of enforcement action, this has been considered to represent "other enforceable means".

b) **FFIEC BSA AML Examination Manual:** In June 2005 the Federal Financial Institutions Examination Council (comprising the five Federal Banking Agencies),[55] working in conjunction with FinCEN, published its Bank Secrecy Act/Anti-Money Laundering Examination Manual ("FFIEC Manual"). The intention was to ensure consistency in the application of the AML/CFT requirements, and in the compliance examination procedures. This manual (which extends to 330 pages) provides a comprehensive description of the systems, controls and procedures that are expected of federally-regulated banks, credit unions, trust companies and thrifts in order to comply with the legal and regulatory requirements. It also describes the examination techniques that will be employed to test compliance with the requirements. Contained within the FFEIC Manual is a considerable amount of guidance that is undoubtedly accepted by the banks as the benchmark for the minimum standard for compliance with their AML/CFT obligations. While

[55] For further information on the role of the FFIEC, see section 3.10.1 below.

the guidance has no direct force of law, the regulators consider that, since they conduct AML examinations both under formal delegation from FinCEN (31 CFR 103.56) and in the broader context of their safety and soundness procedures, non-compliance with the principles enunciated in the FFEIC Manual (in as far as they are not directly supported by primary or secondary legislation) would provide a basis for administrative enforcement action.

In support of this assertion, the authorities have shown precedent in the form of actions taken under Title 12 (banking legislation) in respect of AML deficiencies. The following sample language that requires affirmative action to address safety and soundness deficiencies in customer due diligence procedures is found in several actions taken by the Federal Reserve over the past two years. This reflects concepts addressed within guidelines that preceded the FFIEC Manual.

> "Within 60 days of this Agreement, the Bank shall submit to the Reserve Bank an acceptable written customer due diligence program designed to reasonably ensure the identification and timely, accurate, and complete reporting of all known or suspected violations of law against or involving the Bank and suspicious transactions at the Bank to law enforcement and supervisory authorities as required by the suspicious activity reporting regulations. At a minimum, the program shall include:
>
> (a) a methodology for assigning risk levels to the Bank's customer base;
>
> (b) a risk focused assessment of the Bank's customer base to:
>
> (i) identify the categories of customers whose transactions and banking activities are routine and usual; and
>
> (ii) determine the appropriate level of enhanced due diligence necessary for those categories of customers that pose a heightened risk of conducting potentially illicit activities at or through the Bank;
>
> (c) for each customer whose transactions require enhanced due diligence, procedures to:
>
> (i) determine the appropriate documentation necessary to verify the identity and business activities of the customer; and
>
> (ii) understand the normal and expected transactions of the customer; and
>
> (d) procedures designed to ensure proper identification and reporting of all known or suspected violations of law and suspicious transactions, including but not limited to:
>
> (i) effective monitoring of customer accounts and transactions, consistent with industry sound practices; and
>
> (ii) appropriate participation by senior management in the process of identifying, reviewing, and reporting potentially suspicious activity."

In addition the OCC has cited two cases where BSA enforcement actions involving non-compliance with the guidelines set forth in the OCC's BSA Handbook (a predecessor to the FFIEC Manual) were brought:

- Banco do Estado Parana (Federal Branch) (April 1998) — cease and desist action and formal order of investigation brought for, among other things, unsafe and unsound banking practices for failure to comply with the "know-your-customer" (customer due diligence) guidelines and the guidelines concerning payable though accounts contained in the BSA/AML Handbook.

- Broadway National Bank (April 1998) - cease and desist action and formal

order of investigation brought for, among other things, unsafe and unsound banking practices resulting from failure to comply with the "know-your-customer" (customer due diligence) guidelines contained in the BSA/AML Handbook.

Therefore, the prescriptive elements of this manual (as opposed to those that are clearly "for consideration") are deemed to be "other enforceable means" for the purposes of this report.

c) **Interagency guidance:** The regulatory authorities have issued a number of joint guidance notes addressing specific details of the AML requirements (e.g. under cover of Supervision and Regulation Letters issued by the Federal Reserve). These may take the form of statements of future practice, interpretive guidance or frequently asked questions. The language adopted in such guidance is of an interpretive nature, and the authorities have indicated that institutions may reasonably rely on the guidance in fulfilling their responsibilities, to the extent that an "aggressive" position is taken by the regulators in respect of its application by the institutions. Guidance issued in this form appears to have the same status as that contained in the FFIEC manual and is, therefore, considered to be "other enforceable means".

d) **Guidance by SROs to Securities Sector Participants:** In addition to information published in the Federal Register as part of their rule making process, both the NYSE and NASD provide guidance to broker-dealers that are member firms in the form of NYSE Information Memos and NASD Notices to Members (NtMs), respectively. For instance, in February 2006, NYSE issued NYSE Information Memo 06-04 and NASD issued NtM 06-07 discussing recent changes to their respective AML program rules. NASD and NYSE also have previously provided guidance to broker-dealers on AML compliance programs required under the BSA (e.g. NASD NtM 02-21). In addition, NASD has published an AML Template for Small Firms to assist broker-dealers in fulfilling their responsibilities to establish an AML program in compliance with applicable rules and regulations. The SROs and the SEC consider that a failure to comply with BSA regulations as interpreted in the SRO guidance constitutes a basis for administrative enforcement action.

e) **Advisories:** FinCEN routinely issues Advisories relating to specific threats, and these frequently contain guidance on appropriate measures to be taken to counter the threat. An Advisory places a financial institution on notice of high risk activity. Consequently, an institution's failure to incorporate these risks into its anti-money laundering program, and in particular, its procedures for filing suspicious activity reports, could be a factor in determining whether a financial institution failed to comply with its BSA obligations. According to a notice issued by FinCEN, if published in the Federal Register, the guidance in such Advisories has "persuasive precedential effect and may be relied upon by those financial institutions subject to the specific provision of 31 CFR part 103". In such circumstances it constitutes "other enforceable means"; otherwise it is considered to provide "useful insight" into FinCEN's application of the AML legislation.

Preamble: Effectiveness

393. The assessment team considered very carefully how best to assess the effectiveness of the implementation of the preventive measures in the financial sector and, where relevant, in the DNFBP sectors. Typically, this might be achieved by reviewing the procedures undertaken by a sample of private sector institutions, combined with discussions with the regulatory community about their findings (and enforcement action) resulting from their examination program. The team undertook a number of visits to financial institutions of various types and in different locations. However, as the U.S. financial sector is extremely large and diverse, it was clearly impossible, within the constraints of this type of evaluation, to take a representative sample of institutions. Therefore, the main approach adopted by the team was to explore with both federal and state regulators their experience of undertaking BSA compliance examinations, to see if there were any trends emerging that might give rise to questions about the quality of implementation of the legal and regulatory requirements by different sectors of the financial industry. In the following review of the financial and DNFBP sectors,

the measures described in the report are deemed by the evaluation team to have been implemented effectively, except where explicit references to the contrary are made.

Preamble: Approach taken towards ratings

394. The diversity and complexity of the U.S. institutional and financial systems, combined with the fact that different components of the AML regime have been applied to different parts of the financial sector (in line with the risk-based approach adopted by the U.S.), has posed a particular challenge for the evaluation team in arriving at the ratings for compliance with many of the FATF Recommendations. The team based its final view of the level of compliance with the individual Recommendations on its sense of the overall effect of the measures in achieving a robust regime. Necessarily, this involved taking a view that certain financial and other activities (as defined in the Recommendations) were more prone to the risk of money laundering than others, or were more dominant within the US economy. Therefore, the report has focused on these core activities, and has not sought to describe the situation with respect to each of the thirteen financial activities listed in the Recommendations. Also, in the interests of brevity, the team has, for the most part, not sought to describe the relative weighting of the factors that it took into account in each case.

Customer Due Diligence & Record Keeping

3.1 Risk of money laundering or terrorist financing

395. The definition of "financial institution" within the BSA encompasses not only core financial service providers, but also a range of non-financial businesses. Implementing regulations have been issued for all of the significant types of financial institutions, and proposed rules have been issued for certain additional types of financial institutions deemed to pose a less significant risk of money laundering, based upon risk assessments of each type of institution performed by Treasury and FinCEN, in consultation with law enforcement and the relevant federal regulators when appropriate. A description of the overall risk assessment process is contained in section 1 of this report.

396. The following explains the current U.S. view about the extent to which certain activities should be brought within the coverage of the AML rules.

Banking sector

397. The vast majority of institutions included in the very broad category of “bank” under the BSA regulations are subject to the full range of BSA AML requirements, including requirements to file SARs and CTRs, to maintain records of bank and cashiers check purchases and funds transfers, and all other required transactions, and to implement AML compliance and customer identification programs. Through an historical regulatory anomaly, the only types of “banks” not yet directly subject to AML program requirements are a small number of limited purpose entities (discussed further below in paragraph 428). However, FinCEN intends to amend its regulations to eliminate the regulatory anomaly to bring uniformity to the banking sector.

Securities broker-dealers and futures commission merchants (FCMs)

398. Substantive implementing regulations have been issued in respect of the primary securities and commodities sectors. Broker-dealers and FCMs are by far the most important in these industries, inasmuch as they form the backbone of the securities and futures sectors. They maintain the vast majority of accounts in these sectors and are involved in virtually all transactions.

Mutual funds and other investment companies

399. Section 356(c) of the USA PATRIOT Act required a study of investment companies which was completed in December 2002. The study concluded that mutual funds (i.e., registered investment

companies) present a money laundering risk because they offer to redeem their shares continuously. Accordingly, they were required to implement an anti-money laundering program in April 2002 and a customer identification program in September 2003. In April 2006, FinCEN issued a final rule that will require mutual funds to file suspicious activity reports beginning in October 2006. In addition, FinCEN, in consultation with the SEC and the CFTC, has been reviewing other types of investment companies that may pose a risk of money laundering or terrorist financing [67 FR 60617 (26 September 2002) (NPRM)], and has concluded that companies which offer interests that are not redeemable, or that are redeemable only after a lengthy holding or "lock-up" period, lack the liquidity that would make them attractive to money launderers in the first place. According to FinCEN, such illiquid investments as real estate investment trusts (investment vehicles in which the contributions of the participants are pooled to invest in real estate and sometimes in real estate-related securities) require lengthy investment periods without the ability to redeem assets, and, therefore, pose a low risk of money laundering.

400. In light of this approach, FinCEN has issued proposed rules (which are not in force) that would narrow the definition of "unregistered investment company" to exclude certain types of illiquid companies. FinCEN is continuing to review this type of financial institution, and the federal functional regulators have further refined their definitions of various investment companies and investment advisers, and have subjected certain participants to further regulation [69 FR 72054 (10 December 2004) Registration Under the Advisers Act of Certain Hedge Fund Advisers].

Investment advisers[56]

401. The U.S. has considered the risks posed by investment advisers, defined as anyone who, for compensation, engages in the business of advising others as to the value of securities or as to the advisability of investing in, purchasing, or selling securities, or who issues reports concerning securities. Investment advisers may also engage in managing clients' assets with varying degrees of discretionary authority. However, investment advisers registered with the SEC are generally prohibited from directly holding clients' funds or securities [17 CFR 275.205(4)-2]. Instead, assets are held in custody of qualified custodians, a role typically fulfilled by banks or broker-dealers, but it is possible that advisory clients' assets may be held in accounts where the underlying clients are known only to the investment adviser. Services provided to mutual funds represent an important part of investment advisers' business in the U.S. As of April 2006, approximately USD 9.2 trillion of the total USD 31.4 trillion of investment advisers' assets under management were those managed for mutual funds, and already subject to the AML/CFT regime applicable to mutual funds.

402. The U.S. concluded that investment advisers who manage assets are at a greater risk of having clients who are money launderers and terrorist financiers than those that issue research reports, assist in financial planning, or are involved in pension planning. FinCEN and the SEC have also analyzed the degree of risk posed to an investment adviser by different types of customers. For example, an employee retirement savings plan sponsored by a public corporation that accepts assets only in the form of payroll deductions or rollovers from other similar plans presents no realistic opportunity for money laundering, whereas an offshore vehicle not itself subject to any AML Program requirement would present a more significant risk.

403. In light of these conclusions, FinCEN has issued a proposed rule (in May 2003) that would include investment advisers in the definition of "financial institutions" in the BSA (as businesses that engage in similar activities to those businesses included in the definition of "financial institutions") (68 FR 23674). The proposed rule would require investment advisers to establish AML Programs and would permit them to tailor their programs to address the risks presented by the nature of their services and clients in a manner reasonable in light of the firms' size and resources.

[56] While the term "investment adviser" is specifically not included within the FATF definition of financial activities (but is treated under Recommendation 20), it has to be noted that in the U.S., such advisers may also manage very substantial assets on behalf of their clients. Therefore, they are treated as financial institutions within this report.

404. The proposed rule defines two groups of advisers located within the U.S. that would be required to have AML Programs. The first group consists of advisers that: (1) have a principal office and place of business in the U.S. (U.S. advisers), (2) are registered with the SEC, and (3) report to the SEC that they have assets under management. This group includes advisers registered with the SEC that have either discretionary or non-discretionary authority to manage client assets. It excludes, however, advisers that are not registered with the SEC because they are smaller, state-registered firms that have less than USD 30 million of assets under management, as well as advisers that are registered with the SEC but do not manage client assets. Because these excluded firms, unlike many financial institutions such as banks or broker-dealers, do not accept funds or hold financial assets directly, and have relatively few (or no) assets under management, the U.S. authorities consider that these firms are unlikely to play a significant role in money laundering.

405. The second group consists of U.S. advisers that are not registered with the SEC, but have USD 30 million or more of assets under management and are relying on the registration exemption provided by section 203(b)(3) of the Advisers Act [15 USC 80b–3(b)(3)] (unregistered advisers). Under this section, advisers that have fewer than 15 clients and do not hold themselves out generally to the public as investment advisers are exempted from SEC registration. Many of the advisers that use this registration exemption may control substantial client assets, either because they have a few individual clients with very large accounts or because they advise certain types of pooled investment vehicles, such as limited partnerships. Subsequent to the proposed rule, however, the SEC adopted rules requiring hedge fund advisers to include investors in hedge funds in the count of "clients" for purposes of section 203(b)(3). As of the end of April 2006, approximately 2,400 hedge fund advisers were registered with the SEC, approximately 1,180 of them as a result of the new rules. Many of the newly registered hedge fund advisory firms may now be included in the first group of advisers. With respect to this second group of investment advisers, the proposed rule would exclude those entities that would qualify as unregistered advisers but that are otherwise required to have an AML Program under the BSA because they are dually registered as a financial institution in another capacity and are examined by a federal functional regulator for compliance with the requirement in that other capacity.

406. FinCEN is currently preparing, in consultation with the SEC, final rules relating to application of AML Program requirements to investment advisers. FinCEN also continues to consider whether investment advisers should be subject to additional BSA requirements, including filing suspicious activity reports and complying with account holder identification and verification procedures. In preparing a final rule, FinCEN is taking into consideration amended SEC rules under the Investment Advisers Act which requires investment advisers to certain pooled investment vehicles to register with the SEC.

Commodity trading advisors[57]

407. Commodity trading advisors (CTAs) are defined as "financial institutions" under the BSA, but are not currently required to implement AML Programs. In May 2003, FinCEN issued a notice of proposed rulemaking (68 FR 23640) seeking public comment on whether to impose AML Program requirements on commodity trading advisors. The proposed rule defines "commodity trading advisor" as any person registered or required to be registered with the CFTC under the Commodity Exchange Act (CEA) that directs client commodity futures or options accounts. The CEA defines a CTA generally as any person who, for compensation or profit, engages in the business of advising others, either directly or indirectly, as to the value or advisability of trading futures contracts or commodity options authorized under the CEA, or issues analyses or reports concerning trading futures or commodity options.

408. FinCEN limited the application of its proposed rule to CTAs that not only provide trading advice tailored to the circumstances of particular clients, but also direct such clients' accounts. This is because a CTA that only provides commodity trading advice, without directing the account, is not in a

[57] Commodity trading advisors are treated within this report in the same way as investment advisers.

position to actually observe potentially suspicious activity; indeed, a CTA whose service is limited to providing trading advice may not even know whether the client actually follows that advice.

409. FinCEN is currently preparing, in consultation with the CFTC, final rules relating to application of AML Program requirements to CTAs. FinCEN also continues to consider whether CTAs should be subject to additional BSA requirements, including filing suspicious activity reports and complying with accountholder identification and verification procedures.

Insurance sector

410. The issuance by FinCEN of the final rules requiring insurers to establish AML Programs and file SARs, published in November 2005, was based upon an AML/CFT risk assessment of the insurance industry. Before FinCEN published its proposed rules in 2002, Treasury and FinCEN studied the industry to make a preliminary determination as to the potential AML risks. This included reviewing existing data and analyses, meeting with industry trade associations and research groups, National Association of Insurance Commissioners representatives, and obtaining law enforcement input. Evidence suggests that most money laundering schemes involving the insurance sector have used life insurance policies or other products with investment or cash redemption features. Variations in typologies have emerged as the range of retail insurance products has expanded to include sophisticated investment options and other features that make products vulnerable to money laundering. Based upon this data, Treasury and FinCEN determined that the life insurance sector (including annuities) posed a significant risk of money laundering (and not property/casualty or health insurance).

411. Treasury and FinCEN also made a preliminary determination that the insurance distribution system, which includes independent insurance agents and insurance brokers, could most efficiently be addressed by requiring their insurance company principals to integrate them into their program, rather than imposing an independent obligation on the agents and brokers. However, it is noted that it may pose a challenge for life insurers to integrate independent insurance agents and insurance brokers into their AML programs.

412. This assessment is confirmed by the "U.S. Money Laundering Threat Assessment" which identifies that:

> "A number of money laundering methods have been used to exploit the insurance sector, primarily term life insurance policies and annuity products. Money launderers exploit the fact that insurance products are often sold by independent brokers and agents who do not work directly for the insurance companies. These intermediaries may have little know-how or incentive to screen clients or question payment methods. In some cases, agents take advantage of their intermediary status to collude with criminals against insurers to perpetrate fraud or facilitate money laundering."

413. Additionally, the U.S. authorities acknowledged in their response to the mutual evaluation questionnaire that even when insurers have AML Programs in place, agents who sell insurance policies and investment contracts often are not employed directly by the insurer or service provider, potentially making it difficult for companies to ensure their AML policies and procedures are followed. Further complicating AML practices, the policyholder, or purchaser of an insurance contract, may not be the beneficiary or even the subject of the insurance coverage. The potential for multiple parties to be involved in a single contract makes it difficult to perform customer due diligence. The inclusion of investment products with the usual portfolio of insurance policies increases the potential for insurance companies to be used as money laundering conduits. Money laundering through insurance has been generally confined to life insurance products although the actual typologies vary significantly.

414. FinCEN also determined through its risk assessment process that certain life insurance products, including group products and term insurance, do not present a significant risk of money laundering or

terrorist financing.[58] Thus, the final rules focus on those covered insurance products possessing features that make them susceptible to being used for money laundering or the financing of terrorism. As such, FinCEN's final rules cover the following insurance products:

(a) permanent life insurance policies;

(b) annuity contracts; and

(c) any other insurance products with features of cash value or investment features.

415. The insurance products that are not covered are:

(a) group life insurance policies;

(b) group annuity contracts;

(c) reinsurance and retrocession contracts;

(d) term life (which includes credit life) insurance;

(e) property and casualty insurance;

(f) health insurance; and

(g) any other kinds of insurance products to the extent that they do not exhibit features of cash value or investment features.

416. This approach does comply in substance with the FATF's 40 Recommendations that defined "financial institutions" to include "underwriting and placement of life insurance and other investment related insurance" and footnote 9 which clarified that "this applies both to insurance undertakings and to insurance intermediaries (agents and brokers)". Although agents who sell insurance products subject to the AML and SAR rules are not directly subject to those rules, the insurance companies that issue the products subject to these rules are required to integrate such agents into their AML programs and to ensure that their AML policies and procedures are followed.

417. In addition, it is important to note that many of the insurance products that involve an investment risk (i.e. products where the cash value or death benefit depend upon the investment experience of the amounts paid in under the policy) must be sold by registered securities broker-dealers who are the only persons permitted to offer certain variable insurance products on behalf of insurance companies. These persons are required to adopt and implement separate AML and suspicious activity reporting programs under separate AML regulations that apply to securities broker-dealers.

418. So far, the insurance sector is not yet subject to CIP rules that would require insurers to establish and verify the true identity of their customers. The U.S. authorities said that this was done based on a risk assessment which determined the risk as being sufficiently low to justify an exception to these requirements at this time. However, the team was not provided with a risk assessment on this issue and is, in any event, not convinced by the reasonableness of that conclusion, having regard to the other risk assessments available on the insurance sector (see, in particular, the preambles of the AML program and SAR reporting rules applicable to the insurance industry) as well as the latest U.S. Threat Assessment 2006.

Scope issues

419. As previously discussed, with respect to the banking sector, the overwhelming majority of institutions included in the category of "bank" under the BSA are subject to the full range of BSA AML requirements [e.g. recordkeeping and reporting for suspicious activities, CTRs, wire transfers, and

[58] The U.S. authorities have provided a note concerning the deliberative regulatory risk assessment process employed by Treasury in adopting AML Program, SAR and other rules to implement the BSA in respect of the insurance sector.

implementation of a Customer Identification Program (CIP)], and all but four categories (which are not significant in terms of number or of AML risk) are also subject to the AML program requirement. With respect to the securities sector, the most significant category has been subject to AML and SAR rules since 2002; while mutual funds have been required to have an AML program since 2002 and will be subject to SAR reporting in October 2006. Unregistered investment companies, investment advisers and commodity trading advisors have had proposed rules pending for some time and these are expected to be brought on line in the near future. In the life insurance sector, all those institutions issuing products posing a greater risk of money laundering are subject to AML and SAR rules beginning May 2006, and are required to integrate their agents into their AML programs.

420. These gaps in the scope of the AML obligations affect the ratings relative to some of the Recommendations discussed in section 3.

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)

3.2.1 Description and Analysis

Introduction

421. The BSA is currently the cornerstone of the U.S. AML legal framework. The amendments to the BSA contained in the USA PATRIOT Act (signed into law on 26 October 2001) were the most significant of recent amendments in a series of legislative acts intended to codify and enhance the U.S. response to money laundering. The law was expanded significantly to require application of AML safeguards to a number of businesses beyond depository financial institutions. The term "financial institution" is very broadly defined in the BSA (31 USC 5312) to include:

- insured banks (1)
- commercial banks or trust companies (1)
- private bankers (5)
- agencies or branches of foreign banks in the U.S. (1)
- credit unions (1)
- thrift institutions (1)
- brokers or dealers registered with the SEC (1)
- brokers or dealers in securities or commodities (1)
- investment bankers or investment companies [includes mutual funds (1) and unregistered investment companies (2)]
- currency exchanges (1)
- issuers, redeemers or cashiers of travelers' checks, money orders or similar instruments (1)
- operators of a credit card system (1)
- insurance companies (1)
- dealers in precious metals, stones or jewels (1)
- pawnbrokers (3)
- loan or finance companies (3)
- travel agencies (4)
- money services businesses (MSBs), including persons engaged in providing informal remittance services (1)

- telegraph companies
- businesses engaged in vehicle sales, including automobile, airplane and boat sales (4)
- persons involved in real estate closings and settlements (4)
- the U.S. Postal Service (1)
- agencies of the U.S. government or of a state or local government carrying out a duty or power of a listed business
- casinos or gaming establishments (including Indian gaming operations) with an annual gaming revenue of USD 1 million (1)
- any business or agency that engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, or a substitute for any activity in which any of the above businesses is authorized to engage.
    - Futures commission merchants (1)
    - Commodity trading advisors (2)
    - Commodity pool operators (2)
    - Investment advisers (2) (Treasury/FinCEN has issued a proposed AML rule determining investment advisers to be financial institutions)

    Key:

    (1) Subject to AML rule and other AML requirements

    (2) Proposed AML rule issued

    (3) AML/CFT risk analysis completed, proposed rule to be issued

    (4) Advance notice of proposed rulemaking issued, risk analysis ongoing

    (5) Only one "private banker" (as that term is described in the discussion under Recommendation 5) is known to exist, and it is subject to some BSA AML requirements and to examination by the New York Stock Exchange and the New York State Banking Department.

    (No number indicates no AML rule planned due to a determination by the U.S. authorities that these activities pose a low risk of money laundering, or to the fact that no such entities are known to exist).

422. The application of the BSA requirements to these financial activities is subject, in all cases, to the promulgation of implementing regulations. A number of these institutions have been subjected to AML program requirements since enactment of the BSA, and more have been incorporated since the enactment of the USA PATRIOT Act. Proposed rules have been issued and are pending, following risk assessments performed with respect to certain types of institutions. In other cases, FinCEN intends to issue proposed rules or is still conducting a risk analysis. For those sectors where AML program requirements have not yet been introduced, Form 8300 reporting requirements apply to those industries, which is a BSA requirement (31 CFR 103.30) (see section 3.7 of this report for a more detailed description of these requirements).

423. Subject to the promulgation of implementing regulations for specific categories of business, financial institutions are required (under the amendment introduced by section 352 of the USA PATRIOT Act) to establish an AML Program, which, at a minimum, must include: (1) development of internal policies, procedures, and controls; (2) designation of a compliance officer; (3) an ongoing employee training program; and (4) an independent audit function to test programs. Rules were issued in 2002 stating that institutions subject to regulation by a federal functional regulator (i.e. the Federal Banking Agencies, the SEC and the CFTC) or a self-regulatory organization (SRO) would meet this

requirement if they complied with equivalent provisions specified by their regulators. The Federal Banking Agencies had previously issued regulations in relation to BSA compliance (e.g. in respect of the Federal Reserve Board under 12 CFR 208.63). The SROs issued AML program rules applicable to securities broker-dealers, futures commission merchants and futures introducing brokers in 2002. FinCEN has issued separate AML Program requirements for credit card operations, MSBs, mutual funds, insurance companies, and dealers in precious metals, stones and jewels, and has proposed AML rules for unregistered investment companies, investment advisers, and commodity trading advisors.

424. Financial institutions subject to AML program rules are required to establish and implement "policies, procedures, and internal controls reasonably designed to achieve compliance with the BSA and the implementing regulations thereunder." Regulators generally interpret this to require customer identification and verification, monitoring of transactions, and reporting of suspicious activity to appropriate authorities, all as required or appropriate. In addition, section 326 of the USA PATRIOT Act mandated the promulgation of regulations establishing minimum standards for financial institutions regarding the identification of customers opening new accounts at financial institutions. The implementing regulations require those financial institutions for which account relationships actually exist to implement reasonable CIP procedures for: (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (3) determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.

425. FinCEN, in conjunction with other federal regulators, has issued CIP final rules for banks (both federally and state regulated), savings associations (thrifts), trust companies, credit unions, securities broker-dealers, futures commission merchants, introducing brokers, and mutual funds (or open-end investment companies). These rules impose specific requirements in terms of the information that must be gathered at the account-opening stage (see discussion in the banking section below). In January 2006, FinCEN also issued final rules requiring special due diligence with respect to correspondent banking and private banking accounts for non-U.S. persons, including PEPs.

426. In implementing its AML requirements generally, the U.S. uses a risk-based approach to the extent that this is not overridden by the prescriptive requirements under the USA PATRIOT Act. This risk-based approach is coupled with supervision, regulatory oversight and enforcement by the supervisory agencies. The FFEIC Manual (pp. 37-39) expressly provides that the cornerstone of a strong BSA/AML compliance program is the adoption and implementation of comprehensive customer due diligence (CDD) policies, procedures and processes for all customers, particularly those that present high risk for money laundering and terrorist financing. The risk-based approach for CDD requires that policies and procedures should focus on higher risk areas and customers within an institution, based on that individual institution's assessment of the overall AML/CFT risk within its business. This risk assessment should weigh a number of factors, including the risk identification and measurement of products and services offered, volume of business, nature and demographic of customer base, and geographic locations, and it should assist the institution in effectively managing its AML/CFT risks.

427. Due to the wide variety and disparity of financial institutions and financial products and services offered, this risk-based approach is widely supported by financial industry, although some smaller institutions (and some of the business lines within the larger organizations) have expressed a preference to have greater certainty (i.e. more specific rules) on some of their obligations. In discussions with individual institutions, it was apparent that a considerable amount of effort and investment is currently being put into developing risk-based models and procedures. One of the primary challenges cited by the industry is the need to balance their business needs with the required risk assessment, including the risk that they see of regulatory action resulting from a divergence of view between the institution and its regulators on the effectiveness of the risk mitigation. In this

context, it should be noted that the regulatory agencies have made considerable efforts to provide appropriate guidance to certain parts of the financial sector.

Recommendation 5 (Customer identification and due diligence)

428. For ease of reference in the following discussion of CDD, unless otherwise specified, the term "bank" is used to cover all banks (whether federally or state regulated), thrifts, trust companies and credit unions; while "securities" is used to encompass broker-dealers, futures commission merchants, introducing brokers and mutual funds.

Banking sector

429. The application to the banking sector of the various AML and customer identification program requirements is described in the table below. This should be referenced in the following discussion of the CDD requirements for the banking sector.

Type of Institution (Including Approximate Number)	BSA Regulations*	AML Program	CIP	Correspondent and Private banking	Shell Bank Dealings
Insured, federally-regulated banks (including federally regulated trust companies) (8960)	Yes	Yes	Yes	Yes	Yes
Uninsured national trust company (90)	Yes	Yes	Yes	Yes	Yes
Uninsured, non-federally regulated trust company (113)	Yes	No	Yes	No	Yes
Insured, federally-regulated savings association (862)	Yes	Yes	Yes	Yes	Yes
Uninsured, non-federally regulated bank or savings association (7)	Yes	No	No	No	No
Federally Insured, federally-regulated credit union (8695)	Yes	Yes	Yes	Yes	Yes
Privately insured, non-federally regulated credit union (319)	Yes	No	Yes	N/A	Yes
Foreign bank branches and agencies (269)	Yes	Yes	Yes	Yes	Yes
Private Banking Group/Partnership (1)	Yes	No	Yes	No	Yes
Edge Act corporations (79)	Yes	Yes	Yes	Yes	Yes

*Includes requirements to file suspicious activity and currency transaction reports and maintain all BSA records, including check purchases and fund transfers above USD 3000 and records of all other required transactions.

430. Since 1987, all federally regulated banks have been subject to an AML program requirement prescribed by their federal regulator. These institutions comprise the overwhelming preponderance of all depository institutions in the U.S. by both numbers and size.

431. However, there are currently the following four categories of non-federally insured state chartered banks in the U.S. which are not subject to an AML program requirement:

(1) According to information provided by the National Association of State Credit Union Supervisors, 319 privately insured credit unions are chartered in nine states and territories. These are small institutions that offer accounts only to members of a group who share a "common bond." Their state regulators use the same AML examination procedures for them as for other banks that they examine, and generally take the position that, in order to comply with these requirements, they must implement an AML program, just like that required for federally insured credit unions and other banks.

(2) Based on a recent survey conducted by the CSBS, there are estimated to be approximately 113 state chartered non-depository trust companies in the U.S.[59] These entities, which are more like investment advisors than banks, are typically smaller than depository trust companies and provide investment management, estate planning and trust administration services. They cannot accept deposits, maintain transaction accounts, or execute wire transfers. All of these entities are subject to examination by their state banking department for compliance with the applicable AML requirements.

(3) There is only one known private banking group/partnership currently operating in the U.S. It operates one private banker that is chartered, regulated, and examined for AML compliance by the New York Banking Department and one private bank that is chartered, regulated and examined by the Pennsylvania Department of Banking. The group/partnership is also a member of, and is subject to the AML rules of and examined for AML compliance by, the NYSE.

(4) Based on a recent survey conducted by the CSBS, there appear to be seven active uninsured state chartered banks in the U.S., of which six are savings and loan or building and loan associations and one is owned by the state of North Dakota. All of them are examined by their state regulator for AML compliance. Additionally, the activities of these entities are generally restricted and, with the exception of the state-owned bank, they are generally small in size.

432. The U.S. approach to dealing with certain types of depository institutions in different ways, which has an historical basis, results in the appearance of an excessively complex system. For instance, there seems to be no compelling reason why certain non-federally regulated institutions are subject to all of the individual BSA requirements (including filing SARs and implementing a CIP), but are exempt from the AML Program obligation. This appears at odds with the concept, generally stated by the authorities, that the CIP has normally to operate within the framework of the AML Program. However, the authorities justify this on the following grounds. First, in order to comply with all of the AML requirements to which these institutions are subject, as a practical matter they would have to establish a program substantially similar to the type of AML program required of the federally regulated banks. (In fact, this is the position taken by the states that charter and examine the privately insured credit unions that make up the largest group of these entities.) Second, as discussed above, due to the inherent restrictions on the activities of these entities and their generally small size, they present a relatively low money laundering risk. Nevertheless, FinCEN intends to amend its regulations to eliminate this regulatory anomaly to bring uniformity to the banking sector.

433. **Anonymous accounts:** There is no explicit prohibition on the maintenance of anonymous accounts or accounts in fictitious names. However, the CIP rules require an institution to have procedures that enable it to form a reasonable belief that it knows the true identity of each customer. Therefore, the effective implementation of these rules should preclude such accounts from being opened.

434. The BSA requires financial institutions to identify and verify the identity of customers that open an account. In addition, financial institutions must identify and verify the identity of customers undertaking certain transactions whether or not an account at the financial institution is involved. This transaction-based identification and verification arises when customers engage in large currency transactions, the purchase of certain financial instruments, or certain wire transfers. The details of account-based and transaction-based identification and verification are discussed below.

435. **When establishing business relations:** The statutory requirement on account-opening procedures has been implemented through regulations (31 CFR 103.121 for banks) issued jointly by FinCEN and the regulatory agencies. In the case of the banking sector, an account is defined to mean "a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account or other extension of credit",

[59] Because several states did not respond to the CSBS survey, the actual number could be greater.

and it is further defined to include "a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian, and trust services".

436. The regulations require covered financial institutions to implement a written CIP. The CIP must be part of the financial institution's AML Program required by the BSA. Specifically, the CIP "must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practical", and "must enable the (institution) to form a reasonable belief that it knows the true identity of each customer". Further, the regulations require that procedures must be based on the institution's assessment of the risks presented by the various types of accounts it maintains, the various methods it provides for opening accounts, the type of identifying information available, and the institution's size, location and customer base. The CIP must also include procedures for responding to circumstances in which the financial institution cannot form a reasonable belief that it knows the true identity of a customer.

437. While the regulations generally emphasize the need for a risk-based approach to customer identification, they specifically require that, as part of its CIP, a financial institution must collect (at a minimum) the following identifying information about a customer at the time the customer seeks to open the account: (1) name; (2) for individuals, date of birth; (3) for individuals, a residential or business street address, or, if there is no street address available, an Army Post Office or Fleet Post Office box number or the street address of next of kin or of another contact individual; or, for persons other than individuals, the principal place of business, local office or other physical location; and (4) for U.S. persons, a U.S. taxpayer identification number; or, for non-U.S. persons, one or more of the following: a U.S. taxpayer identification number, passport number and country of issuance; alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

438. The CIP must also contain documented procedures for verifying the identity of customers within a reasonable time after the account is established. The regulations specify that verification may be done through documentary or non-documentary methods or a combination of the two. They further specify that, for individuals, documentary verification may be completed using such items as an unexpired, government-issued photo-identification card evidencing nationality or residence (e.g. passport or drivers license). For persons other than an individual, reliance may be placed on documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument. Non-documentary methods specified by the regulations include verifying identity through the comparison of the information from the customer with information from a consumer reporting agency, public database or similar source. The non-documentary procedures are also required to address the situation where some of the basic identification documents may not be available or may be unfamiliar to the institution.

439. **When carrying out occasional transactions:** The BSA requires financial institutions to report to FinCEN "each deposit, withdrawal, exchange of currency or other payment or transfer, by, through or to such financial institution which involves a transaction in currency of more than USD 10,000" (31 USC 5313 and 31 CFR 103.22). Such reports are filed on a CTR form (FinCEN Form 104). The customer identification requirements in making such filings are described in section 3.7 of this report.

440. **When purchasing certain financial instruments:** Financial institutions must also keep records and identifying information pertaining to the sale of bank checks, drafts, cashier's checks, money orders, and traveler's checks in excess of USD 3,000 in currency (3 CFR 103.29). Verification, in the case of an existing account holder, may be either through a signature card or other file or record at the financial institution, provided the account holder's name and address were previously verified, or by examination of a document that is normally acceptable within the banking community as a means of identification when cashing checks for non-depositors. If the purchaser does not have a deposit account with the financial institution, the institution is required to record the name and address of the purchaser, the social security or alien identification number and date of birth, and must verify the name and address by examination of a document which is normally acceptable within

the banking community as a means of identification when cashing checks for non-depositors and which contains the name and address of the purchaser, and the institution must also record the specific identifying information, such as state of issuance and number of driver's license.

441. **When carrying out wire transfers:** The BSA authorizes Treasury to issue regulations requiring financial institutions to keep records of wire transfers. These regulations (31 CFR 103.33) require records to be maintained of wire transfers by non-customers of USD 3,000 or more. Financial institutions must record the name, address and taxpayer or alien identification number, and verify the identity of the person placing the payment order (if made in person) and of the person to whom the proceeds of the wire are delivered (if delivered in person). Verification is by examination of a document (other than a customer signature card). The document, preferably one that contains the person's name, address, and photograph, must be one that is normally acceptable by financial institutions as a means of identification when cashing checks for persons other than established customers (see the extended discussion in section 3.5.1 on Special Recommendation VII).

442. The primary focus of the occasional transaction regime under the BSA is cash. With the exception of the specific provisions on the purchase of certain monetary instruments and on wire transfers, there are no requirements in the legislation in relation to occasional non-cash transactions of any size undertaken by, or on behalf of, persons who do not have an ongoing business relationship

443. **When there is a suspicion of money laundering:** There is no legal obligation to review the CDD process when an institution has suspicions that a customer may be engaged in money laundering. However, if a bank's CDD information is incorrect or contrary to actual experience with a particular customer, the bank would be expected to investigate and update its CDD information accordingly. Allowing inadequate or inaccurate CDD information may be considered a compliance program deficiency. Should a bank have suspicions that a customer is engaged in money laundering, then it should investigate the circumstances and consider filing a SAR consistent with its SAR policy and the SAR regulations.

444. **When there are doubts about the veracity/adequacy of previously obtained customer identification data:** The CIP must include procedures for responding to circumstances in which the financial institution cannot form a reasonable belief that it knows the true identity of a customer [31CFR 103.121(b)(2)(ii)]. These procedures are required to address circumstances when the institution should not open the account, or, if already opened, when it should close it; the terms under which a customer may use the account pending verification of identity; and the circumstances under which it should file a SAR. Guidance is also contained in the FFIEC Manual (pp. 33-34). In principle under this provision, if the institution has doubts about the veracity or adequacy of previously obtained customer identification data, then it cannot have a reasonable belief as to the true identity of its customer under the regulation, and must take additional steps to verify the customer's identity or terminate the account relationship.

445. **Legal persons, legal arrangements and beneficial ownership:** The CIP rule is a critical part of a bank's AML/CTF compliance program and effective CDD. The concept of CDD begins with verifying the customer's identity and assessing the risks presented by that customer. The CIP rule (31 CFR 103.121 for banks) defines "customer" to include only (a) a person who opens a new account and (b) an individual who opens a new account for (1) an individual who lacks legal capacity, such as a minor, and (2) an entity that is not a legal person, such as a civic club. Therefore, the customer is essentially the individual or entity in whose name the account is opened. In general, the CIP rules do not require a financial institution to look through a customer that is an entity to its beneficial owners. However, the preamble to the final rule implementing section 326 of the USA PATRIOT Act provides that, based on a bank's risk assessment of a new account opened by a customer that is not an individual, a bank may need to take additional steps to verify the identity of the customer by seeking information about individuals with ownership or control (including beneficial owners) over the account in order to identify the customer [e.g. 31 CFR 103.121(b)(2)(ii)(C) for banks] or may need to look through the account in connection with the customer due diligence procedures required under

other provisions of its BSA compliance program. In addition, as noted below, the Federal Banking Agencies have issued detailed "frequently asked questions" (FAQs) that provide guidance concerning the term "customer" and related beneficial ownership issues concerning trust accounts, escrow accounts and powers of attorney.

446. Because of the risk based system in the U.S., the CIP rules do not require the bank to verify the identity of a signatory for every account where the account may be held in a corporate name. An original proposal to require this was withdrawn following opposition from the banking industry on the grounds of relevance and administrative burden. For persons other than an individual, the financial institution is required to establish its principal place of business, local office or other physical location, and a taxpayer identification number (in the case of U.S. entities) or some other government-issued identifier (in the case of non-U.S. entities). As means of verification, the institution must obtain documents that show the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument [e.g. 31 CFR 103.121(b)(4)(ii)(A) for banks]. Other than as noted above, there is no other specific reference in this provision to the concept of beneficial ownership, and there is no elaboration on what the additional information specified might include.

447. The only statutory requirements to identify the beneficial owner before or during the course of establishing a business relationship appear in sections 311 and 312 of the USA PATRIOT Act. Section 311 permits the Secretary of the Treasury to require institutions to obtain and retain information on the beneficial ownership of any account opened or maintained in the U.S. by a foreign person (other than a listed company) resident in a country that the Secretary has designated to be of primary money laundering concern (see further discussion under Recommendation 21 in section 3.6 of this report).

448. Section 312 sets minimum due diligence requirements for a private banking account opened for a non-U.S. person only. Specifically, "a financial institution must take reasonable steps to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, the private banking account, as necessary to guard against money laundering and to enable it to report suspicious transactions". Section 312 also requires a bank to identify the owners of certain non-U.S. banks for which correspondent facilities are being provided (see discussion under Recommendation 7 below). Section 312 was self-implementing in July 2002 even though FinCEN was unable to issue a final rule by that time. An interim final rule published that month deferred application of the rule to some categories of depository institutions, and required others to apply a risk-based approach to implementing the strict provisions of section 312, while paying attention to regulatory guidance, specifically a paper issued by the Federal Reserve in June 1997, entitled "Private Banking Activities".

449. On 28 April 2005 FinCEN and the Federal Banking Agencies published inter-agency guidance (in the form of FAQs) to the banking sector on various CIP issues [e.g. Federal Reserve Supervision and Regulation Letter (SR) 05-9]. The banks may reasonably rely on this guidance in relation to trust, escrow and power-of-attorney accounts. In the case of trust accounts, the "customer" is stated to be the trust, whether or not the financial institution is the trustee for the account. A financial institution will not be required to look through the trust to verify the identities of the beneficiaries, and instead will only be required to verify the identity of the named accountholder. A similar principle is stated with respect to escrow accounts, where the person who opens the account is deemed to be the customer, and not the underlying owner of the funds. However, the additional verification principle applies (as for corporate entities) if, based on the financial institution's risk assessment, it considers it necessary to obtain additional information in order to verify the customer's identity. The guidance states that, in certain circumstances, for example, involving revocable trusts, the financial institution may need to gather information about the settler, grantor, trustee, or other persons with the authority to direct the trustee, and who thus have authority or control over the account, in order to establish the true identity of the customer. This additional verification method will apply only when the financial institution cannot adequately verify (to its satisfaction) the customer's identity using the documentary or non-documentary methods described in the CIP regulation

450. With respect to an account opened by an individual who has power-of-attorney (or other agency designations) for a competent person, the guidance specifies that the "customer" will be the named owner of the account rather than the individual with a power-of-attorney who is regarded merely as an agent. By contrast, an individual with power-of-attorney will be the "customer" if the account is opened for a person who lacks legal capacity [e.g. 31 CFR 103.121(a)(3)(i)(B)(1) for banks].

451. In July 2002, FinCEN issued an Interim Final Rule implementing, for certain financial institutions, the correspondent and private banking provisions of section 312. On 4 January 2006, FinCEN issued a final rule refining and expanding the application of the regulatory requirements under section 312. The private banking provisions of the final rule apply to depository institutions, securities broker-dealers, futures commission merchants and introducing brokers, and mutual funds, and relate only to private banking accounts held by non-U.S persons, where the institution itself requires a minimum aggregate deposit of funds or other assets of not less than USD 1 million dollars. In this context alone, the final rule issued under Section 312 requires institutions to identify both the nominal and beneficial owner of an account. The beneficial owner of an account is defined as:

> "an individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, however, without corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner."

452. Thus, the term excludes those who have a financial interest in the account and no corresponding ability to "control, manage or direct" the funds in the account.

453. FinCEN has provided further guidance as to what measures it expects institutions to take, as follows:

> "We expect that covered financial institutions will look through the nominal owner of the account to determine who has effective control over the account. For example, when an account is opened by a natural person, the financial institution should establish whether the client is acting on his or her own behalf and should perform additional diligence if doubt exists as to the identity of the beneficial owner(s). For an account holder that is a legal entity that is not publicly traded (such as a private investment company), a financial institution should ensure that it has sufficient information about the structure of the entity, including its directors, shareholders, and those with control over the account, and should determine which individual (or individuals) constitutes the beneficial owner(s) for purposes of due diligence. Likewise, in the case of a trust, the financial institution should ascertain which individual (or individuals) controls the funds of the trust, should identify the source of the funds, and should perform due diligence as appropriate."

454. The final rule will become effective on 5 July 2006 for private banking (and correspondent banking) accounts opened after that date, and will become effective on 2 October 2006 for accounts opened prior to 5 July.

455. The practices adopted by the sample of banks interviewed during the evaluation varied in relation to the identification of beneficial ownership. Generally, the larger banks appear to apply the risk-based approach, and seek to drill down to the beneficial owner only in the case of certain structures specified within their risk framework. Personal investment companies and trusts were typically identified as triggering such action, while commercial and other businesses would not, unless there were exceptional circumstances. On the other hand, the smaller banks indicated that their general practice was to identify beneficial ownership as a matter of course. The difference in practice may be determined by the scale, risk assessment and diversity of the respective products, services and customer bases, rather than conservatism on the part of the smaller banks.

456. **Purpose for the account:** There is no specific requirement within the CIP rules that financial institutions should obtain information on the purpose and intended nature of the business relationship. However, page 38 of the FFIEC Manual states that:

> "Management should have a thorough understanding of the money laundering or terrorist financing risks of the bank's customer base. Under this approach, the bank will obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations."

457. The FFEIC Manual also provides a more specific list of information and documents that might be expected in the case of a high-risk customer, both at account opening and throughout the relationship, including the purpose of the account, the customer's occupation or type of business, and description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers.

458. **Ongoing due diligence:** There is no explicit legal requirement to undertake ongoing due diligence in all cases. However, the U.S. authorities interpret the SAR reporting obligations as necessarily requiring institutions to have policies and procedures in place to undertake ongoing due diligence generally. This is based on the fact that the SAR regulations require financial institutions to report any transaction that "is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts . . ." (31 CFR 103.18(a)(2)(iii)). Consequently, the authorities argue this presupposes the existence of ongoing customer due diligence in order for the institution to be able to know what sort of transactions the customer normally undertakes.

459. There are specific requirements only with respect to correspondent banking and private banking, including PEPs. Title 31 CFR 103.178(b)(4) requires each covered financial institution that has a qualifying private banking account to "review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds, and with the stated purpose and expected use of the account, as needed to guard against money laundering, and to report, in accordance with applicable law and regulation, any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking account."

460. The AML Program requirements are risk-based, and so a financial institution's AML policies, procedures, and processes are expected to include guidelines that are commensurate with the financial institution's AML risk profile, paying particular attention to high-risk customers. For the banking sector the FFIEC Manual states generally (p.38) that "CDD procedures should include periodic monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information (e.g. change in employment or business operations)"; and that (p.37) "procedures should include enhanced CDD for high-risk customers and ongoing due diligence of the customer base". The essential components of CDD policies and procedures are also deemed to include processes to "ensure that the bank maintains current customer information". For high-risk customers, there is an expectation that "customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank" (p.38). Allowing inadequate or inaccurate CDD information may constitute a compliance program deficiency.

461. Banks have an obligation to report both suspicious transactions and certain transactions over designated thresholds. To comply with this obligation, they are expected to establish and maintain systems that will permit them to monitor transactions under risk-based procedures. According to the FFIEC Manual (p.41) "the level of monitoring should be dictated by the bank's assessment of risk, with particular emphasis on high-risk products, services, customers and geographic locations".

462. The FATF standard on ongoing monitoring of accounts requires the obligation to be framed explicitly in law or regulation. At present, the U.S. relies on the regulatory guidance (which is considered to be "other enforceable means") and on a reasonable expectation that, in order to comply

with the SAR requirements, institutions will have to undertake account monitoring on a risk-sensitive basis. The regulators enforce this expectation and will cite the failure to have effective SAR identification procedures as a cause of concern (or violation of law or regulation i.e. 12 CFR 21.11) during examinations. Therefore, in practice it appears reasonable to rely upon an institution fulfilling the SAR obligation coupled with its CDD obligation to understand the customer and routine transactions as the basis for its undertaking ongoing monitoring processes.

463. **Customer risk:** The anti-money laundering program requirements that apply to U.S. financial institutions are risk-based, requiring institutions to have CDD procedures commensurate with the risk in the business identified by management. To complement this approach, the U.S. has also enacted legislative measures against certain potential higher risk scenarios, requiring enhanced CDD in such cases, thereby strengthening the effectiveness of the AML requirements (e.g. sections 311-313 of the USA PATRIOT Act, dealing with jurisdictions of primary money laundering concern, correspondent accounts and private banking accounts for foreign customers, and shell banks).

464. Under the regulations, a financial institution's CIP must enable it to have a reasonable belief that it knows the true identity of a customer. To establish a CIP, the regulations [e.g. 31 CFR 103.121(b)(2) for banks] require a financial institution to assess relevant risks, including those presented by the various types of accounts maintained by the institution, the various methods of opening accounts provided by the institution, the various types of identifying information available, and the institution's size, location, and customer base. The FFIEC Manual (pp.19-21) provides guidance to banks on the factors that should be taken into account in the risk assessment. These factors include the nature of the customer's business activity, occupation, or anticipated transaction activity, the range of products and services and the geographic location. Furthermore, the FFEIC Manual provides lists of what may be high-risk situations under these categories.

465. Potentially higher risk customers are identified in the FFEIC Manual to include: foreign financial institutions, non-bank financial institutions, senior foreign political figures, non-resident aliens and other non-U.S. persons, foreign corporations with transaction accounts, particularly offshore corporations located in high-risk jurisdictions, deposit brokers (particularly foreign), cash-intensive businesses, non-governmental organizations and charities, and professional service providers. Examples cited of potentially higher-risk products include: electronic funds payment services, electronic banking, private banking, trust and asset management services, monetary instruments, foreign correspondent accounts, international trade finance (letters of credit), special use or concentration accounts, lending activities, particularly loans secured by cash collateral, marketable securities, and credit card lending, and non-deposit account services. Examples of high-risk geographic locations include: countries subject to OFAC sanctions, countries identified as supporting international terrorism, jurisdictions of primary money laundering concern, NCCTs and offshore financial centers.

466. With respect to trusts and other agency accounts, guidance contained in the FFIEC Manual (p.150) suggests that banks should assess account risk based on factors that could include: (1) the type of trust or agency account and its size; (2) the types and frequency of transactions; (3) the country of residence of the principals or beneficiaries, or the country where established, or source of funds; and (4) accounts and transactions that are not usual and customary for the customer or for the bank. Based on this assessment, the banks are advised that enhanced due diligence may be appropriate in situations such as those where the financial institution is entering into a relationship with a new customer; the account principals or beneficiaries reside in a foreign jurisdiction, or the trust or its funding mechanisms are established offshore; international funds transfers are conducted, particularly through offshore funding sources; accounts or relationships are maintained in which the identities of the principals, or beneficiaries, or sources of funds are unknown or cannot easily be determined; accounts benefit charitable organizations or other non-governmental organizations (NGOs) that may be used as a conduit for illegal activities; account assets include personal investment companies; and PEPs are parties to any accounts or transactions.

467. The FFIEC Manual specifies that "due diligence policies, procedures and processes should be enhanced" in respect of high risk customers. Further guidance (pp.38-39) recommends that, in such cases, banks "should consider obtaining" the following information both at account opening and throughout the relationship: (1) purpose of the account; (2) source of funds and wealth; (3) beneficial owners of the accounts, if applicable; (4) customer's (or beneficial owner's) occupation or type of business; (5) financial statements; (6) bank references; (7) domicile (where the business is incorporated); (8) proximity of the customer's residence, place of employment, or place of business to the bank; (9) description of the customer's primary trade area and whether international transactions are expected to be routine; (10) description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers; and (11) explanations for changes in account activity.

468. Section 312 of the USA PATRIOT Act amended the BSA to add a new provision that requires each U.S. financial institution that establishes, maintains, administers, or manages a correspondent account or a private banking account in the U.S. for a non-U.S. person to subject such accounts to certain additional AML measures (see more detailed discussion below under Recommendations 6 and 7). In particular, financial institutions must establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to enable the financial institution to detect and report instances of money laundering through these accounts. Section 312 sets minimum due diligence requirements for a private banking account for a non-U.S. person. Specifically, "a financial institution must take reasonable steps to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, the private banking account, as necessary to guard against money laundering and to enable it to report suspicious transactions". The interim final rule, issued in July 2002, directed institutions to apply a risk-based approach to dealing with non-US private banking clients, and to adopt a program consistent with guidance issued previously by the federal banking regulators, specifically the 1997 paper on "Private Banking Activities".

469. The final rule was published on 4 January 2006. This requires certain financial institutions to establish, as a part of the institution's general AML program, risk-based due diligence policies, procedures and internal controls for private banking accounts involving non-US persons, which, at a minimum, must include procedures to:

(a) identify the beneficial owner of non-U.S. private banking accounts (see discussion of beneficial ownership above)

(b) ascertain whether the account holder or beneficial owner is a senior political person (see discussion of PEPs below)

(c) ascertain the source of funds, and the purpose and expected use of the account; and

(d) review the account to ensure that its operation is consistent with the information obtained about the source of funds.

470. The rule comes into effect on 5 July for accounts opened on or after that date, and on 2 October 2006 for accounts opened prior to 5 July.

471. **Reduced CDD:** In terms of reduced CDD options, the CIP rules explicitly do not apply with respect to certain easily identifiable customers, specifically U.S. or State government entities, financial institutions regulated by a federal functional regulator, banks regulated by a state regulator, and entities whose stock is listed on the NYSE, the American Stock Exchange and the NASDAQ, provided that, if the entity is a financial institution, the exemption applies only to its U.S. domestic operation (dealings with its foreign offices being subject to normal CIP procedures). In all other cases, institutions are required to apply the CIP rules on a risk-sensitive basis, subject to the minimum requirements laid down in the regulations (see above).

472. U.S. regulators have chosen not to designate specific countries where reduced due diligence may be applied. However, they have listed the types of geographic locations that are to be considered

high risk, where enhanced due diligence would be appropriate and necessary. These locations would not include jurisdictions that subject their financial institutions to requirements consistent with the FATF Recommendations. Under the CIP rules financial institutions must assess the potential risks of their customer base and formulate their own risk-based CDD policies. According to the guidance provided in the FFIEC Manual the geographic location of the customer is a factor to be taken into account in assessing the level of risk.

473. The approach to customer risk for AML purposes is something that is clearly engaging the banks in considerable reflection and work. All of the banks interviewed were seeking to develop automated systems, of varying degrees of complexity, to provide at least an initial filter for their account opening and monitoring procedures. The concern expressed by some (including some regulators, based on their examination experience) was the uncertainty of the quality of output from such systems. Undoubtedly, all the institutions have practical problems of identifying the higher risk customers, and many are seeking to make their systems more sensitive to a range of variables, while hoping for further guidance from the regulators on specific instances of what they consider to be higher risk categories.

474. **Timing of verification:** There is no statutory obligation to complete the verification process before or during the establishment of the relationship. Instead, financial institutions are required to verify the identity of their customers "within a reasonable time after the account is opened" (e.g. 31 CFR 103.121 for banks). In finalizing this rule the Treasury noted that the amount of time it may take to verify the customer's identity may depend on a variety of factors, such as the type of account opened, whether the customer is physically present when the account is opened, and the type of identifying information available. Thus, financial institutions have been given some flexibility in when they complete the verification process. In practice, the financial industry interprets "reasonable time" to mean up to 30 days, and the authorities have concurred with this view.

475. The authority to verify the identity of the customer after the establishment of the business relationship is granted generally, and is not predicated on an essential need not to interrupt the normal course of business. There are no restrictions imposed, by regulation, on the operation of the account pending completion of the verification process. However, the rules require that the financial institution's CIP must include risk-based procedures for responding to circumstances in which the financial institution cannot form a reasonable belief that it knows the true identity of the customer. These procedures should describe: (1) when the bank should not open an account; (2) the terms under which a customer may use an account while the bank attempts to verify the customer's identity; (3) when the bank should close an account, after attempts to verify the customer's identity have failed; and (4) when the bank should file a SAR in accordance with applicable law and regulation. In addition, the preamble to the final rule notes that a bank may maintain an account at the direction of a law enforcement or intelligence agency, even though the bank does not know the true identity of the customer. It may constitute a compliance program deficiency and a violation of the CIP rule if the terms for maintaining accounts pending the verification of a customer's identity were unreasonable. [31 CFR 103.121(b)(2)(iii) for banks].

476. The preamble to the rule states that the rule does not specifically require a bank to close the account of a customer whose identity the bank cannot verify, but instead leaves this determination to the discretion of the bank (68 FR 25101). The preamble notes certain concerns raised by financial institutions that to require closure would violate certain state regulatory and borrower liability laws governing consumer rights. However, these concerns may be overstated in light of the fact that bank account relationships in the U.S. are not a right or entitlement, and that financial institutions may terminate account relationships subject to the terms of their agreements with customers and applicable law.

477. This flexibility for verification procedures is not provided in the case of specified occasional transactions involving cash transactions in excess of USD 10,000, the purchase for cash of certain financial instruments in excess of USD 3,000 (bank checks and drafts, cashier's checks money orders

and travelers' checks) and wire transfers in excess of USD 3,000. In these cases, the verification must be completed prior to the completion of the transaction.

478. **Treatment of existing customers:** The general provisions of the CIP are not retroactive. For the purposes of the CIP, a customer is defined specifically to exclude "a person who has an existing account with the (institution), provided that the (institution) has a reasonable belief that it knows the true identity of the person" [e.g. 31 CFR 103.121(a)(3)(ii)(C) for banks]. Therefore, there is no obligation to apply the formal CIP procedures to such customers, subject to the proviso being met. According to guidance provided by the Federal Banking Agencies on 28 April 2005 (SR 05-9 issued by the Federal Reserve Board) this principle applies also when an existing client opens a new account with the same institution. In the same guidance, the agencies indicated their interpretation as to how an institution could demonstrate that it had a reasonable belief that it knows the true identity of an existing customer, as follows:

> "Among the ways a bank can demonstrate that it has "a reasonable belief" is by showing that prior to the issuance of the final CIP rule, it had comparable procedures in place to verify the identity of persons that had accounts with the bank as of October 1, 2003, though the bank may not have gathered the very same information about such persons as required by the final CIP rule. Alternative means include showing that the bank has had an active and longstanding relationship with a particular person, evidenced by such things as a history of account statements sent to the person, information sent to the IRS about the person's accounts without issue, loans made and repaid, or other services performed for the person over a period of time. This alternative, however, may not suffice for persons that the bank has deemed to be high risk.

479. In circumstances where the institution could not demonstrate this level of knowledge of the customer's true identity, it is required by the regulations to perform the CIP procedures, as for a new customer. However, no guidance appears to have been provided on the timing of the review of existing customer files to determine whether the institution did indeed have a suitable level of comfort that it knows the customer's true identity. Existing accounts are subject to all other aspects of the AML Program required to be implemented by institutions.

480. The only provisions that must explicitly be applied retrospectively to existing customers are in relation to correspondent banking and private banking facilities provided to non-U.S. persons (section 312 of the USA PATRIOT Act). Under an Interim Final Rule issued In July 2002, the correspondent and private banking provisions of section 312 were implemented for depository institutions, and the private banking provisions of section 312 were implemented for securities broker-dealers and futures commission merchants and introducing brokers in commodities. Under the final rule issued by FinCEN on 4 January 2006, the enhanced due diligence procedures must be applied to all accounts established on or after 5 July 2006. Institutions have until 2 October 2006 to complete this.

Securities sector

481. The legal provisions that are applicable to the securities sector in relation to customer identification and due diligence are essentially the same as those described above for the banking sector.

482. The following table seeks to draw out which entities are subject to which rules addressing key elements within the CDD process:

Institution	BSA regulations apply	AML Program	CIP	Private banking (incl. PEPs)	Correspondent banking
Securities brokers - dealers registered with the SEC	Yes	Yes	Yes	Yes	Yes
Futures Commission Merchants and Introducing Brokers registered with the CFTC	Yes	Yes	Yes	Yes	Yes

Unregistered investment companies	No	No	No	No	No
Investment and Commodity trading advisers	No	No	No	No	No
Mutual Funds	Yes	Yes	Yes	Yes	Yes

483. **When establishing business relations:** The CIP requirements on account opening for securities sector participants are set out as follows: securities broker-dealers (31 CFR 103.122), mutual funds (31 CFR 103.131), futures commission merchants and introducing brokers in commodities (31 CFR 103.123). These regulations require sector participants to implement reasonable procedures to verify the identity of any person seeking to open an account, to the extent reasonable and practicable; and to maintain records of the information used to verify the person's identity. While the guidance contained within the FFIEC Manual does not apply to the securities sector, FinCEN, the SEC, and the SROs have issued guidance specific to the securities sector.

484. In the case of a securities broker-dealer, an account is deemed to include "a formal relationship with the broker-dealer established to effect transactions in securities, including, but not limited to, the purchase or sale of securities and securities loaned and borrowed activity, and to hold securities or other assets for safekeeping or as collateral". This notion does not include accounts that the broker-dealer acquires through any acquisition, merger, purchase of assets, or assumption for liabilities. Similar concepts of the account relationship are defined for other institutions within the securities sector.

485. Securities broker-dealers are also subject to SRO rules requiring them to "Know Your Customer". NASD member firms are required, under NASD Rule 3110, to

> "obtain certain information about their customers when opening an account, including the following: the customer's name and residence; whether the customer is of legal age; the signature of the registered representative introducing the account and signature of the member or partner, officer, or manager who accepts the account; and if the customer is a corporation, partnership, or other legal entity, the names of any persons authorized to transact business on behalf of the entity. Member firms are also required to make reasonable efforts to obtain the following additional information (for accounts other than institutional accounts and accounts in which investments are limited to transactions in open-end investment company shares not recommended by the member or its associated persons) prior to the settlement of an initial transaction in the account: a customer's tax identification and SSN; the customer's occupation and name and address of the employer; and whether the customer is an associated person of another member"

486. In its initial guidance to member firms on the USA PATRIOT Act (NASD Notice to Members 02-21, pages 5-7), NASD stated that securities broker-dealers are required to make reasonable efforts to obtain and verify information about a customer. If the customer is an individual, a firm will need, to the extent reasonable and practicable, to obtain and verify certain information concerning the individual's identity, such as the individual's name, address, date of birth, and government issued identification number". NASD issued later guidance to its firms when the final customer identification regulations were issued by Treasury and the SEC [NASD Notice to Members 03-34 (June 2003)]. Securities broker-dealers that are NYSE members must exercise diligence as to accounts "to learn the essential facts relative to every customer, every order, every cash or margin account accepted" (NYSE Rule 405).

487. The SEC confirmed that the overriding philosophy is that, at the time of account opening, the securities participant must know and believe who the customer is. In addition, broker-dealers must contact customers at least every three years to confirm, as applicable, the customer's name, tax identification number, address, telephone number, date of birth, employment status, annual income, net worth (excluding value of primary residence), and the account's investment objectives. [17 CFR 240.17a-3(a)(17)(B)(i)] In the case of a corporate customer, at account opening, securities participants examine the company's articles of incorporation. In the ordinary course, the initial CDD process will not go further—unless the identity of the company cannot be verified (e.g. because the company's

documentation comes from an unfamiliar jurisdiction) , the company is identified as being a high risk client, or in the course of the broker-dealer's ongoing CDD of the company's account, the company's activity appears inconsistent with its investment objectives or otherwise appears suspicious. In such cases, further CDD must take place, including, where appropriate, looking through to the ultimate beneficial owner. Securities regulators have brought enforcement actions for failure to identify beneficial owners in these circumstances (e.g. in 2005, NASD sanctioned and fined a firm for failure to determine the beneficial owners of certain Panamanian accounts carried by the firm).

488. Similarly, futures commission merchants and introducing brokers in commodities have customer identification obligations that are separate and apart from their obligations under the BSA. For example, CFTC Rules address the following issues:

- 17 CFR 1.37 requires customer identification including the true name and address of the person for whom such account is carried or introduced and the principal occupation or business of such person; name of any other person guaranteeing such account or exercising any trading control over the account;
- 17 CFR 17.01 requires enhanced due diligence for reportable accounts including omnibus accounts; identify owner and its registration, legal organization, and principal business/occupation; name and location of all persons having a ten percent or more financial interest in the account; and the names and addresses of all persons with trading authority, if there are five or fewer such persons;
- 17 CFR 18.04 requires reporting and enhanced due diligence for customers with large/reportable trading position; name, address, principal business and occupation, name and address of each person whose trading is controlled by the reporting trader; name, address and business phone of each person who controls the trading of the reporting trader; names and locations of guarantors and persons with a financial interest of 10 percent or more in the reporting trader or its accounts; and
- NFA Rules 2-30 requires customer identification including true name, address, principal occupation or business, current estimated annual income and net worth, age, previous investment and futures trading experience.

489. **Financial intermediary accounts:** Securities brokers-dealers, mutual funds, futures commission merchants and introducing brokers in commodities engage in transactions through omnibus accounts and sub-accounts established by financial intermediaries. In these situations, (1) the omnibus account or relationship is established by or on behalf of a financial intermediary for the purpose of executing transactions that will clear or settle at another financial institution, or the omnibus accountholder provides limited information to the broker-dealer solely for the purpose of delivering assets to the custody account of the beneficial owner at another financial institution; (2) the limited information given to the financial institution about the beneficial owner is used primarily to assist the financial intermediary with recordkeeping or to establish sub-accounts that hold positions for a limited duration to facilitate the transfer of assets to another financial institution; (3) all transactions in the omnibus account or sub-accounts at the financial institution are initiated by the financial intermediary; and (4) the beneficial owner has no direct control over the omnibus account or sub-accounts at the broker-dealer.

490. With respect to such omnibus accounts, guidance, in the form of question and answer releases, has been issued to broker-dealers, futures commission merchants and introducing brokers in commodities to clarify who should be regarded as the customer in such cases. The guidance confirms that institutions are not required to look through the intermediary to the underlying beneficial owners, if the intermediary is identified as the accountholder. Even if the institution has some information about a beneficial owner of assets in an omnibus account (e.g. batch execution account) or a sub-account, under the circumstances described above, the financial intermediary (not the beneficial owner) should be treated as the customer for purposes of the CIP rule.

491. Guidance has also been issued on similar matters relating to mutual funds. Mutual fund shares that are purchased by investors through third parties (such as banks and securities broker-dealers) often are maintained in omnibus accounts. When mutual fund shares are purchased through a broker-dealer, the broker-dealer would be the customer of the mutual fund for purposes of the customer identification rule. Similarly, if a mutual fund sells its shares to a qualified retirement plan or to a trust, then the plan or trust, and not its participants, will be the mutual fund's customer for purposes of the CIP rule.

492. Much of the customer identification information that must be collected under the CIP already had to be collected pursuant to the industry's books and recordkeeping rules (e.g. customer name, address and date of birth). The requirement to verify such information was, however, a new step for the industry.

493. The securities industry (like the banking sector) applies a risk-based approach with regards to its implementation of the BSA obligations, including CDD. The SEC reports that, even before the amendments to the USA PATRIOT Act came into effect, larger securities firms had extensive experience using the risk-based approach and had implemented very robust customer identification programs. This was confirmed during the on-site visit. One of the larger securities firms, for example, reported having spent millions of dollars implementing the CIP rule (apart from annual maintenance costs). Another large firm confirmed that a substantial part of its client intake procedure is now focused on meeting the CDD requirements of their AML Program. Nevertheless, through drill-down testing, the SEC has found that the smaller and mid-size securities firms have had more difficulty in applying the risk-based approach and still have some way to go in implementing these obligations (even though the concept is not unfamiliar to them given that the securities industry itself is a risk-based industry). Nevertheless, progress is ongoing, and no particularly serious concerns have arisen. Moreover, it should be noted that the ten largest broker-dealers in terms of customer accounts hold about 81% of customer accounts, and the ten next largest hold about 12% of customer accounts. The SEC and NASD advised that their view of the risk based approach is that, if a securities broker determines that a particular entity presents more risk, then that broker must take additional steps pursuant to the CIP that often include identifying the beneficial owner.

Insurance sector

494. There are currently no CIP rules requiring an insurance company to have procedures to verify the identity of each customer and enable it to form a reasonable belief that it knows the customer's true identity. The CIP provisions of the BSA enacted in the USA PATRIOT Act were designed to impose a set of specific CDD obligations on financial institutions that maintain account relationships [see 31 USC 5318(1), "Identification and verification of account holders"]. The U.S. has not yet determined that it would be appropriate to apply these specific provisions to the insurance industry separate and apart from the overall CDD requirements under AML programs that insurance companies obtain "all relevant customer-related information necessary for an effective AML Program. The U.S. authorities state that they will continue to assess the industry and the need and efficacy of imposing these requirements.

495. Despite the absence of a CIP rule, under 31 CFR 103.137(c), a life insurer is required to have policies and procedures for obtaining "all relevant customer-related information necessary for an effective anti-money laundering program". According to the preamble of the regulation, a life insurance company is also "responsible for integrating its agents and brokers into its anti-money laundering program, for obtaining relevant customer-related information from them, and for using that information to assess the money laundering risks presented by its business and to identify any 'red flags'. The specific procedures for conducting such a program are left to the discretion of the insurance company." In addition, under the regulation introducing SAR reporting for insurance companies [31 CFR 103.16(b)(3)(i)], an insurance company "shall establish and implement policies and procedures reasonably designed to obtain customer-related information necessary to detect suspicious activity from all relevant sources including from its insurance agents and insurance brokers". However, neither the AML Program or SAR reporting requirements expressly require life

insurers to collect and verify the specific customer identification information that is required by Recommendation 5.

496. Life insurance companies are not expressly required to undertake CDD measures when establishing business relations or when they have doubts about the veracity or adequacy of previously obtained customer identification data. However, it is noted that insurance products that fall within the definition of a "security" under the federal securities laws and do not fall within the "insurance exemption" found in the Securities Act of 1933 must be sold by registered securities broker-dealers, who are required to adopt and implement AML program rules, CIPs, and suspicious activity reporting programs under the BSA regulations.

497. When carrying out a cash transaction exceeding USD 10,000 in value: Insurance companies are required to file a Form 8300 for cash transactions in excess of USD 10,000 instead of having to file a CTR. The customer identification requirements in making such filings are described in section 3.7 of this report.

498. Generally, the covered insurance products (i.e. life policies) are purchased by individuals and not by legal persons or arrangements. The exception is a "key-man" policy where the policyholder is the employer and, therefore, likely to be a legal person. However, "key-men" policies are generally bought on the lives of more than one employee and therefore are group policies that are not insurance products covered under the BSA. As such, the legal status, ownership and control structure of legal persons or legal arrangements are not required to be verified in the implementation of the final rule on AML Program, unless the risk assessment of the transaction or the customer required to be conducted by the insurance company warrants such additional due diligence.

499. The insurance laws of some U.S. states provide for viatical settlements and/or life settlements (see the Viatical Settlement Act of California, Florida and New York; see also subchapter of the Texas Insurance Code on "Life and Viatical Settlements". A viatical settlement occurs when a person who is terminally ill (i.e. a person whose illness will cause them death within 24 months) sells his/her life insurance policy to a viatical settlement provider. A viatical settlement provider is a company that purchases the life insurance policy by paying the insured person a fraction of the policy's value in exchange for the insured person naming the company as the policy's beneficiary. Upon the insured's death, the benefits payable under the policy are paid out to the viatical settlement provider. A life settlement follows the same basic model, except that the insured is not terminally ill. Usually, the insured is 65 or more years of age with a life expectancy of approximately 10 years. Viatical settlements are considered to be registerable securities.[60]

Money services business sector (including money remitters and foreign exchange)

500. An MSB is generally defined within the BSA to include: (1) a currency dealer or exchanger; (2) a check casher; (3) an issuer, seller or redeemer of travelers' checks, money orders or stored value; (4) a money transmitter; and (5) the U.S. Postal Service (except with regards to its sale of postage or philatelic products. The following table identifies the relative obligations imposed on the MSB sector.

Institution	BSA regulations apply	AML Program	CIP	PEPs requirements	Correspondent banking
MSB	Yes	Yes	No	No	No

501. MSBs do not maintain what would typically be considered account relationships with their customers, but they must obtain and maintain a record of identification information when a customer:

[60] In the case of SEC v. Life Partner, the SEC successfully argued that viatical settlements are securities that are registrable under the securities laws in the Appellate Court of Columbia. Some promoters of viatical settlements register them under the federal securities laws.

(1) buys a monetary instrument involving currency in amounts of USD 3,000 to USD 10,000 inclusive (31 CFR 103.29); or (2) makes a funds transfer of USD 3,000 or more (31 CFR 103.33). In the former case the MSB must obtain the customer's name and account information; in the latter case it must obtain the customer's name and address; in each case, the MSB must verify the identity of the customer [31 CFR 103 125(d)(1)(A)]. In addition, MSBs must meet the CTR filing requirements. The customer identification requirements in making such filings are described in section 3.7 of this report.

502. As with other financial institutions, MSBs are required to implement AML Programs which, in the case of this particular sector, includes a requirement to have policies, procedures and internal controls "for verifying customer identification".

Operators of credit card systems

503. The BSA implementing regulations define an operator of a credit card system as a person doing business in the U.S. that operates a system for clearing and settling transactions in which the operator's credit or debit card is used to purchase goods or services or to obtain cash advances. The regulations do not impose any specific customer identification requirements on such operators, but require them to maintain risk-based systems and controls to guard against their cards being used to facilitate ML or FT. This requirement focuses on the relationship between the operator and the "issuing" and "acquiring" institutions (i.e. the banks). The obligation to identify the credit card holder lies with the banks since the definition of an account under 31 CFR 103.121(a)(i) includes a relationship involving the extension of credit. There is, therefore, no obligation or need for credit card operators to identify the credit card holder.

504. In practice, it appears that the credit card operators exercise control through their contractual relations with the card issuers, wherein they can specify the standards and procedures (including AML) that the issuer expects be maintained. Ongoing monitoring of the performance under these contracts is undertaken by the operator, and there has been confirmation that several issuing banks have been suspended by the operators for failure to comply with defined AML standards. Where such action is considered necessary, the operator has the power contractually and technically, to deactivate the cards instantly.

Recommendation 6 (Politically exposed persons)

Banking sector

505. Financial institutions are required, as part of their AML program to implement procedures for identifying potentially high-risk customers and products. The Federal Banking Agencies, the Treasury and the State Department issued "Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption" on 16 January 2001 ("2001 Guidance"). Although the context of this document clearly indicates that its application extends beyond the banking sector, neither the document itself nor the accompanying press release provide an indication of the scope of the term "financial institution". This guidance urges U.S. financial institutions to apply enhanced scrutiny to their private banking and similar high dollar-value accounts and transactions where such accounts or transactions may involve the proceeds of corruption by senior foreign political figures, their immediate families or close associates ("covered person"). A "senior foreign political figure" is defined as a senior official in the executive, legislative, administrative, military or judicial branches of a foreign government, a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation. It extends also to any corporation, business or other entity that has been formed by, or for the benefit of, a senior foreign political figure. The "immediate family" is deemed to include parents, siblings, spouse, children and in-laws. A "close associate" is a person who is widely and publicly known to be a close associate of the senior foreign political figure.

506. The 2001 Guidance advises that financial institutions should ascertain the identity of the account holder (and the account's beneficial owner) in the course of opening or maintaining an account for a

covered person. Financial institutions should also obtain adequate documentation regarding covered persons, understand the covered person's anticipated account activity, determine the covered person's source of wealth and funds and apply additional oversight to the covered person's account. The guidance goes on to list suspicious activities or red flags to which financial institutions should pay particular attention. It also indicates that the decision to accept or reject establishing an account for a covered person should directly involve a person more senior than the usual account-opening officer.

507. Section 312 of the USA PATRIOT Act requires institutions to establish special due diligence procedures with respect to private banking accounts held by, or on behalf of, a non-U.S. person. Such accounts are narrowly defined to include only those that meet two conditions, namely that the bank requires the account to be maintained in an amount of USD 1 million or more; and that it be "assigned to, or administered or managed by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account". The due diligence must include ascertaining the identity of the nominal and beneficial owners of, and the source of the funds deposited into, the account. In addition, enhanced scrutiny is required of private banking accounts that are maintained by or on behalf of senior foreign political figures, their immediate families and close associates. In July 2002, FinCEN issued an interim final rule implementing the private banking provisions of section 312 for depository institutions, securities broker-dealers, futures commission merchants and introducing brokers in commodities. (67 FR 48348) The interim final rule directs the financial institutions to review the existing 2001 Guidance. It states that, pending the introduction of the final rule, "a program that is consistent with applicable government guidance on private banking accounts…..would be reasonable, so long as it incorporates the requirements of (section 312)" (67 FR 48350).

508. The FFIEC Manual (p.76) (which was published prior to adoption of the final rule and will be updated to reflect its provisions) recognized that institutions would be unable to craft and implement final comprehensive due diligence policies, procedures and controls pursuant to the requirements of section 312 until the final rule is issued. The FFEIC Manual advises that banks should specifically identify PEP accounts and assess the degree of risks involved. Furthermore, banks are directed to mitigate the risk posed by offering such accounts by having senior management involved in the decision to accept a PEP account. If bank management determines after-the-fact that an account is a PEP account, they should "evaluate the risks and take appropriate steps".

509. A final rule was published on 4 January 2006. It defines a private banking account as:

> "an account (or any combination of accounts) maintained at a covered financial institution that
>
> (1) requires a minimum aggregate deposit of funds or other assets of not less that USD 1,000,000;
>
> (2) is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account; and
>
> (3) is assigned to, or is administered or managed by, in whole or in part, an officer, employee, or agent of a covered financial institution acting as a liaison between the covered financial institution and the direct or beneficial owner of the account."

510. Within this context, the final rule requires institutions to have CDD programs that permit them to identify whether a customer is a senior foreign political figure. The definition of a senior political figure is the same as contained in the 2001 Guidance, except with respect to the definition of close associate, which was modified to include "a person who is widely and publicly known (or is actually known by the relevant covered financial institution) to be a close associate" of the senior foreign political figure. Although the rule itself is silent on what measures an institution might reasonably be expected to take to identify such persons, the preamble in the Federal Register (71 FR 510) offers specific guidance on the due diligence procedures as follows:

"As we believe most covered financial institutions already do, the procedures should require obtaining information regarding employment and other sources of income. First, the institution should seek information directly from the individual regarding possible senior foreign political figure status. Second, the institution should check references, as appropriate, to determine whether the individual holds or has previously held a senior political position or may be a close associate of a senior foreign political figure. Third, the institution should also make reasonable efforts to review public sources of information in meeting this obligation."

511. The enhanced due diligence procedures for PEPs under the rule are generally the same as for other non-US holders of private banking accounts, and include an obligation to ascertain the source of funds and the purpose for which the account is being opened. The rule imposes an additional obligation, specific to PEPs, to establish arrangements for enhanced scrutiny of the account such that the institution may reasonably identify and report transactions that might involve the proceeds of foreign corruption. Although there is no specific mention in the rule, the preamble (71 FR 511) indicates that a financial institution should involve senior management when deciding to open an account for PEP, and that information regarding the account should be available for review also by senior management.

512. FinCEN's final rule relating to the section 312 requirements, which was published 4 January 2006, is effective on 5 July 2006 for accounts opened after that date, but is also retrospective, requiring the application of the measures to all existing accounts by 2 October 2006.

513. The difficulty of identifying PEPs, and the weaknesses in procedures to facilitate this, was a common theme during discussions with the financial sector and regulators. Within the U.S. this has been a high profile issue since the action taken against Riggs Bank, and a common refrain from the banking industry was that they hoped for more concrete information from the authorities on actual names, rather than definitions. This is not a realistic expectation, and in practice many of the banks are relying on commercial databases to interface with their account-opening and monitoring systems. While these are undoubtedly of considerable value, there is a risk that the banks may be relying on them as their sole warning system, rather than developing concurrent in-house monitoring procedures.

514. While the underlying requirements and guidance on dealing with PEPs are reasonable, it is surprising that they have been circumscribed by the narrow definition of private banking. In principle, this is a significant weakness that could undermine the clear objectives of the U.S. authorities in this area. During the consultation period on the rule, the banks themselves questioned the potential loophole that would exempt an institution from applying the PEP standards, simply because it did not require USD 1 million as a condition of maintaining the account. When publishing the final rule, FinCEN recognized this point, but stressed that it had to work within the strict letter of section 312 of the USA PATRIOT Act. However, it indicated that it would review the application of the law if there were evidence of abuse of the principles. More significantly, although this is not apparent from the preamble to the section 312 rule, FinCEN and the Federal Banking Agencies have also indicated that the 2001 Guidance remains in force in dealing generally with PEPs, and that they would take a robust position on banks' adherence to the guidance (pp 153-154 of the FFIEC Manual). This guidance does not contain the value threshold specified within section 312 and is not limited to private banking operations. Thus, a financial institution's BSA compliance program is expected to provide enhanced due diligence procedures over PEPs, even if the account is not subject to the final section 312 rule. Financial institutions have been sanctioned for failing to comply with the 2001 Guidance, one such example being In the Matter of Banco de Chile, Federal Reserve Board of Governors Docket No., 05-001-B-FR (1 February 2005).

Securities sector

515. The legal provisions that are applicable to the securities sector in relation to politically exposed persons are the same as those described above for the banking sector.

Insurance and money service business (including money remitters and foreign exchange) sectors

516. Insurance companies and MSBs are not currently covered under rules introducing the PEP requirement, although they are both subject to the AML program and SAR reporting rules. As indicated above, PEPs have been defined only within the context of private banking regulations. However, registered securities broker-dealers, who are the only individuals permitted to sell any insurance product that is considered a security, are subject to all the AML requirements (including those relative to PEPs) that apply to securities broker-dealers, as noted earlier in this report. In the preamble to the private banking rules in which its risk assessment process is described, FinCEN indicated that, in its understanding, no sectors other than banking and securities offer such facilities.

Additional elements

517. The U. S. was one of the first nations to sign the United Nations Convention Against Corruption when it was opened for signature in December 2003. It is currently proceeding with its internal processes to ratify the convention.

518. The U.S. has no intention of extending the definition of a senior political figure to encompass residents of the U.S., but expects institutions to be alert to the money laundering threats that may arise from such customers, and to mitigate the risks through their normal CDD processes.

Recommendation 7 (Correspondent banking and similar relationships)

Banking sector

519. All financial institutions, when providing correspondent banking services for non-U.S. persons, are required by section 312 of the USA PATRIOT Act to "establish appropriate, specific and, where necessary, enhanced due diligence policies, procedures and controls that are reasonably designed to detect and report instances of money laundering through those accounts". In addition, special enhanced due diligence policies and procedures are required when opening or maintaining a correspondent account in the U.S. on behalf of certain foreign banks operating under: (1) an offshore banking license;[61] (2) a banking license issued by a foreign country that has been designated as non-cooperative with international AML principles or procedures by an intergovernmental group or organization of which the U.S. is a member, and with whose designation the U.S. representative to the group or organization concurs; or (3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

520. In circumstances where special enhanced due diligence is required, section 312 states that banks must establish policies, procedures, and controls to ensure that the bank takes reasonable steps to:

(a) ascertain, for any such foreign bank whose shares are not publicly traded, the identity of each of the owners of the foreign bank, and the nature and extent of the ownership interest of each such owner;

(b) conduct enhanced scrutiny of any accounts held by such banks to guard against money laundering and report any suspicious transactions in accordance with SAR regulations; and

(c) ascertain whether such foreign bank provides correspondent accounts to other foreign banks and, if so, to ascertain the identity of those foreign banks and conduct due diligence as appropriate under the requirements of subsection 5318(i)(1) (i.e., the bank's general due diligence program) [31 USC 5318(i)(2)(B)(i) through (iii)].

521. On 23 July 2002 FinCEN issued an interim final rule (31 CFR 103.81 and 103.82) implementing the correspondent provisions of section 312 for depository institutions, and deferring

[61] The USA PATRIOT Act defines an offshore banking license as a license to conduct banking activities that, as a condition of the license, prohibits the licensed entity from conducting banking activities with the citizens of, or with the local currency of, the country that issued the license. Refer to 31 USC 5318(i)(4)(A).

application of such provisions to other types of financial institutions pending adoption of a final rule. The deferral was on the grounds that a final rule could not reasonably be implemented within the statutory deadline, that there was no immediate evidence that correspondent relationships existed in other than the banking sector, and that the term "correspondent account" had not yet been defined outside of the banking sector. The preamble to the Federal Register notice of the interim final rule contains guidance that indicates what FinCEN regards as "reasonable" practice for a bank pending publication of the final rule. It encourages banks to give priority to conducting due diligence on:

(a) high-risk foreign financial institutions for which it maintains correspondent deposit or equivalent accounts;

(b) correspondent accounts used to provide services to third parties; and

(c) high-risk correspondent accounts maintained for foreign financial institutions other than banks, such as money remitters.

522. Reference is also made to the need to follow current best practice on dealing with correspondent accounts, including guidelines issued by the New York Clearing House Association (NYCHA) in March 2002 (Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking), and the Basel Committee's paper on Customer Due Diligence for Banks published in October 2001. Among other things, the NYCHA guidance states, "the bank should develop and maintain policies, procedures and controls under which all applicants are approved by at least one person other than the relationship manager primarily responsible for the establishment of the applicant's correspondent account, which other person may be an officer senior to the relationship manager in the same department as the relationship manger, or an officer in another department (for example, the risk management department or compliance department) of the Bank." In terms of complying with the enhanced due diligence requirements for high risk correspondent relationships, banks were advised in the Federal Register to take reasonable measures to comply with the strict directives of section 312, but within the broad context of a risk-based approach.

523. Page 73 of the FFIEC Manual states that a bank's general due diligence program should include policies, procedures and processes to assess the risks posed by the bank's foreign financial institution customers, and provides the following factors that may be used to help identify potential risk characteristics of such customers:

(a) the foreign financial institution's jurisdiction of organization, chartering, and licensing;

(b) products and services offered by the foreign financial institution;

(c) markets (including customer base) and locations served by the foreign financial institution;

(d) purpose of the account (e.g., a proprietary operating account or a customer-directed account);

(e) anticipated activity (e.g., dollar amount, number, and types of transactions) of the account;

(f) the nature and duration of the bank's relationship with the foreign financial institution (and, if relevant, with any affiliate of the foreign financial institution); and

(g) any information known or reasonably available to the bank about the foreign financial institution's AML record, including public information in standard industry guides, periodicals and major publications.

524. In terms of defining the relationship with the correspondent institution, the FFIEC Manual (p.98) states that:

> "Each relationship that a U.S. bank has with a foreign correspondent financial institution should be governed by an agreement or a contract describing each party's responsibilities and other relationship details (e.g. products and services provided, acceptance of deposits, clearing of items forms of payments, and acceptable forms of endorsement). The agreement or contract should also consider the foreign correspondent's AML responsibilities, customer base, due

diligence procedures, and customer referrals from the correspondent to the U.S. bank, clearly defining all referral terms (e.g., customer type and business profile, customer's geographic location, and any special terms)."

525. On 4 January 2006, FinCEN issued a final rule (31 CFR 103.176) on dealing with most aspects of correspondent accounts opened for foreign financial institutions, and sought additional comment for 60 days on enhanced due diligence measures for high-risk accounts (see below). Until a final rule relating to enhanced due diligence is issued and becomes effective, banks are required to continue to apply the enhanced due diligence provisions of section 312 to their correspondent accounts in accordance with the July 2002 interim final rule. The final rule extends the scope of the banking sector that is covered to include uninsured trust banks and trust companies that are federally regulated and that are subject to an AML Program requirement. Credit unions and non-depository trust companies that do not have a federal functional regulator remain outside the net until an unspecified future date; however, this is not a substantive AML issue. The rule applies to all correspondent accounts opened for foreign financial institutions, which are defined to include foreign banks; the foreign offices of covered financial institutions; non-U.S. entities that, if they were located in the United States, would be a securities broker-dealer, futures commission merchant, or mutual fund; and non-U.S. entities that are engaged in the business of, and are readily identifiable as, a currency dealer or exchanger or a money transmitter.

526. The general principle contained within the final rule is that banks should include within their AML Program specific policies, procedures and controls as are appropriate to mitigate the risk in establishing and maintaining accounts for foreign correspondents. In determining the risk, the rule requires institutions to take account of the following:

(a) the nature of the foreign financial institution's business and the markets it serves;

(b) the type, purpose, and anticipated activity of the correspondent account;

(c) the nature and duration of the covered financial institution's relationship with the foreign financial institution (and any of its affiliates);

(d) the anti-money laundering and supervisory regime of the jurisdiction that issued the charter or license to the foreign financial institution, and, to the extent that information regarding such jurisdiction is reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered; and

(e) information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record.

527. The rule also contains a specific obligation to include within the procedures a periodic review of each correspondent account to determine consistency with the information obtained about the type, purpose and anticipated activity of the account. The rule does not contain any reference to the involvement of senior management in approving the opening of individual correspondent accounts, and the closest to any such requirement appears in the NYCHA guidance, which specifies the separation of the approval process from the relationship management function. However, the overall AML program, including the procedures relating to correspondent accounts, must be approved by the board of directors, but senior management involvement in decisions on opening individual accounts is determined by the institution's risk-based procedures and is not required on a systematic basis.

528. The rule comes into effect on 5 July 2006 for accounts opened after that date, but is retroactive, with effect from 2 October 2006, for accounts opened before 5 July.

529. Separately, regulations adopted pursuant to Section 319(b) of the USA PATRIOT Act (dealing with record keeping) require any covered financial institution that provides a correspondent account to any foreign bank (irrespective of the whether the jurisdiction is high-risk for money laundering) to maintain records of the foreign bank's owners (except when the shares are publicly traded) and the

name and address of an agent in the U.S. designated to accept service of legal process for the foreign bank for records regarding the correspondent account. The regulations also prohibit the provision of correspondent banking services on behalf of foreign shell banks, defined as banks with no physical presence. U.S. financial institutions subject to section 313 of the Patriot Act are further prohibited from providing such services "indirectly." The regulation provides a safe harbor for compliance with this prohibition and the service of process record-keeping requirements, provided that a covered financial institution obtains a certification from its foreign bank customers and renews this at least once every three years. If the certificate is not obtained within thirty days after the date on which the account was established, the institution is required to close all correspondent accounts for the foreign bank "within a commercially reasonable time". Information on correspondent accounts existing prior to the introduction of the regulations had to be obtained by 31 March 2003. If the institution, at any time, has reason to suspect that the information contained in the certificate (or otherwise provided) is no longer correct, it must request the foreign bank to verify or correct it. Failure to obtain an adequate response within 90 days also triggers a requirement to close all accounts for the foreign bank.

530. The Federal Banking Agencies have discouraged U.S. banks from maintaining payable-through accounts (PTAs) for their foreign correspondents, and it is believed that their use is relatively rare, and restricted largely to the national banks operating in Miami. In March 1995 the banking agencies published guidance (SR 95-10) on the need to maintain systems that allowed financial institutions to be able to identify the ultimate users of such accounts. More recently, the FFIEC Manual (p. 103) states that:

> "U.S. banks offering PTA services should develop and maintain adequate policies, procedures and processes to guard against possible illicit use of these accounts. At a minimum, policies, procedures, and processes should enable each U.S. bank to identify the ultimate users of its foreign financial institution PTA and should include the bank's obtaining (or having the ability to obtain through a trusted third-party arrangement) substantially the same information on the ultimate PTA users as it obtains on its direct customers.
>
> Policies, procedures, and processes should include a review of the foreign financial institution's processes for identifying and monitoring the transactions of sub-accountholders and for complying with any AML statutory and regulatory requirements existing in the host country and the foreign financial institution's master agreement with the U.S. bank. In addition, U.S. banks should have procedures for monitoring transactions conducted in foreign financial institutions' PTAs.
>
> In an effort to address the risk inherent in PTAs, U.S. banks should have a signed contract (i.e., master agreement) that includes:
>
> - Roles and responsibilities of each party.
> - Limits or restrictions on transaction types and amounts (e.g., currency deposits, funds transfers, check cashing).
> - Restrictions on types of sub-accountholders (e.g., casas de cambio, finance companies, funds remitters, or other non-bank financial institutions).
> - Prohibitions or restrictions on multi-tier sub-accountholders.
> - Access to the foreign financial institution's internal documents and audits that pertain to its PTA activity.
>
> U.S. banks should consider closing the PTA in the following circumstances:
>
> - Insufficient information on the ultimate PTA users.
> - Evidence of substantive or ongoing suspicious activity.
> - Inability to ensure that the PTAs are not being used for money laundering or other illicit purposes."

531. The decision (announced in the January 2006 notice) to seek additional comment on rules governing enhanced due diligence procedures for specified high-risk correspondent accounts was based on the significant number of industry comments received on the original notice of proposed rule-making published in May 2002. On 4 January 2006, FinCEN published another proposal, seeking comments for 60 days on a risk-based approach to dealing with accounts opened by banks falling within the three specific categories identified under section 312 of the USA PATRIOT Act. The proposal would require the risk assessment to include the following:

(a) obtaining and reviewing documentation relating to the foreign bank's anti-money laundering program;

(b) considering whether such program appears to be reasonably designed to detect and prevent money laundering;

(c) monitoring transactions to, from, or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity; and

(d) obtaining information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account, and the sources and beneficial owner of funds or other assets in the payable-through account.

532. In addition, an institution would be required: (a) to determine (and apply appropriate measures) if the account opened by the foreign bank was, in turn, also able to be used by other banks through "nested" correspondent accounts maintained by the foreign bank; and (b) to identify any person who, directly or indirectly controls 10% or more of any class of the foreign bank's securities, where it is not a publicly-traded entity.

533. The obligations imposed on banks with respect to foreign correspondent accounts have given rise to criticism from the industry that the section 312 requirements are excessively prescriptive and burdensome. Some regulators have reported that failure to comply fully with the obligations is a relatively common theme identified during their AML examinations. Some banks say they have selectively closed foreign correspondent accounts on the basis solely that the cost of compliance with the monitoring requirements exceeds the commercial value of the business. Others (particularly the smaller institutions) have adopted a general practice of not offering this service, apart from in exceptional circumstances (which, on a risk basis, may be a desirable outcome for a small institution). The substantially risk-based approach provided within the final rule may allay some of the concerns expressed by industry, and there is every indication that the focus on this issue has instilled a culture of caution within the industry.

Securities sector

534. In its final rule published in January 2006, FinCEN extended the obligations on correspondent relationships to securities broker-dealers, mutual funds, and futures commission merchants and introducing brokers. In the case of broker-dealers, such accounts are deemed to be: (1) accounts to purchase, sell, lend or otherwise hold securities; (2) prime brokerage accounts that clear and settle securities transactions for clients; (3) accounts for trading foreign currency; (4) custody accounts for holding securities or other assets in connection with securities transactions as collateral; and (5) over-the-counter derivatives contracts. In the case of mutual funds, the rule relates to accounts for foreign financial institutions in which they may hold investments in the mutual funds as principals or for their customers, and which the foreign financial institution may use to make payments or handle transactions. For futures commission merchants and introducing brokers, a correspondent account includes accounts for foreign institutions to engage in futures or commodity options transactions, funds transfers, or other financial transactions, whether for the financial institution or its customers.

535. The basic rules governing these accounts are the same as for correspondent banking relations, but there is currently not the same supplementary guidance that has been issued to the banking industry.[62]

Other sectors

536. The U.S. has concluded in the preamble to the rule published in January 2006 (31 CFR 103.175) that no similar types of relationship exist in other parts of the financial sector.

Recommendation 8 (New payment technologies)

Banking sector

537. The Federal Banking Agencies recognize electronic banking as a higher risk area and require that banks ensure that their procedures and monitoring systems adequately address the risks that may arise in this area. The FFIEC Manual (p.113) states that:

> "Banks should establish BSA/AML monitoring, identification, and reporting for unusual and suspicious activities occurring through e-banking systems. Useful management information systems for detecting unusual activity in high-risk accounts include ATM activity reports, funds transfer reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses, and tax identification numbers). In determining the level of monitoring required for an account, banks should include how the account was opened as a factor. Banks should consider whether customers seeking certain financial services, such as electronic banking, should be required to open accounts on a face-to-face basis. Other controls, such as establishing transaction dollar limits for large items that require manual intervention to exceed the preset limit, may also be instituted by the bank."

538. The implementing regulation to Section 326 of the USA PATRIOT Act specifically requires that, as part of its risk-based CIP, a financial institution must take particular precautions when opening an account in a non face-to-face situation. Specifically, a financial institution's non-documentary procedures must address situations where an individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the financial institution is not familiar with the documents presented; the account is opened without obtaining documents; the customer opens the account without appearing in person at the financial institution; and where the financial institution is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents [e.g. 31 CFR 103.121(b)(2)(ii)(B)(2)].

539. In August 2001, the Federal Banking Agencies developed interagency guidance (published under the auspices of the FFIEC) entitled "Authentication in an Electronic Banking Environment". It summarized the risks and risk management controls of a number of existing and emerging authentication tools necessary to verify the identity of new customers and authenticate existing customers that access electronic banking services. This guidance was updated with the publication, in October 2005, of "Authentication in an Internet Banking Environment". The latest publication was introduced to reflect the significant legal and technological changes since 2001 with respect to the protection of customer information; the increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies. The document is divided into two parts; the main portion provides financial institutions with guidance on authentication and discusses appropriate risk assessments, customer authentication, verification of new customers, and monitoring and reporting; while an appendix provides more detail about various authentication technologies.

[62] FinCEN, the SEC and the CFTC have indicated that they intend to issue such guidance in due course.

540. The latest publication stresses that the agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. It requires institutions to apply techniques that are appropriate to the risks associated with the products and services, and states that they should periodically:

(a) ensure that their information security program:

– identifies and assesses the risks associated with Internet-based products and services;

– identifies risk mitigation actions, including appropriate authentication strength; and

– measures and evaluates customer awareness efforts;

(b) adjust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information; and

(c) implement appropriate risk mitigation strategies.

541. The appendix to the document provides an extensive list of authentication techniques, processes and methodologies. Institutions are advised that the use of any technique should be based on its own risk assessment.

Securities sector

542. Certain sectors of the securities industry routinely operate on a non-face-to-face basis, which has been recognized in the regulations. Investors in securities or debt securities can place their orders through a broker by telephone, online by computer, or in person, but the majority of orders are currently placed by telephone. Brokerage firms also can buy and sell securities and commodities on electronic communication networks (ECNs), which are computer networks that automatically list, match, and execute trades. ECNs may be registered with the SEC as a securities broker-dealer or as a securities exchange. Securities broker-dealers may provide large investors with direct access to ECNs, exchange facilities, or dealer markets.

543. The legal provisions that are applicable to the securities sector in relation to non face-to-face business are similar to those described above for the banking sector. The implementing regulation to Section 326 of the USA PATRIOT Act specifically requires that, as part of its risk-based CIP, a financial institution must take particular precautions when opening an account in a non face-to-face situation. According to these regulations an institution's non-documentary evidentiary procedures must address situations where an individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the financial institution is not familiar with the documents presented; the account is opened without obtaining documents; the customer opens the account without appearing in person at the financial institution; and where the financial institution is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents.

Insurance sector

544. Even though some insurers and insurance agents offer covered insurance products through the internet, there is no federal law requiring insurers to have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions.

Money services business sector (including money remitters and foreign exchange)

545. There is no legal provision requiring MSBs to have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. FinCEN is working with law enforcement to better understand the risks posed by various types of stored value

and internet payment products. Once its risk analysis is completed, FinCEN anticipates amending current rules to better address any risks that are found

3.2.2 Recommendations and Comments

546. The U.S. regulations address in detail a substantial number of the FATF requirements on CDD. However, as indicated, in certain key areas on which the FATF places considerable emphasis, the approach adopted by the U.S. appears to fall short. Therefore the following recommendations are made:

(a) Introduce a primary obligation to identify the beneficial owners of accounts (which may, of course, be implemented on a risk-based approach with respect to low-risk customers or transactions).

(b) Implement a CIP requirement for the insurance sector.

(c) Introduce an explicit obligation that financial institutions should conduct ongoing due diligence, rather than rely on an implicit expectation within the SAR requirements and on the existing guidance.

(d) In the case of occasional transactions, extend the customer identification obligation to non-cash transactions.

(e) Other than with respect to non-face-to-face business, securities transactions, and life insurance business, limit the circumstances in which institutions may open an account prior to completing the verification process, and introduce a presumption that institutions should close an account whenever the verification cannot be completed, for whatever reason. If necessary, accompany this with some form of indemnification against other conflicting statutes.

(f) Introduce an explicit requirement that the opening of individual correspondent accounts should involve senior management approval.

(g) Extend AML/CFT obligations (including the PEPs requirements) to investment advisers and commodity trading advisers, in line with those applicable to the rest of the securities industry.

(h) Publish confirmation that, despite the promulgation of the final section 312 rule, the 2001 Guidance on PEPs remains in force and that it applies to all relevant financial institutions.

(i) Introduce an explicit requirement for the life insurance and MSB sectors to address the specific risks associated with non-face to face business relationships or transactions.

(j) Extend the obligation for AML Programs and CIP (as applicable) to all depository institutions to remove the historical anomaly.

3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	PC	• No obligation in law or regulation to identify beneficial owners except in very specific circumstances (i.e. correspondent banking and private banking for non-U.S. clients). • No explicit obligation to conduct ongoing due diligence, except in certain defined circumstances. • Customer identification for occasional transactions limited to cash deals only. • No requirement for life insurers issuing covered insurance products to verify and establish the true identity of the customer (except for those insurance products that fall within the definition of a "security" under the federal securities laws). • No measures applicable to investment and commodity advisers. • Verification of identity until after the establishment of the business relationship is not limited to circumstances where it is essential not to interrupt the normal course of business. • No explicit obligation to terminate the business relationship if verification process cannot be

		completed. • The effectiveness of applicable measures in the insurance sector (which went into force on 2 May 2006) cannot yet be assessed.
R.6	LC	• Measures relating to PEPs do not explicitly apply to MSBs, the insurance sector, investment and commodity trading advisers.
R.7	LC	• No obligation to require senior management approval when opening individual correspondent accounts.
R.8	LC	• No explicit provision requiring life insurers MSBs, or investment and commodity trading advisers to have policies and procedures for non-face-to-face business relationships or transactions.

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis

Recommendation 9 (Third parties and introduced business)

Banking sector

547. The BSA implementing regulations (31 CFR 103.121) permit an institution to rely on the performance of any of the elements of the CIP procedures (including identity verification and record-keeping) by another financial institution (including an affiliate) located in the U.S. under very specific circumstances. This is limited to where:

(a) the customer will have an account with both financial institutions, the reliance is reasonable under the circumstances;

(b) the relied-upon financial institution is required to establish and maintain an AML Program and is regulated by a federal functional regulator; and

(c) there is a written contract requiring the relied-upon financial institution to certify annually to the relying financial institution that it has implemented its own AML Program, and that it will perform the specified elements of the CIP on the relying financial institution's behalf.

548. Under this arrangement, the relying financial institution will not be liable for any failure of the relied-upon financial institution if the relying financial institution demonstrates that its reliance was reasonable, it enters into the required contract, and it obtains the required certification from the relied-upon financial institution. Such an arrangement is quite separate from any agency agreement that an institution might have with a service provider, where the BSA obligations remain entirely with the institution.

549. The regulations do not permit reliance on financial institutions located outside the U.S.; nor may reliance be placed on a third party to accomplish identity verification of customers undertaking large currency transactions, the purchase of specified financial instruments, and certain wire transfers. In addition, no reliance may be placed on a third party for any of the broader aspects of CDD.

550. Regardless of whether the CIP is performed by a financial institution or a different financial institution under the reliance provision, the CIP rule requires that identifying information obtained about a customer at the time of account opening be retained for five years after the date the account is closed. It is expected that the financial institutions using the reliance provision for obtaining CIP information will have policies, procedures and processes in place to obtain the required information from any institution that has performed the financial institution's CIP requirements. However, there is no legal or regulatory requirement specifying what minimum information must be obtained at the outset by the relying institution.

551. Section 319 of the USA PATRIOT Act requires a financial institution to respond to a request by an appropriate Federal Banking Agency for information related to AML compliance by a financial institution or a customer of such financial institution within 120 hours after receiving the request. As a result, a bank

that relies on another institution to conduct CIP or other records management functions must be in a position to ensure that the documents can be retrieved within 120 hours to comply with section 319.

552. It is generally believed that the narrow conditions under which introduced business is permitted, combined with the existence of the 120-hour rule, provide very little incentive to institutions to adopt this approach, and this was supported by comments from the banking industry. However, where use is made of the provision, there is no explicit requirement as to what minimum information the bank must obtain from the introducing institution. Reliance seems to be placed on the fact that the bank will wish to protect its interests with respect to the 120-hour rule.

Securities sector

553. The legal provisions that are applicable to the securities sector in relation to third parties and introduced business are identical to those described above for the banking sector.

Insurance

554. Insurers may sell insurance products directly or rely on third parties such as insurance agents and insurance brokers to introduce business. However, there are no measures in place to implement the specific obligations of Recommendation 9 in the insurance sector. For instance, there is no express legal provision for insurers that rely on insurance agents and insurance brokers to introduce business to immediately obtain from them the necessary information relating to CDD requirements. Regulation 31 CFR 103.16(b)(3) only requires insurers to have procedures in place reasonably designed to obtain customer-related information from its insurance agents and insurance brokers necessary to detect suspicious activity. The specific means to obtain such information are left to the discretion of the insurer, including amending existing agreements with them to integrate them into its AML Program [70 FR 66756; 31 CFR 103.137(a)-definitions] and to ensure that it receives the necessary customer identification information and other relevant documentation upon request without delay. For the reasons mentioned earlier in this report, it is questionable how the covered life insurers could effectively rely on introducers like independent insurance agents and insurance brokers to provide them with the necessary information relating to CDD requirements.

Money services business sector (including money remitters and foreign exchange)

555. This Recommendation does not apply to MSBs given the nature of their business.

3.3.2 Recommendations and Comments

556. The U.S. is substantially compliant with the FATF requirements on third-party introduced business. However, the U.S. should introduce a requirement that the relying bank or other financial institution should obtain immediately from the introducing institution details relating to the identity of the account holder, the beneficial owner, and the reason for which the account is being opened. Additionally, it should extend such measures to investment and commodity trading advisers, and the insurance sector (including insurance agents and brokers).

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	LC	• No explicit obligation on relying institution to obtain core information from introducer. • No measures have been applied to investment and commodity trading advisers, or the insurance sector.

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

Right to Financial Privacy Act (RFPA)

557. The principal U.S. statute protecting the confidentiality of financial information is the Right to Financial Privacy Act (RFPA), codified at 12 USC 3401-22. Generally, the RFPA governs both how U.S. federal agencies obtain information from financial institutions and under what circumstances they may disclose such information. The overall purpose of the RFPA is to protect individuals who are customers of financial institutions from unwarranted intrusion into their records by the government. The Act makes it unlawful for a financial institution to release financial records of any individual customer or partnership of five or fewer individuals to the U.S. Government, except in accordance with the provisions of the Act. It defines "financial institution" to include any of the following entities located in any state or territory of the U.S.: any office of a bank; savings bank; card issuer [as defined in 15 USC 1602(n)]; industrial loan company; trust company; savings association; building and loan or homestead association (including cooperative banks); credit union; and consumer finance institution.

558. The RFPA states that no federal government agency may have access to information contained in the financial records of any individual or partnership of five or fewer individuals from a "financial institution" (as defined in the RFPA) unless the financial records are reasonably described and:

(a) the customer authorizes access;

(b) there is an appropriate administrative subpoena or summons

(c) there is a qualified search warrant;

(d) there is an appropriate judicial subpoena; or

(e) there is an appropriate written request from an authorized government authority.

559. The RFPA also governs the transfer of covered financial records by the federal agencies holding those records; the RFPA permits transfer of records by a financial institution supervisor to the Attorney General if there is reason to believe that the records are relevant to a federal crime, or to the Secretary of the Treasury "for criminal investigative purposes relating to money laundering and other financial crimes" [12 USC 3412(f)].

560. The RFPA applies to requests for information by the federal government, not by U.S. state or local governments, and it does not govern uses of information by private firms. As indicated, it applies only to accounts of individuals or partnerships of five or fewer individuals at depository institutions, credit card issuers, and consumer finance institutions. Thus, it does not cover any account information of corporations, or larger partnerships, (except in the relatively rare situation in which a corporation or other legal entity is acting as an "authorized representative" of an individual or small partnership), and it has no application to business relationships between any persons and securities broker-dealers or other classes of non-depository financial institutions (except credit card issuers and consumer finance companies).

561. The RFPA generally prohibits disclosure of information to federal government authorities without notice to the customer and an opportunity for the customer to challenge the request. However, there are numerous exceptions that work to assure the free flow of information to the government with respect to criminal investigations. In particular, the RFPA generally does not apply to information subject to a grand jury subpoena. Accordingly, when it uses a grand jury subpoena to obtain the financial records of a customer from a financial institution, DOJ is not required by the RFPA to give any notice to the customer or provide certification of RFPA compliance to the financial institution.

562. The RFPA also provides for access to financial records through other mechanisms, including an administrative subpoena or judicial subpoena. Administrative subpoenas or summons are issued by an

agency in order to gather evidence in contemplation of an administrative or civil enforcement action and authorized by different statutes and federal regulations for different agencies and purposes. Of particular note, federal offices of inspectors general have authority to issue administrative subpoenas pursuant to the Inspector General Act of 1978 (5 USCA app.3). Administrative subpoenas, as well as subpoenas issued by a court in other proceedings, such as civil forfeiture proceedings, would be subject to notice and challenge procedures. However, the government can apply for an *ex parte* court order to authorize delay of customer notification (12 USC 3405, 3407, 3409). Alternatively, law enforcement also may execute a judicially approved search warrant to obtain financial records [12 USC 3406(a)].

563. There are exceptions, in which disclosure by a "financial institution" is always permitted, and no authorization, subpoena, or warrant is required under the RFPA. These exceptions include:

(a) examinations by an appropriate supervisory agency, which includes the Federal Banking Agencies, the SEC, State banking or securities departments or agencies, and, with respect to the BSA, the Secretary of the Treasury [12 USC 3413(b) and 3401(7)];

(b) financial records or information required to be reported in accordance with any federal statute or rule promulgated there under [12 USC 3413(d)];

(c) disclosures by financial institution supervisors and other agencies of information (including documents) to the Attorney General or the Secretary of the Treasury if there is reason to believe that the information is relevant to a violation of federal criminal law [12 USC 3412(f)]; and

(d) disclosure to federal agencies authorized to conduct investigations of, or intelligence or counterintelligence analyses relating to, international terrorism, or other national security protective functions. [12 USC 3414(a)]

564. The RFPA does not apply to mandatory SARs. That is, although the RFPA contemplates that notice will be given to customers when financial records are transferred from one agency to another, notice is not given to customers when SARs are furnished by FinCEN to law enforcement officials. SARs may be disclosed and disseminated only under strict guidelines.

State-level privacy laws

565. Many states have imposed financial privacy laws similar to the provisions of the RFPA.

Information sharing systems

566. Section 314(b) of the USA PATRIOT Act permits financial institutions, upon providing notice to the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. Financial institutions may share the information after providing notice to the Department of the Treasury by filing the "Notice for Purposes of Section 314(b) of the USA PATRIOT Act and 31 CFR 103.110" (notice form). The final rule became effective 26 September 2002. However, only those financial institutions [as defined by 31 USC 5312(a)(2)] that are located in the U.S. and required to have AML compliance programs pursuant to Section 352 of the USA PATRIOT Act may participate in the voluntary program. A financial institution that is not subject to such an AML Program and does not abide by the conditions set forth in the implementing rules found at 31 CFR 103.110, (notice, verification of counterpart, and use and security information), cannot enjoy the statutory safe harbor from liability for the voluntary information sharing under section 314(b). The right to share information shall be effective for the one-year period beginning on the date of the notice, which is the execution date appearing on the notice form. To continue the sharing of information after the end of the one-year period, a financial institution or association of financial institutions must submit a new notice form. Section 314(a) of the USA PATRIOT Act also requires certain financial institutions to receive specific information requests from federal government agencies through FinCEN, conduct record searches, and respond to FinCEN with positive record matches of targeted individuals or entities (31 CFR 103.100).

Effective 1 March 2005, FinCEN implemented its web-based USA PATRIOT Act 314(a) secure communications system allowing financial institutions to access subject information. The system allows for more efficient reporting of matches to FinCEN.

3.4.2 Recommendations and Comments

567. The U.S. is compliant with this Recommendation.

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	C	• This Recommendation is fully observed.

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis

Recommendation 10 (Record keeping)

Banking sector

568. U.S. regulations do not require that banks necessarily retain copies of the documentation upon which reliance was placed for verification of the customer's identity, on the grounds that such a practice might fall foul of certain state laws governing privacy and consumer protection, and that it may increase the risk of identity theft. Instead, the institution must maintain a record of all identifying information about a customer, as well as noting the type of document, any identification number, the place and date of issue, and the expiration date of any document it used to obtain that information. The record must also include a description of the method used to verify identity. Records of customer identification data collected under the CIP rules (31 CFR 103.121 for banks) must be retained for a period of five years after the date on which the account is closed. With regard to the maintenance of records of correspondent accounts for foreign banks [pursuant to Section 319(b) of the USA PATRIOT Act] originals or copies of documents provided by the foreign bank must be retained for at least five years after account closure [31 CFR 103.177(e)]. A similar retention period is specified for any reports (including background documentation) filed with FinCEN under the CTR and SAR requirements.

569. There is a requirement [31 CFR 103.38(d)] that all such records required under the range of rules promulgated under Part 103 must be retained for a period of at least five years from the date of the transaction. There is no general obligation to maintain whatever records might be necessary to allow all transactions to be reconstructed. However, the specific records identified under Part 103 [31 CFR 103.33, 103.34(b) and elsewhere] are extensive and, indeed, appear to be duplicative in some instances and are applicable to all "banks," a term which is very broadly defined for these purposes. These records include:

- information regarding the purchaser and purchase transaction with respect to the issuance or sale of a bank check or draft, cashier's check, money order, or traveler's check for currency amounts between USD 3,000 and USD 10,000;
- a record of each extension of credit in an amount over USD 10,000, except when the extension is secured by an interest in real property;
- a record of each advice, request or instruction given or received regarding a transaction which resulting in the transfer of funds, currency, checks, investment securities, other monetary instruments, investment securities, or credit, of more than USD 10,000, to or from any person, account or place outside the U.S.;
- a record of each advice, request or instruction given to another financial institution or other person located within or outside the U.S., regarding a transaction intended to result in a transfer

of funds, currency, checks, investment securities, other monetary instruments or credit, of more than USD 10,000, to a person, account or place outside of the U.S.;

- the original or copy of each statement, ledger card or other record on each deposit or share account showing each transaction involving the account;
- the original or copy of each document granting signature authority over each deposit or customer account;
- the original or copy of each item (including checks, drafts, or transfers of credit) relating to a transaction of more than USD 10,000 remitted or transferred to a person, account or place outside the U.S.;
- the original or copy of each check or draft in an amount in excess of USD 10,000 drawn on or issued by a foreign bank which the domestic bank has paid or presented to a non-bank drawee for payment;
- each item relating to any transaction, including a record of each receipt of currency, other monetary instruments, checks, or investment securities and of each transfer of funds or credit, of more than USD 10,000 received on any one occasion directly and not through a domestic financial institution from a bank, broker or dealer in foreign exchange outside the U.S. or from any person, account or place outside of the U.S.;
- the original or copy of records prepared or received by a bank in the ordinary course of business which would be needed to reconstruct a demand deposit account and to trace a check in excess of USD 100 deposited in such demand deposit account through its domestic processing system or to supply a description of a deposited check in excess of USD 100;
- a record containing the name, address and taxpayer identification number, if available, of any person presenting a certificate of deposit for payment, as well as a description of the instrument and the date of the transaction;
- the original or copy of each deposit slip or credit ticket reflecting a transaction in excess of USD 100 or the equivalent record for direct deposit or other wire transfer deposit transaction including the amount of any currency involved;
- blotters, ledgers, or records of original entry regarding all purchases and sales of securities, all receipts and deliveries of securities, all receipts and disbursements of cash and all other debits and credits, with respect to cash and margin accounts; and
- a memorandum of each brokerage order, and of any other instruction, given or received for the purchase or sale of securities, whether executed or unexecuted, and copies of confirmations of all purchases and sales of securities.

570. In addition, the U.S. imposes specific recordkeeping obligations on banks and other financial institutions that conduct funds transfers. These are discussed in detail with respect to Special Recommendation VII below.

571. The Federal Banking Agencies do not have separate regulations regarding all transaction records of a financial institution other than those that are required by the Bank Secrecy Act and its regulations. In section 1829(b)(1) of the Federal Deposit Insurance Act, the U.S. Congress authorized the U.S. Treasury to prescribe regulations for the maintenance of bank records that have been determined to have "a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." Regulation 31 CFR 103.34(b) describes the category of records that satisfy these requirements.

Securities sector

572. The basic BSA provisions that are applicable to the securities sector in relation to record keeping are similar to those described above for the banking sector. However, the BSA includes a

section regarding additional records to be made and retained for five years by securities broker-dealers in which it also incorporates other records by reference to 17 CFR 240.17a-3 (31 CFR 103.35). Securities broker-dealers are required to make and keep current books and records detailing, among other things, securities transactions, money balances, securities positions, and emails. They also must keep records for required periods and furnish copies of those records to the SEC on request. In addition, securities broker-dealers must notify the SEC and the appropriate SRO regarding recordkeeping and other operational problems, and in some cases file reports regarding those problems, within certain time periods (17 CFR 240.17a-2, 240.17a-7, 240.17a-8, 240.17a-10 and 240.17a-13). Institutions are required to preserve these records in an easily accessible place for the first two years (17 CFR 240.17a-4).

573. Futures commission merchants (FCM) and introducing brokers in commodities (IB-C) are required to keep full, complete and systematic records along with all relevant data and memoranda of all transactions relating to its business dealings in commodity futures, commodity options and cash commodities (17 CFR 1.32-37). Such records should include all orders (filled, unfilled or cancelled), trading cards, signature cards, street books, journals, ledgers, canceled checks, copies of confirmations, copies of statements of purchase and sale and all other records, data and memoranda prepared in the course of business dealing in commodity futures, commodity options and cash commodities. FCMs and IB-Cs are also required to maintain records of all securities and property received from customers or option customers in lieu of money to margin, purchase, guarantee or secure the commodity, or commodity option transactions of those customers.

Insurance Sector

574. Record keeping by insurers appears to be limited to the SAR [31 CFR.103.16(e)] and Form 8300 and related documents, which must be kept for five years from the date of filing and which must be made available to FinCEN and other appropriate law enforcement and supervisory authorities, on request [s.103.16(e)]. Insurance companies also are required to retain all records that support their AML program, e.g., the program itself and all records regarding customers, information relating to the customers, and records showing training and audits.

575. Requirements imposed at the state level may vary from state to state. For instance, in California, under Section 10508 of the California Insurance Code, every insurer in the state is required to maintain records related to the activities of its life, life and disability and disability agents for examination by the Commissioner. Records are required to be delivered within 30 days of receipt of the written request. The records may be maintained in originals, carbon copies, facsimile copies, microfilm copies or electronic data processing records, as long as printouts are readily available. Records are to be maintained for a minimum of five years and kept readily available for inspection as all times. Civil penalties are applied for non-compliance.

Money services business sector (including money remitters and foreign exchange)

576. The BSA requires MSBs to collect, and retain for a period of at least five years, certain information for reports and records specified in the Act. Records, including supporting documents, must be kept relating to the following.

(a) Currency transactions involving more than USD 10,000 in currency during any one day by or on behalf of one person (31 CFR 103.22): The information required includes name, address taxpayer identification number and details of the transaction (31 CFR 103.28).

(b) Suspicious activity involving USD 2,000 or more in funds or other assets, or USD 5,000 for issuers of traveler's checks or money orders reviewing clearance records: However, this record keeping requirement does not apply to check cashers (31 CFR 103.20). A copy of the SAR and the supporting documentation must be retained.

(c) Purchases of bank checks and drafts, cashier's checks, money orders and travelers checks instrument involving currency in amounts of USD 3,000 to USD 10,000 inclusive (31 CFR 103.29): The information required includes the name, address, social security number and date of birth of the purchaser in addition to the data relating to the transaction.

(d) Each funds transfer of USD 3,000 and more (31 CFR 103.33): The information required includes the name and address of the transmitter and the recipient, together with details of the transfer (see further discussion below on SR VII).

Special Recommendation VII (Wire transfers)

577. Wire transfers have been monitored in the U.S. since the introduction of the recordkeeping requirements and the "Travel Rule" (described below), which required financial institutions in the U.S. to include originator information in all wire transfers equal to, or greater than, USD 3,000, other than transactions exempted under 31 CFR 103.11(jj).

Obligations on the originating institution to obtain and maintain information

578. For each payment order in the amount of USD 3,000, handled by a bank, the ordering institution must obtain and retain the following records [31 CFR 103.33(e)(1)(i)]:

(a) name and address of the originator;

(b) amount of the payment order;

(c) execution date of the payment order;

(d) any payment instructions received from the originator;

(e) identity of the beneficiary's institution; and

(f) information, if any, that was provided to identify the beneficiary.

579. If the originator of a payment order is not an established customer of the bank, the ordering institution must obtain and retain not only the information listed above, but also the following additional information, depending on whether or not the payment order is made in person [31 CFR 103.33(e)2)]. If an originator that is not an established customer makes the payment order in person, the ordering institution must verify the identity of the person placing the payment order before it accepts the order. If it accepts the payment order, the ordering institution must obtain and retain a record of the following:

(a) name and address of the person placing the order;

(b) type of identification reviewed;

(c) number of the identification document (e.g. driver's license); and

(d) the person's taxpayer identification number (TIN) [e.g. Social Security number (SSN) or employer identification number (EIN)] or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. If the originator's bank has knowledge that the person placing the payment order is not the originator, the originator's bank must obtain and record the originator's TIN (e.g. SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation of the lack thereof.

580. If an originator that is not an established customer does not make the payment order in person, the ordering institution must obtain and retain a record of the following:

(a) name and address of the person placing the payment order; and

(b) the person's TIN (e.g. SSN or EIN) or, if none, the alien identification number or passport number and country of issuance , or a notation in the record of the lack thereof, and a copy or record of the method of payment (e.g. check or credit card transaction) for the funds transfer. If the originator's bank has knowledge that the person placing the payment order is not the originator, the originator's bank must obtain and record the originator's TIN (e.g. SSN or EIN) or, if none, the alien identification number or passport number and country of issuance, or a notation of the lack thereof.

581. Separate, but similar, provisions relate to transmittals of funds by non-bank financial institutions [31 CFR 103.33(f)]. It should be noted that insurance companies do not execute funds transfers.

The Travel Rule

582. Financial institutions in the U.S. are required to include, if received from the sender, originator information collected under the recordkeeping rule that will travel throughout the payment chain in all domestic and cross-border wire transfers of USD 3,000 or more. This is commonly known as the "Travel Rule" In addition to the information collected by the originating institution, as described above, any intermediary institution must also pass on as many of the following items that as are received with the payment order;

(a) name and address of the beneficiary;

(b) account number of the beneficiary; and

(c) any other specific identifier of the beneficiary.

583. Intermediary financial institutions have no duty to obtain information not provided by the transmitter's financial institution or the preceding financial institution.

584. The beneficiary institution also has defined record-keeping responsibilities (31 CFR 103.33). The beneficiary's institution must keep the original or a copy of each payment order of USD 3,000 or more. In addition, if the beneficiary is not an established customer of the bank, the institution must retain the following information for each payment order of USD 3,000 or more, depending on whether the proceeds are delivered in person or not. If the proceeds are delivered in person to the beneficiary or its representative or agent, the beneficiary institution must verify the identity of the person receiving the proceeds and retain a record of the following:

(a) name and address;

(b) the type of document reviewed;

(c) the number of the identification document;

(d) the person's TIN, or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof; and

(e) if the institution has knowledge that the person receiving the proceeds is not the beneficiary, the institution must obtain and retain a record of the beneficiary's name and address, as well as the beneficiary's identification.

585. If the proceeds are not delivered in person to either the beneficiary or its representative or agent, the beneficiary institution must retain a copy of the check or other instrument used to effect the payment, or the institution must record the information on the instrument. The institution must also record the name and address of the person to whom it was sent.

586. Certain transactions and transmittals of funds can be exempted from the requirements of the record keeping requirements [31 CFR 103.33(e) and (f)] under the following circumstances—if the originator and the beneficiary are:

(a) banks, securities broker–dealers, futures commission merchants, introducing brokers in commodities, or their wholly-owned domestic subsidiaries;

(b) government entities; or

(c) the same person and the transmittal involves a single bank, securities broker-dealer, futures commission merchant, introducing broker in commodities [31 CFR 103.33(e)(6) and (f)(6)].

587. In all cases, records of the information must be stored at a location that would facilitate easy retrieval and allow them to be accessible within a reasonable amount of time. In addition, they generally must be retrievable by name of the originator, transmitter, beneficiary or recipient and in cases where established customer relationships exist, by the account numbers used by the customer. Records must be maintained for a period of five years as required under the BSA.

588. Recent legislation has revised the statutory authority regarding records of wire transfers to allow for additional reporting to FinCEN of certain cross-border transmittals of funds if the Secretary of the Treasury determines that such reporting is "reasonably necessary to conduct the efforts of the (Treasury Department) against money laundering and terrorist financing" (s.6302 of the Intelligence Reform and Terrorism Prevention Act of 2004).[63]

589. Transfers that are not accompanied by complete originator information may result in additional due diligence, including contacting the sending institution for further information, or the filing of a SAR. Although a beneficiary financial institution is not required to obtain complete originator information if it is not received with a wire transfer, when there are other indicia of suspicious activity, the financial institution will need to conduct follow-up investigations to determine if the preparation of a Suspicious Activity Report is required and file the form in accordance with regulation, if deemed necessary. The adoption of risk-based procedures for identifying and handling such wire transfers is part and parcel of the risk-based policies, procedures, and processes banks are to adopt for reporting suspicious transactions. The FFIEC manual (page 290) specifically identifies the following as a money laundering and terrorist financing red flag: "Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected."

Batch transfers

590. The U.S. ACH system is a nationwide electronic payments system used by more than 20,000 participating financial institutions, covering 4 million corporations and 145 million consumers. More than 12 billion ACH payments were made in 2004, a 20% increase over 2003.[64] Consumers initiated almost one billion ACH payments via the Internet, worth more than USD 300 billion last year, which was a 40.4% increase over 2003.[65] The Federal Reserve Banks' FedACH International (FedACHi) transactions are a relatively new method for making cross-border payments. FedACHi transactions represent only a tiny fraction of both total ACH transactions in the U.S. and total cross-border payments involving the U.S. According to National Automated Clearing House Association (NACHA) (which is the private sector rule-making body for the U.S. ACH system), 13.9 billion ACH payments were made in 2005. More than 99.99% of these transactions were entirely domestic (both the originating and receiving financial institutions were in the U.S.). There were only 427,000 cross-border FedACHi transactions in 2005. Of this amount, fewer than 3% were commercial transactions. The rest were U.S. government payments. Approximately 75% of all FedACHi payments are between

[63] In accordance with this Act, FinCEN will provide Congress with a feasibility report on this issue. This report should assess what additional information would support U.S. efforts to identify money laundering and terrorist financing, and the situations in which reporting would be required.

[64] Source: The National Automated Clearing House Association.

[65] Ibid.

the U.S. and Mexico. Within the ACH system, these participants and users are known by the following terms.

(a) "Originators" are the organizations or persons that initiate an ACH transaction and either receive funds from the receiver's account or credit funds to the receiver's account.

(b) "Originating Depository Financial Institutions" (ODFIs) are the depository financial institutions for the originators that forward ACH transactions into the national ACH network through an operator.

(c) "Operators" are the two intermediary organizations (the Federal Reserve Banks and the Electronic Payments Network) that process all ACH transactions that flow between different depository financial institutions.

(d) "Receiving Depository Financial Institutions" (RDFIs) are the depository financial institutions that receive the ACH transaction from the operators and the national network and credit or debit funds from their receivers' accounts.

(e) "Receivers" are the organizations or persons that authorize the initiation of an ACH transaction and either receive funds from the originator or have funds debited from their accounts that are credited to the originator.

591. The Federal Reserve Banks are collectively the largest automated clearinghouse operators in the U.S. and, in 2004, processed more than six billion commercial inter-bank ACH transactions through their FedACHSM service to depository institutions. Agreements are in place between ACH operators and their customers. The Federal Reserve Banks, for example, issue a standard operating circular that serves as a legal agreement with their ACH customers. Finally, ODFIs and their originators, and RDFIs and their receivers, establish bilateral agreements (either as part of their account agreements or separately) with respect to their use of the ACH system. As part of these agreements, the depository financial institutions and their customers agree to follow the rules of the NACHA. The Electronic Payments Network (EPN) is the only private-sector ACH operator that processes ACH transaction. EPN operates through legal contracts with its customers. Along with the Federal Reserve Banks, EPN offers a variety of products and services to manage ACH payments risk.

592. The NACHA issues and is responsible for the primary legal agreement binding ACH participants and users for commercial ACH payments. NACHA is a non-profit private-sector organization with a rulemaking board made up of a limited set of voting members. The NACHA Operating Rules, revised throughout the year and published annually, govern all interregional ACH transactions and those intraregional ACH transactions not implemented by a local rule. NACHA board members create and amend the operating rules. The twenty regional ACH associations around the country are each full voting members of NACHA board. The twenty regional ACH associations represent more than 11,000 depository financial institutions across the country.

593. ACH transactions are batch transfers that are transmitted in electronic files between customers and their financial institutions and among financial institutions and ACH operators. Within each file are batches of individual ACH payment records and their related addenda records. These ACH files, batches, records, and addenda records are formatted in accordance with specifications in the NACHA Rules to include various types of data and information.

594. Other applicable rules and regulations include: regulation 31 CFR 210 (for government ACH payments); The Green Book (an annual publication of detailed operational procedures for government ACH payments that is issued by the Financial Management Service (FMS) of the Treasury); the Electronic Fund Transfer Act (EFTA) and its implementing regulation (Regulation E) (for consumer ACH transactions); and Article 4A of the Uniform Commercial Code (for non-consumer ACH credit transactions).

595. The revised Interpretive Note to SRVII (adopted in October 2005) states that where several individual wire transfers from a single originator are bundled in a batch file for transmission to

beneficiaries in another country, they shall be exempted from including full originator information, provided they include the originator's account number or unique reference number (as described in paragraph 8 of the Interpretative Note), and the batch file contains full originator information that permits the transaction to be traced within the recipient country. The Interpretive Note recognizes that countries will need time to make relevant legislative or regulatory changes and to allow financial institutions to make necessary adaptations to their systems and procedures, and further states that this period should not extend beyond December 2006.

596. Current NACHA rules enable financial institutions to include all originator identification information required by SR VII. Specifically, the current NACHA formatting and data inclusion rules mandate the inclusion of the originator's name and permit the inclusion of the originator's address and account number with each ACH transaction record or its associated addenda record. In addition, each cross-border ACH transaction record and its associated addenda record contain a reference or trace number that ties them together as well as to a specific batch within a particular ACH file. The current NACHA cross-border ACH rules also mandate the inclusion of the receiver's (beneficiary's) account number, require the receiver's name, and permit the inclusion of the receiver's address within either the cross-border ACH transaction record or its associated addenda record.

597. NACHA is in the process of developing and approving a rule that would mandate cross-border ACH transfers to meet the new requirements created by the revised Interpretive Note to SRVII.[66]

Applicable threshold

598. The U.S. applies a threshold of USD 3,000 for recordkeeping associated with wire transfers and other payment orders. FinCEN is evaluating the utility of the current threshold and exploring the feasibility of lowering the threshold to USD 1,000 in line with the revised Interpretive Note to SR VII. No timeframe has been established for completing this review; however, the revised Interpretive Note to SR VII recognizes that countries will need time to make relevant legislative or regulatory changes and to allow financial institutions to make necessary adaptations to their systems and procedures, and further states that this period should not extend beyond December 2006.

Statistics relating to wire transfers

599. No statistics are available concerning the volume of wire transfer activity into or out of the U.S. annually. Such transactions are only specifically recorded if a SAR (wire transfer fraud, unusual use of wire transfer as a violation category or suspicious wire transfer activity recorded in the narrative) has been made. Statistics on wire transfer fraud and unusual use of wire transfer as recorded on SARs are routinely recorded in the FinCEN publication, "Suspicious Activity Reports – By The Numbers". A summary of that information is reflected below.

Suspicious Activity Reports: Wire Transfer as Violation Category				
	Depository Inst.	MSB	Casino	Security/Futures
2000	972	Not Available	4	Not Available
2001	1,527	Not Available	9	Not Available
2002	4,747	Not Available	11	Not Available
2003	6,660	Not Available	54	Not Available
2004*	1,553	Not Available	27	589

*Through June 2004

[66] Changes being considered in the ongoing NACHA rulemaking process would mandate the inclusion of all originator and receiver information within each cross-border ACH transaction record and its associated addenda records so that it could be made available to a receiving gateway operator in another country. This would ensure that full originator information is available and fully traceable within the recipient country, as required by paragraph 7 of the Interpretive Note to SR VII.

Monitoring compliance with Special Recommendation VII

600. Each of the Federal Banking Agencies, the SEC and the SROs has authority to monitor for compliance with BSA requirements, including the wire transfer regulations. Examiners assess the banking organization's compliance with U.S. statutory and regulatory requirements for funds transfers. This includes determining whether an audit trail of funds transfer activities exist and verifying that the organization transmitted payment information as required by U.S. regulation (FFIEC Manual Core Examination Procedures-Funds Transfers, page 196). There appear to be no reliable indicators on the number of wire transfers that lack the relevant information. In the securities sector, auditing by the SROs in relation to implementation of the travel rule found only a limited number of deficiencies overall.

Sanctions

601. Treasury (through FinCEN) has statutory authority under the BSA to take sanctions in this area. Each of the Federal Banking Agencies has the statutory authority under various provisions of Section 8 of the Federal Deposit Insurance Act, 12 USC 1818(b), (c), (e), and (i), and the SEC has authority under the Securities Exchange Act and the Investment Company Act to impose regulatory sanctions against noncompliant financial institutions and institution-affiliated parties. This includes the ability to take appropriate supervisory or enforcement action against financial institutions for non-compliance with the record keeping and Travel Rule requirements. Federal and state banking supervisors have indicated that no specific verification or audit has been performed, but according to some representative of the U.S. private sector about 50% of the incoming wire transfers are received with incomplete originator information. FinCEN has not sanctioned a financial institution directly for violations of the record-keeping requirements for wire transfers. However, FinCEN has assessed civil money penalties for failure to implement adequate anti-money laundering program measures with respect to wire transfers. Specifically, recent enforcement actions have been based, in part, on failures to implement adequate systems and controls and other measures to ensure compliance with the SAR requirements for wire transfer transactions.

Additional elements

602. When a bank processes a transaction for a correspondent bank, the regulations require transaction details to be maintained in the bank's records and also passed along to the next correspondent (if any). While the bank would not be expected to interrupt an automated transfer, it would be expected to review, whether manually or automatically, its transactions to identify any suspicious transaction. Even if the bank could fulfill its recordkeeping obligations, if the payment order lacked sufficient information to enable the U.S. institution to perform its due diligence obligations and comply with SARs obligations, the bank might need to conduct follow-up investigation and contact the correspondent bank.

603. Finally, all financial institutions are subject to U.S. law prohibiting the conduct of transactions for any person whose assets are required under U.S. law to be blocked or frozen. These requirements generally do require the interruption of automated transfers, and they are generally implemented by means of filtering software that is designed for use with automated wire transfer systems.

3.5.2 Recommendations and Comments

604. The U.S. is mostly compliant with the standard record-keeping requirements of Recommendation 10. Life insurers are only required to keep limited records relating to their AML Program, and SAR and Form 8300 reporting requirements. The U.S. should extend full record-keeping requirements to the insurance sector, including insurance brokers and agents. Overall, the record-keeping requirements appear extremely complex with an excessive number of separate obligations, applicable to different sectors and different types of transactions. The U.S. may wish to consider simplifying this framework, thereby reducing the burden on institutions to have to identify each and every discrete obligation.

605. With regard to Special Recommendation VII, the failure to implement a USD 1,000 threshold impacts on the effectiveness of the U.S. system, particularly given the risks identified with low value wire transfers.[67] As well, the failure to require all of the originator information to be attached to the batch file (as required by SR VII) is a concern, given the very high volume of batch transfers that are processed through the U.S. ACH system (USD 300 billion worth of batch payments in 2005). The U.S. should ensure that NACHA completes its current process of developing and approving a rule that would allow cross-border ACH transfers to meet the new FATF requirements with respect to batch transfers before January 2007, in accordance with the revised Interpretive Note to SRVII. Similarly, the U.S. should lower the threshold to USD 1,000 before January 2007.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	LC	• Life insurers of covered products are only required to keep limited records of SARs, Form 8300s, their AML Program and related documents.
SR.VII	LC	• Threshold of USD 3,000 instead of USD 1,000 as is required by the revised Interpretative Note. • It is not mandatory to include all required originator information on batch transfers.

4. ***Unusual, Suspicious and other Transactions***

3.6 Monitoring of transactions and relationships (R.11 & 21)

3.6.1 Description and Analysis

Recommendation 11 (Attention to unusual transactions)

Banking and Securities sectors

606. Banks (as broadly defined), securities broker-dealers, futures commission merchants and introducing brokers in commodities are obligated under the BSA to file suspicious activity reports, and reports on a number of specified types of transactions. Regulation 31 CFR 103.18 characterizes the obligation, in part, as one where "the bank knows, suspects, or has reason to believe that…the transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the facts available, including the background and possible purpose of the transaction". As a result, the FFIEC Manual (p.41) states that, as part of their AML compliance program, financial institutions must have appropriate policies, procedures and processes in place to monitor and identify unusual activity, with particular emphasis on high-risk products, services, customers and geographic locations. In addition, NASD NtM 02-21 specifies a number of red flags that indicate suspicious activity in the securities sector, including transactions that have no apparent economic, business, or lawful purpose, unusual patterns of transactions (such as excessive journal entries between unrelated accounts without any apparent business purpose or transactions that appear to be structured to avoid government reporting requirements), and complex and large transactions.

607. All of these written records must be retained by the reporting financial institution for at least five years.

608. With respect to complex, unusual, large transactions that do not result in the filing of a BSA form, the FFIEC Manual (p.41) states that "after thorough research and analysis, decisions to file or not to file a SAR should be documented". In cases of non-filing, such documentation would then be available to

[67] As mentioned in the revised Interpretative Note to Special Recommendation VII, it is recognized that countries will need time to make relevant legislative or regulatory changes and to allow financial institutions to make necessary adaptations to their systems and procedures. This period should not extend beyond December 2006.

supervisors during examinations, and in cases where SARs are filed, FinCEN and law enforcement have immediate access. The legal provisions that are applicable to broker-dealers require that reports produced to review for unusual activity in customer accounts (commonly referred to as "exception reports") be preserved in a form that can be provided to a representative of the SEC or an SRO. [17 CFR 240.17a-4(e)(8)] Firms are generally required to review these exception reports and determine whether further investigation into the account holders or transactions is required. [31 CFR 103.19].

609. Mutual funds are required to develop and implement a written AML program. An effective AML Program must monitor customer and shareholder accounts for suspicious and unusual transactions. The five (or more) year retention requirement for mutual funds is applicable to BSA records, including records related to suspicious and unusual transactions. Mutual funds track 'red flags' that identify questionable transactions and the appearance of a red flag will tag an account and generate an exception report. Mutual funds are required to review these reports and determine whether further investigation into the account holders or transactions is required.

Insurance and MSB sectors

610. The legal provisions that are applicable to the insurance and MSB sectors in relation to monitoring for suspicious activity are the same as those described above for the banking and securities sectors.[68]

Recommendation 21 (Countries that apply the FATF Recommendations insufficiently)

General

611. Section 311 of the USA PATRIOT Act granted the Secretary of the Treasury the authority, upon finding that reasonable grounds exist for concluding that a foreign jurisdiction, institution, class of transactions, or type of account is of "primary money laundering concern," to require domestic financial institutions to take certain "special measures" against the primary money laundering concern. The authority to take such action has been delegated to the Director of FinCEN. Section 311 establishes a process for FinCEN to follow, and identifies federal agencies to consult before FinCEN may conclude that a subject is of primary money laundering concern. The statute also provides similar procedures, including factors and consultation requirements, for selecting and imposing specific special measures.

612. Before making a finding that reasonable grounds exist for concluding that a foreign financial institution is of primary money laundering concern, the Secretary is required by the BSA to consult with both the Secretary of State and the Attorney General. The Secretary also is required by section 311 to consider ''such information as the Secretary determines to be relevant, including the following potentially relevant factors:

(a) the extent to which such financial institution is used to facilitate or promote money laundering in or through the jurisdiction;

(b) the extent to which such financial institution is used for legitimate business purposes in the jurisdiction; and

(c) the extent to which the finding that the institution is of primary money laundering concern is sufficient to ensure, with respect to transactions involving the institution operating in the jurisdiction, that the purposes of the BSA continue to be fulfilled, and to guard against international money laundering and other financial crimes."

613. Section 311 provides a range of special measures that can be imposed individually, jointly, in any combination, and in any sequence. These are implemented through various orders and regulations that are incorporated into 31 CFR Part 103. The measures listed under section 311 are as follows.

[68] In order to clarify the requirements in relation to the monitoring of unusual transactions and associated record-keeping, FinCEN is publishing in May 2006 an FAQ in its SAR Activity Review- Trends, Tips & Issues to confirm that the statement in the FFIEC manual applies to all financial institutions subject to a SAR rule.

(i) Recordkeeping and Reporting of Certain Financial Transactions

614. FinCEN may require domestic financial institutions and domestic financial agencies to maintain and/or to file reports concerning the aggregate amount of transactions or the specifics of each transaction with respect to a subject that is of the primary money laundering concern. The records and reports shall include whatever information FinCEN deems to be relevant, including, but not limited to:

(a) the identity and address of the participants in the transaction or relationship;

(b) the legal capacity in which the participants are acting;

(c) the identity of the beneficial owner of the funds involved; and

(d) a description of the transaction.

(ii) Information Relating to Beneficial Ownership

615. FinCEN may require domestic financial institutions and domestic financial agencies ''to take such steps as FinCEN may determine to be reasonable and practicable to obtain and retain information concerning the beneficial ownership of any account opened or maintained in the U.S. by a foreign person (other than a foreign entity whose shares are subject to public reporting requirements or are listed and traded on a regulated exchange or trading market)'' or a representative of such foreign person, that involves a subject that is of primary money laundering concern.

(iii) Information and Action Relating to Certain Correspondent and Payable-Through Accounts

616. FinCEN may require domestic financial institutions and domestic financial agencies that open or maintain a correspondent or payable-through account in the U.S. involving a subject that is of primary money laundering concern to: (1) identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and (2) obtain information about each such customer (and representative) that is substantially comparable to that which a U.S. depository institution obtains in the ordinary course of business with respect to its customers residing in the U.S. As is most often the case, FinCEN, after the respective consultations, can also prohibit, or impose conditions on, domestic financial institutions and financial agencies opening or maintaining such accounts in the U.S.

617. Pursuant to Section 311, any of the above information-gathering or reporting measures can be imposed by order, regulation, or as otherwise "permitted by law." If an order is issued, it can remain in effect for 120 days, unless authorized by a regulation promulgated before the end of the 120-day period. Prohibiting or conditioning the opening or maintenance of correspondent and payable through accounts can only be imposed through the issuance of a regulation. Thus far, Treasury has issued four final rulemakings (three against foreign financial institutions, and one against a jurisdiction); seven determinations of primary money laundering concern (one of which was subsequently withdrawn); and six proposed rules (five against foreign financial institutions and one against a jurisdiction).

618. Outside the specific powers granted under the USA PATRIOT Act, the U.S. uses a number of channels to advise financial institutions about concerns in the AML/CFT systems of other countries. These include the following:

(a) **Alerts:** The Federal Banking Agencies and Treasury periodically issue alerts, advisories and rulemakings concerning institutions or individuals who may be engaged in fraudulent activities or be deemed to be of high-risk for money laundering or terrorist financing activities..

(b) **Secure Web Sites:** Secure web-sites maintained by the Federal Banking Agencies provide access to authorized user to various information on potential terrorist activity that the FBI or other law enforcement agencies may issue.

(c) **FinCEN Advisories:** FinCEN issues Advisories to financial institutions operating in the U.S. advising them, among other things, to give enhanced scrutiny to all financial transactions originating in or routed to or through certain identified countries, in which there are concerns about weaknesses in the AML/CFT systems.

(d) **FATF NCCTs:** Institutions are directed to pay attention to the NCCT listing.

(e) **International Narcotics Control Strategy Report (INCSR):** The INCSR, published annually in March by the State Department, identifies major money laundering countries and jurisdictions. The INCSR's mandate is to address money laundering related to narcotics trafficking. Given the difficulty of identifying the specific crime from which the illegal proceeds emanate, the INCSR, however, discusses money laundering from all relevant crimes. Additionally, the INCSR now addresses each jurisdiction's efforts to deter terrorist financing, and includes a prescriptive paragraph for each country. This report now includes summaries and comparative analyzes on more than 130 governments.[69]

(f) **OFAC Sanctioned Countries & SDNs:** OFAC is responsible for issuing regulations that restrict transactions by U.S. persons or entities (including banks) with certain foreign countries, their nationals, or SDNs. Violations of these laws can expose financial institutions to substantial penalties.

(g) **Other publications:** A list of the countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State appears in the State Department's annual report "Patterns of Global Terrorism."

Banking sector

619. The AML Program requirements that apply to U.S. financial institutions are risk-based. Thus, a financial institution's AML policies, procedures, and processes are expected to be commensurate with the financial institution's risk profile, paying particular attention to high-risk customers and other risk factors. In the FFIEC Manual (p.20) indicators of high-risk geographical locations are deemed to include:

(a) countries subject to OFAC sanctions, including state sponsors of terrorism;

(b) countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State;

(c) jurisdictions determined to be "of primary money laundering concern" by FinCEN, through authority delegated to FinCEN by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act;

(d) jurisdictions/countries identified as non-cooperative by the FATF;

(e) major money laundering countries and jurisdictions identified in the State Department's annual INSCR, in particular, countries that are identified as jurisdictions of primary concern;

(f) offshore financial centers (OFCs) as identified by the State Department; and

(g) other countries identified by the financial institution as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

[69] On 6 March 2006, the House passed legislation (The Regulatory Relief Act) which, if approved, by the Senate and enacted into law, would require the Treasury to publish annually a report that "identifies the applicable standards of each country against money laundering and states whether that country is a country of primary money laundering concern". The assessment would have to include "a determination of whether the efforts of a country to combat money laundering and terrorist financing are adequate or inadequate".

620. Transactions identified as unusual must be treated in accordance with the general procedures for dealing with such cases (see the above discussion of Recommendation 11).

Securities sector

621. The general provisions described above apply to the securities industry. While the guidance contained in the FFIEC Manual does not apply to the securities sector, broker-dealers are required to perform additional due diligence before proceeding with a transaction involving a customer that is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF. (NASD Notice to Members 02-21, page 10)

Insurance sector

622. Section 103.137(c) requires an insurer to develop a risk-based AML Program that considers all relevant factors affecting risks inherent in its covered products, including whether it issues or underwrites covered products to persons in a jurisdiction, among others, that has been designated by the FATF as non-cooperative with international AML principles.

Money Services Business sector (including money remitters and foreign exchange)

623. According to an interpretive release published in the Federal Register in December 2004 (69 FR 74439), MSBs that utilize foreign agents or counterparties, must have AML Programs that include risk-based policies, procedures, and controls designed to identify and minimize money laundering and terrorist financing risks associated with foreign agents and counterparties that facilitate the flow of funds into and out of the U.S. These obligations extend to all foreign agents or counterparties—not just those who are located in countries that may not or insufficiently apply the FATF Recommendations. The specific requirements are described in section 3.8.1 below.

Countermeasures

624. Countermeasures are available and have been applied. Treasury (through FinCEN) has utilized its authority under section 311 on several occasions to designate financial institutions and jurisdictions of primary money laundering concern. On each such occasion, it has gone beyond imposing the requirement to obtain information on beneficial ownership, and instead has prohibited the opening or maintaining of correspondent accounts with such financial institutions or institutions in such jurisdictions. To date, the Treasury has applied Section 311 to specific jurisdictions on three occasions, each in support of the FATF Non-Cooperative Countries and Territories (NCCT) process, by issuing a finding of primary money laundering concern against Ukraine, Nauru and Burma. In the case of Ukraine, Treasury ultimately revoked its finding of primary money laundering concern owing to rehabilitative measures undertaken by Ukraine and the subsequent removal of Ukraine from the FATF's NCCT list. In the cases of Nauru and Burma, Treasury issued proposed rules that would require U.S. financial institutions to terminate and prohibit any and all correspondent accounts with any financial institution organized or licensed under the laws of that jurisdiction. In the case of Burma, Treasury issued a subsequent final rule requiring U.S. financial institutions to terminate and prohibit any and all correspondent accounts with any financial institution organized or licensed under the laws of that jurisdiction. Treasury has also applied Section 311 in a targeted fashion by designating a number of foreign financial institutions as primary money laundering concerns, and by issuing associated proposed and final rules terminating and prohibiting correspondent accounts with these designated foreign financial institutions, and prohibiting the use of existing correspondent accounts for the benefit of these designated foreign financial institutions.

3.6.2 Recommendations and Comments

625. The U.S. is largely compliant with Recommendation 11. However, the requirement to establish and retain (for five years) written findings that relate to unusual transactions should be extended to those participants in the securities sector that are currently not subject to a requirement to file SARs.

626. The U.S. is compliant generally with Recommendation 21. However, in the insurance sector, the U.S. should require institutions to establish and retain written records of transactions with persons from/in countries that do not or insufficiently apply the FATF Recommendations to the extent that this is not already addressed by the AML program and SAR requirements as discussed above. Additionally, these requirements should be extended to those participants in the securities sector that are currently not covered.

3.6.3 Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating
R.11	LC	• In the insurance, and MSB sectors, there is no specific requirement to establish and retain (for five years) written records of the background and purpose of complex, unusual large transactions or unusual patterns of transaction that have no apparent or visible economic or lawful purpose (outside of the SAR, CTR and Form 8300 requirements) • No measures have been applied to investment and commodity trading advisers.
R.21	LC	• In the insurance sector, there is no specific requirement to establish and retain written records of transactions with persons from/in countries that do not or insufficiently apply the FATF Recommendations. • No measures have been applied to investment and commodity trading advisers

3.7 Suspicious transaction and other reporting (R.13-14, 19, 25 & SR.IV)

3.7.1 Description and Analysis[70]

Recommendation 13 and Special Recommendation IV (Suspicious transaction reporting)

627. FinCEN has issued federal regulations implementing 31USC 5318(g) that require a broad range of financial institutions to report suspicious transactions and apply equally to transactions related to money laundering and terrorist financing.[71] These regulations apply to banks (as broadly defined) (through regulations initially adopted in 1996), securities broker-dealers (through regulations adopted in 2002), MSBs, except check cashers (through regulations adopted in 2000), futures commission merchants and introducing brokers in commodities (through regulations adopted in 2003) and insurance companies (through regulation adopted in 2005 which came into force on 2 May 2006). FinCEN is in the process of finalizing rules that would also require mutual funds to file reports of suspicious transactions.

628. Separately under Title 12, all the Federal Banking Agencies require the financial institutions that they supervise to file suspicious transaction reports with FinCEN (e.g. 12 CFR 208.62 with respect to banks regulated by the Federal Reserve). Federal Banking Agency rules apply to banks, bank holding companies, and non-depository institution affiliates and subsidiaries of banks and bank holding companies.

629. Upon conducting a risk analysis, FinCEN determined that it was appropriate to establish certain transactional thresholds with respect to suspicious transaction reporting. For covered financial

[70] The description of the system for reporting suspicious transactions in s.3.7 is integrally linked with the description of the FIU in s.2.5, and the two texts need to be complementary and not duplicative.

[71] There is no separate text relating to SR.IV because all issues of the relevant issues are the same as for R.13 and they are rated on the same basis.

institutions other than money services businesses, suspicious transactions must be reported only when they involve, singly or in aggregate, at least USD 5,000. MSBs must generally report suspicious transactions when they involve or aggregate at least USD 2,000, but the threshold is USD 5,000 for the issuers of money orders or travelers' checks when they identify suspicious activity from a review of the clearance records.

630. Subject to these monetary thresholds, a bank, securities broker-dealer, futures commission merchant, introducing broker in commodities, insurance company or MSB must file a SAR, if it knows, suspects, or has reason to suspect that:

(a) the transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law;

(b) the transaction is designed to evade any regulations promulgated under the BSA, including structuring to avoid reporting thresholds; or

(c) the transaction has no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

631. A fourth criterion is added with respect to securities broker-dealers, insurance companies and MSB, requiring them to report transactions over the threshold where they identify that the institution is being used to facilitate criminal activity generally [e.g. 31 CFR 103.2(a)(2)(iv) for MSBs].

632. Despite the language of subparagraph (a) above, the suspicious activity reporting rule for banks is not limited to violations of federal law (such as money laundering and terrorist financing offences). Under the regulations of the Federal Banking Agencies and FinCEN, financial institutions must file a SAR on a transaction at the applicable threshold (e.g. USD 5,000 or more for banks) if the financial institution knows, suspects, or has reason to suspect that "the transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds…as part of a plan to violate or evade any law or regulation…" or that "the transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage…" [12 CFR 208.62(c)(4)]. Similarly, the release accompanying the final rule for broker-dealer SAR obligations explicitly states that the broad language used in the rule "should be interpreted to require the reporting of transactions that appear unlawful for virtually any reason...[and that] all criminal violations are required to be reported under the final rule." Thus, the rule requires reporting of known or suspected violations of any law or regulation, not only federal law. Moreover, the regulation does not direct that the determination of whether a transaction has a business or lawful purpose is to be made by reference to federal law. These obligations apply to both attempted and completed transactions.

633. In addition, the SAR form itself identifies particular crimes to be reported that are not confined to federal criminal violations or violations of the BSA. For example, the SAR form lists check fraud, bribery, presenting counterfeit checks, and embezzlement, all of which are generally also violations of state criminal laws.

634. In addition under Title 12, banks have an obligation to file reports with respect to criminal violations involving insider abuse in any amount; criminal violations aggregating USD 5,000 or more when a suspect can be identified; and criminal violations aggregating USD 25,000 or more regardless of a potential suspect. Banks are also "encouraged" under Title 12 to file a copy of their SARs with the state and local law enforcement authorities.

635. Generally, any institution may voluntarily file a SAR under the established threshold specific to their industry when it believes that it is relevant to the possible violation of any law or regulation, but where there is no mandatory reporting obligation [e.g. 31 CFR 103.18(a)(1) for banks].

Preparation of the SAR Form

636. Financial institutions use SAR forms that contain boxes to be checked indicating the particular suspected illegal activity. These boxes correspond to the most common types of suspicious activity, though all forms contain a category marked "other" intended to cover any illegal activity not explicitly listed elsewhere. All of the forms currently contain a category for "terrorist financing", introduced when the form was revised in July 2003.

637. The SAR rules require the financial institution to complete detailed information about the suspect(s) conducting the transaction, the type of suspicious activity, the dollar amount involved, along with any loss to the financial institution, and information about the reporting financial institution. Every SAR form requests a narrative description of the suspect violation and transactions. The narrative is also used to document what supporting information and records the financial institution retains and is considered very critical in terms of explaining the apparent criminal activity to law enforcement and regulatory agencies. The information provided in the narrative should be complete, accurate, and well-organized. It should also contain additional information on suspects, describe instruments and method of facilitating the transaction, and provide any follow-up action by the financial institution.

638. The financial institution is also encouraged to provide a detailed listing of documentation available that supports the SAR filing. All documentation supporting the SAR must be stored by the financial institution for five years and is considered property of the U.S. government.

639. Section 103.16(b)(3)(ii) acknowledges that certain insurance agents and insurance brokers who are also broker-dealers in securities with respect to the sale of variable insurance products may have a separate obligation to report suspicious activity under another section of the BSA. As a result, FinCEN's SAR rule provides for the filing of a joint suspicious activity report where only one of the filing institutions should be identified as the "filer" in the filer identification section in the form. The SAR's narrative must include the words "joint filing" and must identify the other financial institution or institutions on whose behalf the report is being filed.

SAR Filing deadlines and methods

640. By regulation, SAR forms are required to be filed no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of detection of the incident requiring the SAR filing, a financial institution may delay filing for an additional 30 calendar days in order to identify a suspect. In no case shall reporting be delayed more than 60 days after the date of initial detection of a reportable transaction.

641. SARs can be filed in paper form, by magnetic tape, or through BSA E-filing. Financial institutions may contact law enforcement and their financial institution regulatory agency to notify them of the suspicious activity, and these contacts should be noted on the SAR form.

642. In October 2001, FinCEN established a financial institution hotline operational seven days a week, 24 hours a day, for expedited reporting of suspicious transactions that may relate to terrorist activity and transmittal of this information to law enforcement. Use of the hotline is voluntary and is not a substitute for an institution's responsibility to file a SAR in accordance with applicable regulations. FinCEN has also encouraged financial institutions to contact their local FBI field office regarding terrorist-related transactions that require the immediate attention of law enforcement.

Statistics relating to SAR reporting

643. The number of institutions subject to BSA reporting runs in the hundreds of thousands: approximately 29,000 depository institutions (commercial banks, savings and thrift institutions, trust companies, branches of foreign chartered banks doing business in the U.S.) and over 200,000 non-bank financial institutions.

644. As of 30 June 2005, more than 2.6 million SARs had been filed. These filings reveal the following.

(a) Depository Financial Institutions filed 1,921,798 SARs from April 1996 through 30 June 2005.

- The volume of SAR filings in the first six months of 2005 increased 45% over those filed in the same period in 2004.
- The filing category "BSA violations/Structuring/Money Laundering" continues to be the leading suspicious activity in SARs filed by depository institutions.

(b) Money Services Businesses filed 689,462 SARs from October 2002 through 30 June 2005.

- The volume of filings in the first six months of 2005 increased 25% over those filed during the same period in 2004.
- In the first six months of 2005, money transmitters filed 122,218 or 51% of all SARs, followed by issuers of money orders at 38,834 (16%) and sellers of money orders at 23,852 (10%).
- In the first six months of 2005, the characterization of suspicious activity, "alters transaction to avoid filing a CTR form (USD 10,000 or more) increased 132% over the same period in 2004.
- In the first six months of 2005, the characterization of suspicious activity, "offers a bribe in the form of a tip/gratuity" increased 144% over the same period in 2004.
- Filers reported money transfers as the most frequent type of financial service involved in the suspicious activity.

(c) Securities and Futures Industries Firms filed 13,277 SARs from the mandated reporting date of 1 January 2003 through 30 June 2005.

- The volume of SAR filings in the first six months of 2005 increased 27% over those filed during the same period in 2004.
- Between January 2003 and June 2005, the most prevalent characterization of suspicious activity was "Other" (with 4,648 filings or 22.99%), followed by money laundering/structuring at 16.43%.
- In the first six months of 2005, 1,552 filings (58%) reported cash or its equivalent as the type of instrument used in the suspicious activity.
- In the first six months of 2005, 1,580 filings (29%) indicated clearing brokers as the primary type of reporting institution, followed by introducing brokers in commodities with 1,279 filings (23%).

(d) The U.S. Postal Service, one of the largest issuers of money orders, files an average of 47,500 SARs per year relating to postal money orders.

645. The following chart shows the number of SARs filed by depository institutions ranked by suspicious activity, based on filings from 1 April 1996 to 30 June 2004. The category "computer intrusion" was added June 2000 and "identity theft" and "terrorist financing" were added July 2003.

Violation Type	Filings (Overall)	Percentage (Overall)
BSA/Structuring/Money Laundering	769,502	48.22%
Check Fraud	185,839	11.65%
Other	136,021	8.52%
Credit Card Fraud	77,970	4.89%
Counterfeit Check	74,891	4.69%
Check Kiting	55,940	3.51%
Unknown/Blank	46,783	2.93%
Defalcation/Embezzlement	46,323	2.90%
Mortgage Loan Fraud	40,016	2.51%
Consumer Loan Fraud	27,240	1.71%
False Statement	26,724	1.67%
Misuse of Position or Self Dealing	18,460	1.16%
Wire Transfer Fraud	17,634	1.11%
Mysterious Disappearance	17,375	1.09%
Debit Card Fraud	11,315	Less than 1%
Commercial Loan Fraud	10,699	Less than 1%
Identity Theft	10,188	Less than 1%
Computer Intrusion	8,319	Less than 1%
Counterfeit Credit/Debit Card	6,573	Less than 1%
Counterfeit Instrument (Other)	5,142	Less than 1%
Bribery/Gratuity	1,799	Less than 1%
Terrorist Financing	971	Less than 1%

646. The following chart shows the number of SARs filed by each of the different types of reporting institutions from 1996 to 30 June 2005.

SUSPICIOUS ACTIVITY REPORT FILINGS										
	1996	1997	1998	1999	2000	2001	2002	2003	2004	30 June 2005
Depository Institutions	62,388	81,197	96,521	120,505	162,720	203,538	273,823	288,343	381,671	251,092
Securities and Futures Industries	-	-	-	-	-	-	-	4,267	5,705	3,305
Money Services Businesses	-	-	-	-	-	-	5,723	209,512	296,284	177,943

Source: The SAR Activity Review, By The Numbers, Issue 5 February 2006

647. The following chart shows the top ten states for SAR filings from depository institutions from 1 April 1996 through 30 June 2004, which account for two-thirds of all SARs for the period.

Rank	State/Territory	Filings (overall)	Percentage (overall)
1	California	351,784	24.26%
2	New York	167,635	11.56%
3	Texas	92,168	6.36%
4	Florida	89,413	6.17%
5	Illinois	51,004	3.52%
6	Arizona	48,691	3.36%

7	New Jersey	41,403	2.86%
8	Pennsylvania	37,765	2.60%
9	Ohio	34,634	2.39%
10	Michigan	34,506	2.38%

648. Overall, the SAR reporting system has produced impressive results. However, the volume of filings has been uneven across sectors. For instance, large numbers of SARs are being filed by the banking and MSB sectors. However, in the securities sector, the number of filings has been relatively low so far, possibly reflecting the lower risk of laundering cash because the sector does not generally operate on a cash basis. NASD has a webpage devoted to AML/CFT and has issued weekly e-mails to its members (securities brokers) to ensure that they know how to implement their AML/CFT requirements. Concerns were raised by representatives of the banking sector about the risk of defensive filing which could be a reason for the large number of SARs being filed by banks. There have also been reports that improved reporting systems and technology innovations (such as automated transactions monitoring systems) have resulted in an increase in the number and quality of SAR filings. In contrast, the NFA indicated that defensive filings are not a problem in the securities industry which has only been under an obligation to report for about 1.5 years

649. A weakness of the reporting system is the threshold (of USD 5,000 for financial institutions and USD 2,000 for MSBs). This impacts, in particular, the effectiveness of the reporting requirement with respect to terrorist financing-related transactions, as the importance of tracking relatively low-value transactions has been highlighted in this field.

Recommendation 14 (Tipping off)

650. Federal law [31 USC 5318(g)(3)] provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to the SAR instructions. Specifically, the law provides that a financial institution and its directors, officers, employees, and agents that make a disclosure of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the U.S., any constitution, law, or regulation of any state or political subdivision of any state, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold. In the case of the insurance sector (which has newly become subject to a SAR reporting requirement), the safe harbor provision also applies in the following circumstances: (1) reporting suspicious activity not involving any covered life insurance product; and (2) insurance agents and insurance brokers even though they do not have direct responsibility to report suspicious activity under the final rules.

651. The implementing regulations do not require the report to be made in good faith to obtain such protection from liability. This is significant because, in combination with the safe harbor provision, the subject of a SAR would not be able to bring a lawsuit against a SAR filer even under the pretext that the filing was malicious.

652. No financial institution, and no director, officer, employee, or agent of a financial institution, that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. The same prohibition applies to government officials and employees, other than is necessary to fulfill their official duties [31 USC 5318(g)(3)]. Any financial institution that is subpoenaed by or is otherwise requested to disclose to others information contained in a SAR or the fact that a SAR was filed should decline to produce the SAR and should not provide any information or statements that would disclose that a SAR has been prepared or filed [e.g. 31 CFR 103.18(e) with respect to banks and 31 CFR 103.16(f) with respect to insurers]. This

prohibition does not preclude disclosure of business records that are the basis of the SAR, as long as the disclosure does not state or imply that a SAR has been filed on the underlying information. In addition, the prohibition does not apply to requests by FinCEN or an appropriate law enforcement or federal functional regulator and appropriate supervisory self-regulatory organization.

653. The statute and the implementing regulations state clearly that the prohibition on disclosure applies only with respect to any person involved in the transaction. However, FinCEN holds that it interprets the requirement much more tightly than the statutory language. This has been asserted most recently in the "Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies", issued on 20 January 2006, which states that "Implementing regulations issued by (FinCEN) have construed this confidentiality provision as generally prohibiting a banking organization from disclosing the existence of a (SAR) except where such disclosure is requested by appropriate law enforcement agencies, bank supervisory agencies, or (FinCEN)". However, the text of the regulations continues to mirror the language of the statute.

654. Under regulations issued under Title 12, SARs filed by the banks are deemed to be confidential. For example, 12 CFR 208.62(j) states that "SARs are confidential. Any member bank subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed". Courts that have reviewed this issue have opined that the statute and the regulation create an unqualified privilege that cannot be waived by the financial institution or the government. Examples include Wuliger v. OCC, 394 F. Supp. 2d 1009 (N.D. Ohio 2005); Gregory v. Bank One Corp. 200 F. Supp. 2d 1000 (S.D. Ind. 2002); Lee v. Bankers Trust Co., 166 F.3d 540, 543 (2d Cir. 1999) ("Disclosure of even the filing of a SAR, let alone its substance, is prohibited by law."); Whitney Nat'l Bank v. Karam, 306 F. Supp.2d 678 (S.D. Tex. 2004) (holding not only a SAR itself to be protected from disclosure, but also communications pertaining to a SAR or its contents)]. However, it has to be noted that some of these cases hinged on whether the scope of the Title 12 restrictions on SAR disclosure was reasonable, not on whether the BSA restrictions prohibited disclosure to third parties. It is unclear whether this interpretation would apply in cases where there are no relevant supplementary regulations issued by federal regulators.

Recommendation 25 (Feedback and guidance related to SARs)

655. Financial institutions indicated that they do not receive specific feedback from FinCEN on their filed SARs. However, FinCEN does provide general information in their SAR Bulletins on specific issues, the quarterly reports and/or on the website.

656. FinCEN provides feedback to the industry in the form of two separate publications: the "SAR Activity Review—Trends, Tips and Issues", and a companion piece entitled "SARs by the Numbers". "The SAR Activity Review-Trends, Tips & Issues" has been published twice annually since October 2000, but since late 2005, has been published three times per year. The publication is a product of continuing dialogue and close collaboration among financial institutions, law enforcement officials, and regulatory agencies, which provides information about the preparation, use and value of SARs filed by all industries subject to reporting under the BSA regulations. The publication also provides numerous examples of SAR filings that resulted in significant prosecutions.

657. The publication is divided into six sections covering trends and analyses of money laundering and terrorist financing methodologies identified in SAR narratives; summaries of law enforcement cases where SAR filings were helpful; tips on the preparation and filing of SARs; issues and guidance for financial institutions on procedural matters, topics warranting attention and recent court decisions; an industry forum open to financial institutions to outline issues of concern to their community; and a mailbag and feedback section which addresses issues raised by the financial institution industry, such as filing of SARs and identification of suspicious activity categories.

658. The companion publication, "The SAR Activity Review-By The Numbers", is also published on FinCEN's website. This provides statistics outlining the number of filings for each of the SARs required to be filed by depository institutions, money services businesses, casinos and card clubs, and securities and futures industries. The statistics accumulated in the publication include number of filings by U. S. states and territories, by violation reported, and by year and month of filing.

659. FinCEN has also published industry-specific guidance such as information for the money services business sector, for which there is a dedicated website that includes information concerning how MSBs are to comply with the reporting obligation.

660. FinCEN co-ordinates with law enforcement agencies (such as ICE) that are also publishing guidance to industry (For a more detailed discussion of the guidance that ICE gives to industry, see section 3.9 below).

Recommendation 19 (Other types of reporting)

661. The U.S. has implemented a system where financial institutions report certain transactions in currency above a fixed threshold to FinCEN. The various types of large cash transaction reports that must be file with FinCEN are described below.

Currency Transaction Report (CTR)

662. A financial institution (except for insurance companies which must file Form 8300s as described below) must file a CTR (FinCEN Form 104) with FinCEN for all non-exempt transactions (i.e. deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the financial institution) in currency over USD 10,000 involving the physical transfer of currency or other payment or transfer by, through, or to such financial institution.

663. Currency is defined to include notes and coins that are legal tender in the U.S. or any other country, and a transaction is deemed to include multiple transactions where the institution has knowledge that they were carried out by, or on behalf of, any one person.

664. Prior to completing a reportable transaction, the institution is required (31 CFR 103.28) to verify and record the name, street address (a post office box number is not acceptable), SSN or TIN (for non-U.S. resident) and date of birth of the individual presenting the transaction, as well as any person on whose behalf the transaction is being undertaken. The CTR also contains information about the amount and kind of transaction (transactions involving foreign currency should identify the country of origin and report the U.S. dollar equivalent of the foreign currency on the day of the transaction).

665. If the individual indicates that he or she is an alien or not a resident of the U.S., the financial institution must verify identity through examination of a passport, alien identification card, or other official document evidencing nationality or residence. For other individuals, the financial institution must verify identity through examination of a document that is normally acceptable within the banking community as a means of identification when cashing checks for non-depositors (e.g. a driver's license). The financial institution must also record the identity, account number and taxpayer identification number, if any, of any person on whose behalf the transaction is conducted. This information is transmitted to FinCEN with the CTR.

666. Financial institutions are permitted to exempt certain customers from the reporting process. These exemptions include banks, U.S. governmental departments and agencies, companies quoted on the major U.S stock exchanges (and their subsidiaries), and any U.S.-incorporated commercial enterprise (with respect only to its domestic business) that has maintained an account with the institution for at least 12 months and regularly engages in cash transactions in excess of USD 10,000. The exemption for commercial enterprises does not extend to a range of specified business activities [31 CFR 103.22(d)].

667. Upon receipt, CTRs are maintained in a BSA reporting database (Currency Banking Retrieval System), which is made available to various federal financial institution regulators and law enforcement. A completed CTR must be filed with FinCEN within 15 days after the date of the transaction (25 days if filed magnetically or electronically). The bank must retain copies of CTRs for five years from the date of the report [31 CFR 103.27(a)(3)].

668. The following chart shows the number of CTRs filed from 2001 to 2004.

Currency Transaction Reports Filed 2001-2004	
2001	12,711,154
2002	12,576,736
2003	13,299,135
2004	13,355,837
Total	51,942,862

Form 8300 - Reports of Cash Payments Over USD 10,000 Received in a Trade or Business

669. FinCEN/IRS Form 8300 is mandated under both the Internal Revenue Code (26 USC 60501) and the BSA (31 USC 5331), and requires any person engaged in a trade or business (as defined in the form and implementing regulations, and other than financial institutions required to file CTRs) to report to the IRS/FinCEN the receipt of currency in amounts over USD 10,000. This obligation applies to any trade, business or profession, (including insurance companies, jewelry stores, precious metals dealers, real estate sales, attorneys, accountants, automobile dealerships, boat sales, etc.) that receives more than USD 10,000 in cash or certain monetary instruments in a single transaction or in two or more related transactions. Any transactions conducted between a payer, or its agent and the recipient in a 24-hour period are related transactions. Transactions are considered related even if they occur over a period of more than 24 hours if the recipient knows, or has reason to know, that each transaction is one in a series of connected transactions. A transaction is defined as occurring when:

(a) goods, services, or property are sold;

(b) property is rented;

(c) cash is exchanged for other cash;

(d) a contribution is made to a trust or escrow account;

(e) a loan is made or repaid; and

(f) cash is converted to a negotiable instrument, such as a check or a bond.

670. Persons who are required to report a transaction under section 5331 must make that report by filing a joint FinCEN/IRS form (Form 8300) with the IRS (31 CFR 103.2231, CFR 103.30 and 26 USC 6050I).[72] This reporting obligation is similar to, but separate from the CTR obligations imposed on financial institutions under the BSA.

671. In order to file a Form 8300 properly, the person conducting the transaction, as well as the beneficial owner, must be identified and their identities must be verified "by examination of a document normally acceptable as a means of identification when cashing or accepting checks (for example a driver's license or credit card)" [31 CFR 103.30(e)(2)]. Verification of the identity of any person who purports to be an alien must be made by examination of such person's passport, alien identification card, or other official document evidencing nationality or residence. Trades and businesses are required to provide all requested information on the Form 8300, including the following for the person conducting the transaction: name, street address (a post office box number is not

[72] FinCEN's interim rule (66 FR 67680) that took effect from 1 January 2002.

acceptable), SSN or TIN (for non-U.S. residents), date of birth and the document used to verify the identifying information. Additionally, the trade/business must verify and record the identity, account number, and the social security number or tax payer identification number (if any) of any person or entity on whose behalf such transaction is to be effected (31 CFR Part 103.28).

672. Cash is defined as currency and coin of the U.S. or any other country as long as it is customarily accepted as money in the country of issue, and a cashier's check, bank draft, traveler's check, or money order (31 CFR 103.22). Multiple cash transactions under USD 10,000 shall be treated as a single transaction if the transactions are related. For example, related transactions would include:

(a) any transactions between a buyer (or an agent of the buyer) and a seller that occur within a 24-hour period are related transactions;

(b) transactions are related even if they are more than 24 hours apart if the trade or business knows, or has reason to know, that each is one of a series of connected transactions;

(c) installment payments that cause the total cash received within one year of the initial payment to total more than USD 10,000; or

(d) other previously unreported payments that cause the total cash received within a 12-month period to total more than USD 10,000.

673. Trades and businesses are also encouraged to voluntarily file a Form 8300 if they receive USD 10,000 or less in cash, and the transaction appears to be suspicious, for example, if it appears that a person is trying to cause the trade or business not to file Form 8300 or is trying to cause the filing of a false or incomplete Form 8300, or if there is a sign of possible illegal activity. In addition to filing the Form 8300 under these circumstances, the trade or business is also encouraged to contact the local IRS Criminal Investigation Division as soon as possible or call a toll-free telephone number to report the transaction. Every trade or business must ensure that it has appropriate procedures in place to report such transactions. IRS Publication 1544, Reporting Cash Payments of Over USD 10,000 (Received in a Trade or Business), is published to aid trade and businesses in implementing these procedures. This publication outlines the circumstances in which a Form 8300 needs to be filed, what information needs to be included on the form, and the penalties associated with failure to file the form or filing a false form.

674. Upon receipt, Forms 8300 are maintained in a BSA reporting database (Currency Banking Retrieval System), which is made available to various Federal Banking Agencies, other regulatory agencies, and law enforcement. A completed Form 8300 must be filed with FinCEN within 15 days after the date of the transaction. The trade or business must retain copies of Forms 8300 for five years from the date of the report.

675. Although filing a Form 8300 is a requirement under the BSA, the trade or business required to file may or may not be subject to the BSA's AML regime. Businesses subject to this reporting requirement are liable to compliance inspection by the IRS, but not on a routine basis. Civil penalties associated with Form 8300 are available for failure to: (1) file a correct Form 8300 by the date it is due; and (2) provide the required statement to those named in the Form 8300. If a trade or business intentionally disregards the requirement to file a correct Form 8300 by the date it is due, the penalty is the larger of: (1) USD 25,000; or (2) the amount of cash the trade or business received and was required to report (up to USD 100,000).

676. Criminal penalties associated with Form 8300 are available for:

(a) willful failure to file Form 8300;

(b) willfully filing a false or fraudulent Form 8300;

(c) stopping or trying to stop Form 8300 from being filed; and

(d) setting up, helping to set up, or trying to set up a transaction in a way that would make it seem unnecessary to file Form 8300.

677. If a trade or business willfully fails to file Form 8300, it can be fined up to USD 250,000 (USD 500,000 for corporations) or sentenced to up to five years in prison, or both (26 USC 7203; 18 USC 3571). The penalties for failure to file may also apply to any person (including a payer) who attempts to interfere with or prevent the seller (or business) from filing a correct Form 8300. This includes any attempt to structure the transaction in a way that would make it seem unnecessary to file Form 8300.

678. The following chart shows the filings of Form 8300 from 2001 to 2004.

Forms 8300 Filed 2001-2004	
2001	Not Available
2002	120,920
2003	130,795
2004	152,674
Total	404,389

Compliance with the large cash transaction reporting requirements

679. The following chart shows the number of prosecutions for violations of the reporting requirements relating to domestic currency transactions (31 USC 5313) for fiscal year 2004.

Prosecutions for violations of the domestic currency transaction reporting requirements
(31 USC 5313)

Number of...	Fiscal year 2004
Cases	14
Defendants	28
Successful charges	21
Terminated defendant count	28
Guilty	9

3.7.2 Recommendations and Comments

680. There is one key issue that arises with respect to the general SAR requirements. There exists a general USD 5,000 threshold for mandatory reporting, (USD 2,000 for MSBs) although institutions may report voluntarily below this threshold. This conflicts with the FATF standard that requires the reporting of all suspicious transactions, regardless of the amount. An appropriate amendment to the legislation is recommended to bring the U.S. into compliance.

681. Another issue of importance is the failure to extend the SAR obligations to several financial institutions—namely investment advisers and commodity trading advisers.

682. The exclusion of insurance agents and insurance brokers from being directly responsible in filing SARs is unlike the AML regulatory scheme for MSBs and their "agents" which have independent BSA compliance responsibilities. However, as noted in FinCEN's final rule on reporting SAR (70 FR 66765) that "suspicious activity that occurs at the time of sale of the covered product is most likely to be observed by the agent and broker, while suspicious activity that occurs following the issuance of a policy and during the ongoing administration of the product would most likely to be observed by the insurance company." As these insurance intermediaries are in the best position to detect suspicious activity when they sell the covered insurance policies to their customers in a face-to-

face situation, the authorities should consider imposing direct AML obligations on them in compliance with the FATF's Recommendations.

683. Additionally, there are some uncertainties about the scope of the confidentiality provisions relating to SARs. Although the courts have upheld the general confidentiality of SARs under the regulations issued by the Federal Banking Agencies, it remains unclear as to whether the more limited disclosure restrictions under the BSA (i.e. to any person involved in the transaction) would apply in the absence of such supplementary regulations. While the practice has been to regard disclosure to third parties as being prohibited (supported by the courts, so far), the U.S. authorities are encouraged to take action to put this beyond all doubt.

3.7.3 Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13	LC	• The existence of a USD 5,000 threshold for reporting suspicious activity. • No measures have been applied to investment and commodity trading advisers. • The effectiveness of measures in the insurance and mutual funds sectors cannot yet be assessed.
R.14	C	• The Recommendation is fully observed.
R.19	C	• The Recommendation is fully observed.
R.25	C	• The Recommendation is fully observed.
SR.IV	LC	• The existence of a USD 5,000 threshold for reporting suspicious activity. • No measures have been applied to investment and commodity trading advisers. • The effectiveness of measures in the insurance and mutual funds sectors cannot yet be assessed.

Internal controls and other measures

3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)

3.8.1 Description and Analysis

Recommendation 15 (Internal controls) and Recommendation 22 (Foreign operations)

Banking sector

684. Section 352 of the USA PATRIOT Act requires financial institutions to establish AML Programs, including, at a minimum: (1) the development of internal policies, procedures and controls; (2) the designation of a compliance officer; (3) an ongoing employee training program; and (4) an independent compliance function to test programs. In 2002 FinCEN issued an interim final rule stating that a financial institution that is subject to regulation by a federal functional regulator will be deemed to be in compliance with the requirements of section 5318(h)(1) of the BSA if it complies with the regulations of its regulator governing the establishment and maintenance of AML Programs [31 CFR 103.120(b)]. In view of the scope of the BSA, the policies, procedures and controls must, at a minimum, address CDD, record-keeping, the detection of large, unusual and suspicious transactions, and the reporting to FinCEN of certain defined transactions. In all cases, section 352 of the USA PATRIOT Act requires that regulations introduced to implement this provision should be commensurate with the size, location and activities of the institutions to which they apply (i.e. they should be risk-based). When introducing the rule in April 2002, FinCEN deferred subjecting certain non-federally regulated banks to the AML Program requirements. FinCEN intends to amend its regulations to eliminate the regulatory anomaly to bring uniformity to the banking sector.

685. Since 1987, each of the Federal Banking Agencies has adopted regulations requiring AML Programs for the financial institutions under their respective jurisdictions. These regulations currently require that "each bank shall develop and provide for the continued administration of a program reasonably designed to ensure and monitor compliance with the record-keeping and reporting requirements [of the BSA] and the implementing regulations promulgated thereunder. The compliance program shall be reduced to writing, approved by the board of directors and noted in the minutes" (e.g. 12 CFR 208.63 for entities supervised by the Federal Reserve). The regulators' expectations in terms of compliance with the AML Program requirements are covered extensively in the FFIEC Manual.

686. Section 352 of the USA PATRIOT Act specifically requires financial institutions to appoint an AML compliance officer. For the banking sector, the FFIEC Manual (pp.27-28) defines the regulators' expectations as follows:

> "The bank's board of directors must designate a qualified employee to serve as the BSA compliance officer. The BSA compliance officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA compliance officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the bank's adherence to the BSA and its implementing regulations; however, the board of directors is ultimately responsible for the bank's BSA/AML compliance.
>
> While the title of the individual responsible for overall BSA/AML compliance is not important, his or her level of authority and responsibility within the bank is critical. The BSA compliance officer may delegate BSA/AML duties to other employees, but the officer should be responsible for overall BSA/AML compliance. The board of directors is responsible for ensuring that the BSA compliance officer has sufficient authority and resources (monetary, physical, and personnel) to administer an effective BSA/AML compliance program based on the bank's risk profile.
>
> The BSA compliance officer should be fully knowledgeable of the BSA and all related regulations. The BSA compliance officer should also understand the bank's products, services, customers, and geographic locations, and the potential money laundering and terrorist financing risks associated with those activities. The appointment of a BSA compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, or time to satisfactorily complete the job.
>
> The line of communication should allow the BSA compliance officer to regularly apprise the board of directors and senior management of ongoing compliance with the BSA. Pertinent BSA-related information, including the reporting of SARs filed with FinCEN, should be reported to the board of directors or an appropriate board committee so that these individuals can make informed decisions about overall BSA/AML compliance. The BSA compliance officer is responsible for carrying out the direction of the board and ensuring that employees adhere to the bank's BSA/AML policies, procedures, and processes."

687. As part of the core examination procedures outlined in the FFIEC Manual (p.177), examiners are required to determine if the individual designated as the bank's compliance officer has the necessary authority and resources to effectively execute all the duties of the position.

688. With regard to the requirement of section 352 to provide for independent testing for compliance, the FFIEC Manual (pp.26-27) states that, for banks, this should, at a minimum, include the following:

(a) an evaluation of the overall integrity and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes;

(b) a review of the bank's risk assessment for reasonableness given the bank's risk profile (products, services, customers, and geographic locations);

(c) appropriate transaction testing to verify the bank's adherence to the BSA recordkeeping and reporting requirements (e.g. CIP, SARs, CTRs, CTR exemptions and information sharing requests);

(d) an evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable;

(e) a review of staff training for adequacy, accuracy, and completeness;

(f) a review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for BSA/AML compliance; and

(g) an assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the bank's policy.

689. The FFIEC Manual further requires that "any violations, policy or procedures exceptions, or other deficiencies noted during the audit should be included in an audit report and reported to the board of directors or a designated committee in a timely manner. The board or designated committee and the audit staff should track audit deficiencies and document corrective actions".

690. With regard to the BSA compliance program requirement to provide for employee training, the FFIEC Manual (pp.28-29) states that:

> "Banks must ensure that appropriate personnel are trained in applicable aspects of the BSA. Training should include regulatory requirements and the bank's internal BSA/AML policies, procedures, and processes. At a minimum, the bank's training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the person's specific responsibilities. In addition, an overview of the BSA/AML requirements should be given to new staff. Training should encompass information related to applicable operational lines, such as trust services, international, and private banking.
>
> The board of directors and senior management should be informed of changes and new developments in the BSA, its implementing regulations and directives, and the federal banking agencies' regulations. While the board of directors may not require the same degree of training as banking operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the bank. Without a general understanding of the BSA, the board of directors cannot adequately provide BSA/AML oversight; approve BSA/AML policies, procedures, and processes; or provide sufficient BSA/AML resources.
>
> Training should be ongoing and incorporate current developments and changes to the BSA and any related regulations. Changes to internal policies, procedures, processes, and monitoring systems should also be covered during training. The program should reinforce the importance that the board and senior management place on the bank's compliance with the BSA and ensure that all employees understand their role in maintaining an effective BSA/AML compliance program.
>
> Examples of money laundering activity and suspicious activity monitoring and reporting can and should be tailored to each individual audience. For example, training for tellers should focus on examples involving large currency transactions or other suspicious activities; training for the loan department should provide examples involving money laundering through lending arrangements.
>
> Banks should document their training programs. Training and testing materials, the dates of training sessions, and attendance records should be maintained by the bank and be available for examiner review".

691. As a matter of law, specific BSA requirements are not applicable to foreign branches and offices of domestic banks. An initial proposal by FinCEN to extend certain provisions to the foreign branches was dropped after the consultation stage, one consequence being that the foreign branches of U.S.

banks must be treated as non-U.S. persons as far as the U.S. institutions are concerned. However, as a matter of safety and soundness, domestic banks are expected by the regulators to have BSA/AML compliance programs that apply to all departments of the banks, including its foreign branches and operations, to protect against the risks of money laundering and terrorist financing. The FFIEC Manual (pp.93-94) states that:

> "a sound practice for complex organizations is to establish effective programs through the holding company or lead financial institution that view BSA/AML risks across legal entities, and allow management to demonstrate to their boards of directors that they have effective compliance programs in place across the consolidated organization. The program should reflect the organization's structure and be tailored to its size, complexity, and legal requirements that may vary due to the specific business line or host jurisdiction. Enterprise-wide systems that operate on a global basis need to consider the various jurisdictions in which they operate as well as the AML laws and requirements they are subject to, and then incorporate these into their overall program. Internal audit should assess the level of compliance with the enterprise-wide BSA/AML compliance program."

692. The FFEIC Manual goes on further to state that "although specific BSA requirements are not applicable at foreign branches and offices, banks are expected to have policies, procedures, and processes in place at all their branches and offices to protect against risks of money laundering and terrorist financing. In this regard, foreign branches and offices should be guided by the U.S. bank's BSA/AML policies, procedures, and processes. The foreign branches and offices must comply with OFAC requirements and all local AML-related laws, rules, and regulations".

693. With respect to bank's operations in jurisdictions that may not apply the FATF Recommendations, the FFIEC Manual (p.108) states that:

> "Branches and offices of U.S. banks located in high-risk geographic locations may be vulnerable to abuse by money launderers. To address this concern, the U.S. bank's policies, procedures, and processes for the foreign operation should be consistent with the following recommendations:
>
> - The U.S. bank's head office and management at the foreign operation should understand the effectiveness and quality of bank supervision in the host country and understand the legal and regulatory requirements of the host country. The U.S. bank's head office should be aware of and understand any concerns that the host country supervisors' may have with respect to the foreign branch or office.
> - The U.S. bank's head office should understand the foreign branches' or offices' risk profile (e.g., products, services, customers, and geographic locations).
> - The U.S. bank's head office and management should have access to sufficient information in order to periodically monitor the activity of their foreign branches and offices, including the offices' and branches' level of compliance with head office policies, procedures and processes. Some of this may be achieved through management information systems reports.
> - The U.S. bank's head office should develop a system for testing and verifying the integrity and effectiveness of internal controls at the foreign branches or offices by conducting in-country audits. Senior management at the head office should obtain and review copies, written in English, of audit reports and any other reports related to AML and internal control evaluations.
> - The U.S. bank's head office should establish robust information sharing practices between branches and offices, particularly regarding high-risk account relationships.
> - The U.S. bank's head office should be able to provide examiners with any information deemed necessary to assess compliance with U.S. banking laws.

Foreign branches and offices are expected to be guided by the U.S. bank's BSA/AML policies, procedures, and processes. These systems and processes should be risk based and certain high-risk geographies should be a determinative risk factor is assessing overall and account/customer risk."

694. A bank that is unable to observe appropriate AML/CFT measures because of local law prohibitions is not required to inform its home country supervisor of this legal limitation or legal conflict in laws. However, the bank is expected to have an AML compliance program in place that adequately monitors the risks associated with the business. If local laws limit the effectiveness of the financial institution's compliance program, the financial institution would be expected to assess the impact of the local law on its compliance program and determine whether the program can function effectively under this limitation, taking into consideration the adequacy of the existing system to monitor the heightened risks or other the possibility of implementing other risk mitigating processes.

695. Section 327 of the USA PATRIOT Act amends section 3(c) of the Bank Holding Company Act and requires that the Federal Reserve take into consideration the effectiveness of an applicant company in combating money laundering activities, including in its overseas branches, when the Board or a Reserve Bank acts on an application filed under section 3 of the Bank Holding Company Act (i.e. the acquisition of bank shares or assets). Section 327 also requires the Federal Reserve and the other federal financial institutions supervisory agencies to consider the effectiveness of an insured depository institution in combating money laundering activities, including in its overseas branches, in connection with any application filed under the Bank Merger Act. The provisions of Section 327 apply to all applications filed under either of these two laws after 31 December 2001.

696. In terms of the banks' implementation of effective internal controls, it is apparent that considerable time and effort has been, and continues to be, devoted to this issue. It is generally regarded that BSA compliance is the most important issue on which institutions are focusing at present. This was certainly the impression from discussions with the banking sector, which has been alerted to the perils of non-compliance by the heavy fines exacted on several institutions in recent years. However, the regulators report that compliance issues continue to arise from the examinations, although most of the issues are resolved through informal enforcement action. Typical of the problems identified are (in no particular sequence):

(a) weaknesses in systems to identify high-risk customer, including PEPs and their associates;

(b) inadequate independent testing arrangements;

(c) weaknesses in the automated transactions monitoring systems, including inadequate parameters for exceptions reporting; and

(d) deficiencies in the SAR procedures;

697. At the systemic level, the credit union sector as a whole has been identified as having greater problems than other institutions in implementing effective systems. In addition, there has been some indication that the smaller community banks have failed to maintain their procedures at a level to match their search for growth in markets and services.

698. With respect to the application of the BSA principles to their foreign branches, the banks interviewed have reported that they aim to do this as a matter of policy. However, they indicated that the bank secrecy laws in certain jurisdictions hinder them from exercising a centralized, or consolidated approach to AML risk management because the institutions are not permitted to transfer customer information outside the jurisdiction. The regulators also report that their ability to examine compliance in the foreign branches is limited by similar factors, in that they are not permitted to examine individual customer files as part of their sampling procedures. Such restrictions are clearly a hindrance to the implementation by banks of effective global systems and controls.

699. With regard to employee screening there is no explicit obligation imposed upon either banks or other financial institutions, but they are strongly encouraged by the federal regulators to use reasonable employment screening processes to minimize the risk of fraud, embezzlement, money laundering, and other crimes. The authorities consider that a reasonable policy might include checking references, performing credit and/or background checks, Internet searches, and performing criminal background checks, including an FBI fingerprint check, for prospective employees. Financial institutions are also expected to check the websites of its federal regulator to determine if there has been a removal action, personal cease and desist order, or other formal action against the proposed employee. These measures would have particular relevance to those institutions regulated at the federal level, but their application would be limited in respect of institutions such as MSBs and insurance companies.

Securities sector

700. The legal provisions that are applicable to the securities sector in relation to internal controls are similar to those described above for the banking sector, with the following elaboration and/or differences.

701. In 2002 FinCEN permitted the securities and futures SROs to adopt their own rules requiring members to implement AML Programs to meet the requirements of the USA PATRIOT Act, subject to the rules being approved by the SEC. In addition, FinCEN has issued an interim final rule that requires mutual funds to establish AML Programs (31 CFR 103.130). The result is that following securities businesses are currently obligated to establish an AML Program:

(a) securities broker-dealers (31 CFR 103.120; NYSE Rule 445, and NASD Rule 3011);

(b) futures commission merchants and introducing brokers in commodities [31 CFR 103.120; NFA Rule 2-9(c)];

(c) mutual funds (31 CFR 103.130).

702. Rules have also been proposed that would extend the obligation to establish an AML Program to the following sectors:

(a) unregistered investment companies [67 FR 60617, (26 September 2002)];

(b) investment advisers [68 FR 23646 (5 May 2003)]; and

(c) commodity trading advisers [68 FR 23640 (5 May 2003)].

703. With respect to securities broker-dealers, futures commission merchants, and introducing brokers in commodities, SRO rules also require their members to designate an AML Compliance Officer reporting to senior management and establish, maintain, and enforce a system of supervisory control policies and procedures that, for example, test and verify that the member's supervisory procedures are reasonably designed to achieve compliance with applicable securities laws and regulations and applicable SRO rules (e.g. NASD Notice to Members 02-21, pages 13-14). Firms also may be required to create additional supervisory procedures or amend existing ones if such a need is identified by the testing and verification [e.g. NASD Rule 3012. Supervisory Control System, NFA Compliance Rule 2-9(c) and NFA Compliance Rule 2-9 Interpretive Note].

704. SEC staff examining securities broker-dealers and mutual funds and SRO staff examining securities broker-dealers ensure that AML compliance officers designated under relevant Treasury regulations also have sufficient authority and resources to effectively implement the firm's AML Programs under SRO rules.

705. SROs have also advised their members that AML employee training should be developed under the leadership of a firm's AML Compliance Officer or senior management, and should be implemented on at least an annual basis. SROs urge their members to instruct their employees about the following topics, at a minimum:

(a) how to identify "red flags" and possible signs of money laundering that could arise during the course of their duties;

(b) what to do once the risk is identified;

(c) what their roles are in the firm's compliance efforts;

(d) how to perform their roles;

(e) the firm's record retention policy; and

(f) disciplinary consequences, including civil and criminal penalties for non-compliance with the BSA.

706. Securities SROs have also advised that a securities broker-dealer should scrutinize its operations to determine if there are certain employees who need additional or specialized training due to their duties and responsibilities, including appropriate instruction to ensure compliance with the BSA.

707. Effective August 2004, the SEC amended its rules (17 CFR 240.17i-4) to require supervised investment bank holding companies and consolidated supervised entities (which include the largest securities broker-dealers, and which often have foreign subsidiaries), as part of their group-wide internal risk management control systems, to establish, document, and maintain procedures for the detection and prevention of money laundering and terrorist financing. With respect to smaller broker-dealers that are not part of a consolidated supervised entity or supervised investment bank holding company no precise requirement asks for specific implementation by securities broker-dealers to foreign subsidiaries of their home country requirements. A securities broker-dealer that is unable to observe appropriate AML/CFT measures because of local law prohibitions is not required to inform its home country supervisor of this legal limitation or legal conflict in laws.

708. Prospective employees of broker-dealers are subject to extensive screening procedures to ensure high standards. Broker-dealers must have their employees fingerprinted and submit the fingerprints to the Attorney General of the United States for identification and appropriate processing. (17 CFR 240.17f-2). Furthermore, broker-dealers are required by SRO rules to screen prospective employees. For example, NYSE Rule 345.11 (Investigation and Records) requires firms to investigate the records of individuals they contemplate hiring and NYSE Rule 346(f) requires approval when hiring someone subject to statutory disqualification. In addition, under NASD Rule 3010(e) broker-dealers that do business with the public are required to investigate the qualifications of individuals that they are proposing to hire. Firms are required to "ascertain by investigation the good character, business repute, qualifications, and experience of any person" prior to "making a certification in the application of such person for registration" with NASD.

709. Futures commission merchants are required to obtain such information, keep such records, and implement such procedures, policies and controls that are necessary for it to monitor and control the financial and operational risks to it resulting from the activities of any of its affiliates [7 USC 2(c)(2)(B)(ii)(III) and 6f(c); see also 17 CFR 1.14 and 1.15] Consequently, futures commission merchants that are part of a holding company system, should, as part of their group-wide internal risk management control system, establish, document and implement procedures for the detection and prevention of money laundering and terrorism financing.

Insurance sector

710. When the BSA was enacted in 1970, the law provided for statutory authority for record-keeping and reporting for "financial institutions", a term that was defined to include an insurer [31 USC 5312(a)(2)(M)]. Section 352 of the USA PATRIOT Act, which became effective on 24 April 2002, amended 31 USC 5318(h) to require AML Programs for all financial institutions defined in 31 USC 5312(a)(2)—including insurers.

711. In anticipation of the new responsibilities for the insurance sector under the Act, several state insurance regulators (e.g. Connecticut, Delaware, Illinois, Kansas, Kentucky, Maine, Mississippi, Nebraska, Nevada, North Dakota, Utah, Virginia, West Virginia and Wyoming) issued circular letters to advise persons or entities regulated by their respective Insurance Departments of the enactment of the USA PATRIOT Act and noted that insurers were required to be in compliance with the Act by 24 April 2002. Among others, the circular letters advised of the new responsibilities under that Act, i.e. (1) insurers are included in the BSA's definition of financial institution; (2) section 352 of the Act amends the BSA to require that all financial institutions establish an AML Program; and (3) section 326 amends the BSA to require the Secretary of the Treasury to adopt minimum standards for financial institutions regarding the identity of customers that open accounts.

712. In April 2002, FinCEN deferred the AML Program requirement contained in 31 USC 5318(h) that would have applied to the insurance industry.[73] As a result, the state insurance regulators had to issue Supplements to their Circular Letters to update insurers that the Treasury had exercised its authority under section 5318(a)(6) of the BSA to exempt insurers and certain other specified financial institutions, for a period of no more than six months, from the requirement in 31 USC 5318(h)(1) that they establish AML Programs. The deferral was to allow the Treasury time to study the insurance industry and to consider how AML controls could best be applied to that industry, considering the size, location, and services within the industry. The final rules under the BSA requiring insurers to establish AML Programs, as well as to file SARs were issued in 2005.

713. Under these rules, which become effective on 2 May 2006, an insurer that issues or underwrites covered insurance products as a business has to establish an AML Program applicable to its covered life insurance products that is reasonably designed to prevent it from being used to facilitate money laundering or the financing of terrorist activities (70 FR 66754). An insurance company's AML Program must include: (1) policies, procedures, and internal controls based upon its assessment of the money laundering and terrorist financing risks associated with its covered products; (2) designation of a compliance officer who will be responsible for the effective implementation of the program; (3) provide ongoing training for appropriate persons concerning their responsibilities under the program; and (4) provide for independent testing to monitor and maintain an adequate program [31 USC 5318(h)(1)]. These requirements mirror the existing obligation imposed on the banking and securities sector, the details of which have been discussed above.

714. Unlike a life insurance company, an insurance agent or broker is not required to establish an AML Program. Instead, each insurance company is required to integrate its insurance agents and insurance brokers into its AML Program and to monitor their compliance with its program.

715. Also after 2 May 2006, an insurance company is required to provide training for appropriate persons as an integral part of its AML Program. In order for its AML Program to be effective, its employees with responsibilities under the program as well as its insurance agents and insurance brokers must be trained in the requirements of the program and money laundering risks generally so that "red flags" associated with covered products can be identified. Such training could be conducted by outside or in-house seminars, and computer-based training. The nature, scope, and frequency of the training will depend on the functions performed and should include periodic updates and refreshers regarding the AML Program. Instead of training its insurance agents and insurance brokers directly, an insurance company may satisfy the requirement in 31 CFR 103.137(c)(3) by verifying that its agents and brokers have received the required training by another insurance company or by a competent third party with respect to its covered products.

716. BSA requirements do not apply to the foreign branches and offices of domestic life insurers issuing and underwriting covered life insurance products.

[73] 31 CFR 103.170, as codified by IFR published at 67 FR 21110 (29 April 2002) amended at 67 FR 67547 (6 November 2002) and corrected at 67 FR 68935(14 November 2002).

Money Services Business sector (including money remitters and foreign exchange)

717. MSBs are required to develop an anti-money laundering program (31 CFR 103.125). The principles underlying this requirement are the same as for other financial institutions, specifically the AML Program must include: (1) written internal policies and procedures (relating to verifying customer identification, filing reports, creating and retaining records, and responding to law enforcement requests); (2) designation of a compliance officer (to make sure policies and procedures are followed and updated); (3) ongoing employee training (to explain policies and procedures and identify suspicious activities); and (4) independent review of the program (to test the anti-money laundering program and ensure its effectiveness).

718. The U.S. authorities advise that MSBs that are authorized to operate in the U.S. do not have foreign branches or subsidiaries. However, MSBs that utilize foreign agents or counterparties, must have AML Programs that include risk-based policies, procedures, and controls designed to identify and minimize money laundering and terrorist financing risks associated with foreign agents and counterparties that facilitate the flow of funds into and out of the U.S. FinCEN issued interpretive guidance with respect to its expectations in this area on 14 December 2004 (69 FR 74439). Relevant risk factors are specified to include:

(a) the foreign agent or counterparty's location and jurisdiction of organization, chartering, or licensing. This would include considering the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or is considered to have more robust anti-money laundering standards;

(b) the ownership of the foreign agent or counterparty. This includes whether the owners are known, upon reasonable inquiry, to be associated with criminal conduct or terrorism. For example, have the individuals been designated by Treasury's Office of Foreign Assets Control as Specially Designated Nationals or Blocked Persons (i.e. involvement in terrorism, drug trafficking, or the proliferation of weapons of mass destruction);

(c) the extent to which the foreign agent or counterparty is subject to anti-money laundering requirements in its jurisdiction and whether it has established such controls;

(d) any information known or readily available to the MSB about the foreign agent or counterparty's AML, including public information in industry guides, periodicals, and major publications;

(e) the nature of the foreign agent or counterparty's business, the markets it serves, and the extent to which its business and the markets it serves present an increased risk for money laundering or terrorist financing;

(f) the types and purpose of services to be provided to, and anticipated activity with, the foreign agent or counterparty; and

(g) the nature and duration of the MSB's relationship with the foreign agent or counterparty.

719. According to the interpretive guidance, a MSB's AML Program should include procedures for conducting reasonable, risk-based due diligence on potential and existing foreign agents and counterparties to help ensure that such foreign agents and counterparties are not themselves complicit in illegal activity involving the money services business' products and services, and that they have in place appropriate anti-money laundering controls to guard against the abuse of the money services business' products and services. Such due diligence must, at a minimum, include reasonable procedures to identify the owners of the money services business' foreign agents and counterparties, as well as to evaluate, on an ongoing basis, the operations of those foreign agents and counterparties and their implementation of policies, procedures, and controls reasonably designed to help assure that the MSBs' products and services are not subject to abuse by the foreign agent's or counterparty's customers, employees, or contractors. The extent of the due diligence required will depend on a variety of factors

specific to each agent or counterparty. FinCEN expects MSBs to perform due diligence in a manner consistent with the assessed risk.

720. In addition to the due diligence described above, in order to detect and report suspected money laundering or terrorist financing, MSBs should establish procedures for risk-based monitoring and review of transactions from, to, or through the U.S. that are conducted through foreign agents and counterparties. Such procedures should also focus on identifying material changes in the agent's risk profile, such as a change in ownership, business, or the regulatory scrutiny to which it is subject. The review of transactions should enable the MSB to identify and, where appropriate, report as suspicious such occurrences as: instances of unusual wire activity, bulk sales or purchases of sequentially numbered instruments, multiple purchases or sales that appear to be structured, and illegible or missing customer information. Additionally, MSBs should establish procedures to assure that their foreign agents or counterparties are effectively implementing an anti-money laundering program and to discern obvious breakdowns in the implementation of the program by the foreign agent or counterparty.

721. Similarly, money transmitters should have procedures in place to enable them to review foreign agent or counterparty activity for signs of structuring or unnecessarily complex transmissions through multiple jurisdictions that may be indicative of layering. Such procedures should also enable them to discern attempts to evade identification or other requirements, whether imposed by applicable law or by the MSBs' own internal policies. Activity by agents or counterparties that appears aimed at evading the MSB's own controls can be indicative of complicity in illicit conduct; this activity must be scrutinized, reported as appropriate, and corrective action taken as warranted.

722. MSBs should also have procedures for responding to foreign agents or counterparties that present unreasonable risks of money laundering or the financing of terrorism. Such procedures should provide for the implementation of corrective action on the part of the foreign agent or counterparty or for the termination of the relationship with any foreign agent or counterparty that the MSB determines poses an unacceptable risk of money laundering or terrorist financing, or that has demonstrated systemic, willful, or repeated lapses in compliance with the MSB's own anti-money laundering procedures or requirements.

723. There is no explicit obligation in federal law or regulation with regard to employee screening by MSBs to ensure high standards when hiring employees; however, the authorities have advised that some states do include such obligations in their licensing standards and requirements.

Credit Card Operators

724. Under 31 CFR 103.135, the operators of credit card systems are required to maintain AML Programs. In addition to the standard AML Program requirements described above, these programs are required to ensure that:

(a) the operator does not authorize any person to serve as an issuing or acquiring institution without the operator taking appropriate steps to guard against that person issuing the operator's credit card in circumstances that facilitate money laundering; and

(b) the operator applies risk-based procedures which, at a minimum, recognize that the following entities pose a heightened risk of money laundering: (1) shell banks; (2) a person appearing on the OFAC lists; (3) a person located in a jurisdiction designated by the Department of State as a sponsor of international terrorism; (4) a foreign bank operating under an off-shore license (except when it is subject to comprehensive supervision); (5) a person located in a jurisdiction designated as non-cooperative in the fight against money laundering; and (6) a person located in a jurisdiction designated pursuant to 31 USC 5318A.

3.8.2 Recommendations and Comments

725. The requirements imposed on the banking sector to maintain proper AML systems and controls are extensive, and the legal requirements are supported by the specific regulatory expectations addressed in the comprehensive FFIEC Manual. A limited number of non-federally regulated depository institutions remain exempted from the AML Program requirement. However, this exemption which exists for historical reasons, does not give rise to substantive AML concerns, but FinCEN intends to amend its regulations to eliminate this regulatory anomaly to bring uniformity to the banking sector.

726. The requirements imposed on the securities sector to maintain proper AML systems and controls also are extensive. However, while FinCEN has proposed rules that extend the obligations to maintain AML Programs to unregistered investment companies, investment advisers and commodity trading advisers, they have yet to be finalized. The U.S. is strongly encouraged to complete this process.

727. FinCEN's regulations require insurance companies that offer covered products to implement internal controls as part of the AML program by 2 May 2006, the effective date of the regulation. It is not possible yet to assess the effectiveness of these measures in the insurance sector. The regulations do not apply to operations outside the U.S.

728. Financial institutions in the securities sector are required to screen prospective employees for high standards. Other financial institutions should be required to ensure high standards when hiring employees.

3.8.3 Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	LC	• AML Program requirements have not been applied to certain non-federally regulated banks, investment and commodity trading advisers. • It is not yet possible to assess the effectiveness of these measures in the insurance sector • There is no obligation under the BSA for financial institutions to implement employee screening procedures.
R.22	LC	• BSA requirements do not apply to the foreign branches and offices of domestic life insurers issuing and underwriting covered life insurance products.

3.9 Shell banks (R.18)

3.9.1 Description and Analysis

729. The establishment of shell banks is not permitted in the U.S, either at federal or state level. In addition, from the sample of states visited that engage in large-scale formation of companies for non-residents (Delaware and Nevada), legal or administrative arrangements are in place to prevent the registration of companies bearing banking names. There is no evidence to suggest that these arrangements are not working effectively.

730. The BSA was amended by section 313 of the USA PATRIOT Act (and implemented by 31 CFR 103.177) to prohibit U.S. financial institutions from establishing, maintaining, administering or managing a correspondent account in the U.S. for any foreign shell bank (other than a regulated affiliate of a U.S. or foreign bank). This section became effective in December 2001, and FinCEN issued final implementing regulations in September 2002.

731. A foreign shell bank is defined as a foreign bank without a physical presence in any country. For a bank to have a physical presence, the regulation requires that it must maintain a place of business at a fixed address (other than solely a post office box or electronic address) in a country in

which it is authorized to conduct banking activities. At this location, the bank must employ one or more full-time individuals, maintain operating records, and be subject to inspection by a regulatory authority that licensed the bank's activities.

732. Section 313(a)(ii) of the USA PATRIOT Act (and its implementing regulations) requires financial institutions to take reasonable steps to ensure that correspondent accounts provided to foreign banks are not being used to provide banking services indirectly to foreign shell banks (i.e. that the foreign correspondent bank of the U.S. financial institution does not in turn give a foreign shell bank the ability to access the U.S. correspondent account through its account – in other words, indirect access through a nested account). A financial institution is required to terminate immediately any account that it knows to be the account of a foreign shell bank or that it knows is being used indirectly by a foreign shell bank.

733. The final regulation issued under Section 313 provides a safe harbor for compliance with the requirement prohibiting dealings with shell banks (31 CFR 103.177). Pursuant to the safe harbor, a financial institution is required to obtain a certification from its foreign bank customers, and to obtain re-certification at least every three years, to the effect that the customer is neither a foreign shell bank nor provides financial services to foreign shell banks through a correspondent account maintained at the covered financial institution. If a financial institution fails to obtain all the information required by the initial certification within the necessary time period, it must close that account. The institution must also verify such information whenever it might have reason to believe that the information is no longer correct.

3.9.2 Recommendations and Comments

734. The U.S. is fully compliant with the standards to combat the abuse of shell banks.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	C	• The Recommendation is fully observed.

Regulation, supervision, guidance, monitoring and sanctions (R17, 23, 25 & 29)

3.10 Supervision and oversight

3.10.1 Description and Analysis

Role of FinCEN

735. The administration of the regulatory regime under the BSA is a core responsibility for FinCEN. Its regulatory functions are administered by the Regulatory Policy and Programs Division, which consists of three offices:

(a) *The Office of Regulatory Policy* is committed to administer effectively the BSA through the development and implementation of policy via outreach, training, and the issuance of regulations and guidance. Specifically, the Office:

- issues new BSA regulations in key financial sectors;
- identifies issues and areas of concern regarding existing BSA regulations;
- provides interpretive guidance to clarify BSA regulations;
- educates and trains financial institutions, regulatory partners and law enforcement officials;
- facilitates the BSA Advisory Group;

- develops and administers BSA forms;
- contributes significantly to the "SAR Activity Review";
- issues Interagency Advisories with banking agencies;
- operates a "hotline" that facilitates the reporting of suspicious activity concerning terrorist financing and a "helpline" that serves as a resource to financial institutions with questions on regulatory matters; and
- coordinates with state regulatory agencies on a variety of issues, such as state and tribal Gaming Commissions, Associations of State Insurance Commissions, Conference of State Bank Supervisors, Money Transmitter Regulators Association and State Banking Associations.

(b) *The Office of Compliance* works to help ensure industry compliance with the BSA through supporting and working in partnership with the agencies and organizations directly examining financial institutions for compliance. The Office provides support for regulatory agencies that examine financial institutions for BSA/AML compliance by:

- formulating examination best practices across industries;
- providing training to BSA/AML examiners;
- tracking the performance of financial institutions experiencing significant BSA compliance deficiencies;
- analyzing examination, BSA and other data to identify activities or financial institutions that may require further review; and
- identifying trends in BSA/AML compliance deficiencies and violations.

The Office also monitors and assesses the level of BSA compliance across industries and communicates with industry representatives, regulatory partners and law enforcement concerning patterns and trends in BSA deficiencies and violations. In addition, this Office is responsible for negotiating and finalizing Memoranda of Understanding (MOUs) with federal and state regulatory agencies that examine financial institutions for BSA compliance.

(c) *The Office of Enforcement* seeks to sanction violations committed by financial institutions, obtain corrective action and deter future non-compliance. It also seeks to educate and provide guidance to financial institutions. Under the BSA, FinCEN has the authority to:

- investigate alleged violations;
- issue letters of caution or warning letters;
- seek injunctions;
- impose civil money penalties; and
- refer apparent criminal violations to the DOJ.

736. In order to leverage existing examination resources and avoid unnecessary duplication of compliance inspections, FinCEN has formally delegated its authority to examine financial institutions for compliance with the BSA to federal functional and financial regulatory agencies (31 CFR 103.56). These agencies comprise: the FDIC, Federal Reserve, OCC, IRS-SBSE, OTS, NCUA, SEC and CFTC.

737. In the case of the SEC and the CFTC, most of their examination and investigation responsibilities have been further delegated to the SROs, principally the NYSE, NASD and the National Futures Association.

738. The financial regulatory agencies and the SROs have the statutory authority, derived from various sources, to:

(a) examine the institutions that they supervise for compliance with the BSA;

(b) refer BSA violations to FinCEN for action; and

(c) take their own enforcement, supervisory and other actions for BSA violations.

739. While the programs and schedules for examining financial institutions under the delegated authority vary depending on the industry and the regulatory agency, there are several basic concepts that are applicable to all industries and all agencies, specifically:

(a) examinations and inspections are conducted independent of outside influence or pressure;

(b) examinations and inspections are generally conducted pursuant to regular cycles, although special examinations and inspections are initiated whenever necessary;

(c) examiners use standardized procedures to determine compliance with BSA requirements;

(d) examiners review the financial institution's policies, procedures, and internal controls as contained in its written AML Program;

(e) examiners review how the financial institution implements its AML Program, scrutinizing the institution's books and records and its operations;

(f) examiners conduct independent transaction testing as necessary; and

(g) regulatory actions are taken and sanctions imposed for instances of non-compliance.

740. The relationship between FinCEN and the federal regulators with delegated authority does not extend to automatic feedback of the results of all BSA examinations. Under the terms of an MOU (dated September 2004) between FinCEN and the federal banking agencies, the latter provide routine quarterly and annual data on their examination programs, but are required to report back on individual examinations only where there is a "significant BSA violation or deficiency". This phrase is defined to include "a systemic or pervasive BSA compliance program deficiency; systemic or pervasive BSA reporting or record-keeping violations; or a situation where a banking organization fails to respond to supervisory warnings concerning BSA compliance program deficiencies or continues a history of program, or systemic or pervasive record-keeping or reporting deficiencies". A similar MOU is being negotiated with the SEC and the CFTC.

Banking sector

Regulatory Framework

741. U.S. banks may be chartered at either national or state level. However, in the overwhelming majority of cases they are supervised by a "primary" federal bank supervisory agency, regardless of whether the charter is national or state. (More than 98 percent of all depository institutions, holding well over 99 percent of all deposits, fall into this category). The OCC charters, regulates, supervises and examines all national banks. The Federal Reserve supervises and examines all state banks that choose to be members of the Federal Reserve System (member banks), as well as Bank Holding Companies. It is also the dominant supervisor for foreign banks operating in the U.S. The FDIC supervises and examines all insured state–chartered banks that choose not to become members of the Federal Reserve System (non-member banks), but due to its role as the provider of deposit insurance, it also has backup supervisory authority over banks that are primarily overseen by the OCC or the Federal Reserve. The OTS is the primary federal supervisor of U.S. savings associations and their holding companies, and the NCUA has responsibility for federally insured credit unions. The effect of the separate federal and state responsibilities is that most institutions have at least two banking regulatory bodies. In summary, the respective responsibilities of the various regulators may be summarized as follows:

Type of institution	Charter	Supervision

National bank/trust company	OCC	OCC, FDIC
State member bank/trust company	State	Fed, FDIC, State
State non-member bank/trust company	State	FDIC, State
Uninsured, state-chartered bank/trust company	State	State, IRS-SBSE
Federal savings association	OTS	OTS, FDIC
State savings association (insured)	State	FDIC, State
State savings association (uninsured)	State	State, IRS-SBSE
Federal credit union	NCUA	NCUA
State credit union (federally insured)	State	NCUA, State
State credit union (privately insured)	State	State, IRS-SBSE

742. Since 1987, the Federal Banking Agencies have been charged (under federal banking laws 12 USC 1818(s) and 12 USC 1786(q) for banks and thrifts) with ensuring that banks and other depository institutions maintain effective BSA/AML compliance programs. The roles, functions, and duties of the Agencies in this respect are similar, and each has issued two regulations in relation to the BSA: the BSA compliance regulation (e.g. 12 CFR 208.63 for member banks of the Federal Reserve System) and the SARs regulation (e.g. 12 CFR 208.62). The language of each agency's regulations is nearly identical.

743. There remains one small group of state chartered entities, the privately insured credit unions, which are not subject to prudential regulation by a Federal Banking Agency, and therefore have no Federal Banking Agency to which BSA compliance can be delegated. There are currently approximately 319 such institutions. Since, constitutionally, it is not possible to delegate a responsibility from federal to state level without congressional funding, FinCEN has delegated examination authority for BSA compliance of this sector to the IRS. However, it should also be noted that these institutions are examined for BSA compliance by their state supervisors in the eight states and one territory in which they are chartered. As discussed elsewhere in this report, the IRS has been handed a similar role for a very broad range of financial and non-financial businesses that otherwise have no federal regulator, thus putting considerable strain on its resources. The IRS has not yet established a cycle for examination of the credit unions.

744. The Federal Banking Agencies, co-ordinate their supervisory efforts through the FFIEC, which was established by statute in 1979. The FFIEC is a formal inter-agency body, which prescribes uniform federal principles and standards for the examination of depository institutions, promotes coordination of bank supervision among the federal agencies that regulate financial institutions, and encourages better coordination of federal and state regulatory activities. A key output for the purposes of this report was the FFIEC Manual published in June 2005. The Federal Banking Agencies work cooperatively with other functional regulators of financial firms where such firms are part of a banking group. These regulators include the SEC, the CFTC, and state insurance and securities authorities.

745. For the reasons noted above, there has been no delegation of BSA examination responsibilities by FinCEN to the state banking regulators, and, therefore, this report does not examine the state regulatory systems in any detail. However, all state banking departments have Joint Supervisory Agreements in place with the federal agencies, and these agreements set forth their respective and/or shared supervisory responsibilities. According to data compiled by the CSBS,[74] 44 state regulators, the District of Columbia and the territory of Puerto Rico undertake AML compliance inspections in conjunction with the Federal Banking Agencies. The exceptions are Colorado, Kentucky, Michigan,

[74] The CSBS is a professional organization representing bank supervisors in the 50 states. It promotes standards within its membership, and acts as a liaison between the states and the federal agencies.

New Mexico, South Carolina and Wisconsin. Similarly, credit unions are subject to joint supervision by the NCUA and their state supervisor, pursuant to a Document of Cooperation executed by the NCUA and the National Association of State Credit Union Supervisors. In addition, FinCEN has entered into information-sharing agreements with 38 state bank regulators, two state credit union regulators, and the banking regulator in Puerto Rico in order to leverage on their experience, although much information on compliance issues at state level comes to FinCEN via the reporting arrangements under its MOU with the federal agencies. Where agreements have not been established with the states, it is usually because their legislatures would need to enact statutory changes to allow for sharing of information with these entities, or because they have delegated their BSA compliance authority to the primary federal regulators.

746. Any degree of reliance on the work of state regulators occurs only where there are formal arrangements for either joint or alternate examinations with the federal agencies. In the case of the joint BSA examinations, the states work closely with the management of the federal agency for BSA compliance. Greater reliance is placed on the states under the procedures whereby alternate annual examinations are undertaken by the state and federal agencies, but the federal agency still remains responsible in all cases for reviewing the work of the state agency. In all cases where the state banking agencies are involved in BSA compliance inspections, they are now required to use the FFIEC Manual in order to have their work recognized as equivalent to that of the federal agencies. Before the advent of the FFIEC Manual, bilateral agreements on examination procedures were agreed between each federal agency and the states.

747. By way of example of the relationship between federal and state authorities, the New York State Banking Department works on an alternate year basis with the Federal Reserve Bank of New York. Consultation takes place between the agencies in advance of any examination by the state authorities, and all examination papers are made available to the Federal Reserve through a shared electronic database. Any enforcement action in respect of BSA compliance failures, using the State Banking Department's powers in respect of safety and soundness, may only be carried out in consultation with the Federal Reserve Bank. A similar relationship is exemplified in the case of the Florida Office of Financial Regulation and the FDIC, which also undertake alternate examinations. Annual meetings are conducted between the two agencies to discuss the examination plan. All examination exit meetings are attended jointly by the agencies, and any compliance issues requiring follow-up action, including formal enforcement action, are handled jointly. Examinations reports are routinely shared between the agencies, but not the underlying work papers, although there is no statutory obstacle to this.

748. For routine supervisory standards, the CSBS operates a system of accreditation of state agencies, which has been designed to try to ensure consistency in standards of regulation at state level, and is described by the CSBS as involving "a comprehensive review of the critical elements that assure a banking department's ability to discharge its responsibilities through an investigation of its administration and finances, personnel policies and practices, training programs, examination policies and practices, supervisory procedures, and statutory powers". Accreditation takes place every five years. Five states (Alaska, Nevada, New Hampshire, South Carolina and South Dakota) together with the District of Columbia) have yet to be given accreditation, but this is not considered by the federal authorities to be a factor in determining whether they will enter into a cooperative arrangement with any particular state for BSA compliance examinations. FinCEN does not impose any conditions under which the federal agencies may enter into an arrangement with the states.

749. There is one exception to such cooperative arrangements between the federal and state regulatory agencies. Under the principles of federal pre-emption, national banks are not subject to state licensing requirements, and so the state agencies have no authority over such banks for safety and soundness purposes. Therefore, only the OCC is involved in BSA compliance examinations, and there is no established mechanism for sharing information on such examinations with the state agencies.

Market Entry

750. All persons wishing to engage in banking and other depository business in the U.S. must be chartered at either federal or state level. The choice of which charter to seek is left to the prospective owners of the financial institution. The OCC requirements for national banks are typical of procedures adopted by other federal agencies. In reaching its decision, the OCC must consider whether the proposed bank:

(a) has organizers who are familiar with national banking laws and regulations;

(b) has competent management that has ability and experience relevant to the type of products and services to be provided, and the scope and size of the projected risks;

(c) has capitalization, access to liquidity, and risk management systems that are sufficient to support the projected volume and type of business; and

(d) can reasonably be expected to achieve and maintain profitability; and will operate in a safe and sound manner.

751. Central to this process is an evaluation of the fitness and propriety of the management team. In its charter manual the OCC states that it application process "is designed to assure that a director or senior executive officer nominated for a position with a national bank will direct the bank's affairs in a safe, sound and legal manner. A person whose competence, experience, character, or integrity is inconsistent with this objective may serve as a senior executive officer or director in a national bank. The OCC will scrutinize more closely a person with experience in a failed or troubled financial institution". The due diligence procedures employed are discussed below.

752. Similar authorization procedures must be applied to depository institutions that wish to obtain deposit insurance from the FDIC, and to state-chartered banks that wish to become members of the Federal Reserve System.

753. Following the initial licensing process, the Change in Bank Control Act is designed to ensure the probity of persons taking a significant or controlling interest in a bank or a bank holding company. This Act is relevant to all federal agencies that have responsibilities for the authorization of banks. Prior notice is required under the Change in Bank Control Act by any person that seeks to acquire control, directly or indirectly, of an insured depository institution. A "person" may include an individual, a group of individuals acting in concert, or certain entities (e.g. corporations, partnerships, trusts) that own shares of banking organizations but that do not qualify as bank holding companies. A person acquires "control" of a banking organization whenever the person acquires ownership, control, or the power to vote 25 percent or more of any class of voting securities of the institution.

754. The applicant must generally give 60 days prior written notice to the relevant federal regulator of a proposed acquisition of a controlling ownership interest. The notice should include biographical and financial information on the filer(s); details of the proposed acquisition; information on any proposed structural, managerial, or financial changes that would affect the banking organization to be acquired; and other relevant information required by the regulator. The primary forms to be completed as a part of a notice are the Interagency Biographical and Financial Report form and the Interagency Notice of Change in Control. The application may be turned down on the grounds that "the competence, experience, or integrity of any acquiring person or of any of the proposed management personnel indicates that it would not be in the interest of the depositors of the bank, or in the interest of the public to permit such person to control the bank".

755. Similarly, the Bank Holding Company Act, as amended, requires that any company (including corporations, partnerships, business trusts, and associations) that seeks to form a BHC by acquiring control over the voting shares of one or more banks must obtain prior approval of the Federal Reserve Board. Federal Reserve approval is also required for an existing bank holding company to expand its banking activities by acquiring an additional bank or BHC if, after the acquisition, the bank holding company would

own more than five percent of the voting shares of the additional bank or BHC. Applicants must meet competitive, financial, and managerial requirements, including requirements with respect to the competence, experience and integrity of their principals. Foreign bank applicants also must be found to be subject to comprehensive, consolidated supervision by their home country regulators.

756. The Anti-Drug Abuse Act of 1986 requires, in part, that, upon receiving a notice of acquisition of control, the Federal Banking Agency shall conduct an investigation of the competence, experience, integrity and financial ability of each person named in a notice of acquisition of control and shall make an independent determination of the accuracy and completeness of any information required of such person. Upon completion of the investigation, a written report of the finding shall be prepared which will become a record of the agency.

757. Each of the Federal Banking Agencies is also authorized to suspend from office an institution-affiliated party that has been charged with a criminal violation of 18 USC 1956, 1957 or 1960 (conducting an unlicensed money transmitting business) or 31 USC 5322 or 5324. The suspension order prohibits the individual from participating in any manner in the affairs of any financial institution supervised by the agencies until the criminal case is resolved [12 USC 1818(e) and (g)]. If an institution-affiliated party is convicted of one of these crimes, the appropriate Federal Banking Agency may permanently bar the individual from further participation in the affairs of any regulated financial institution. In addition, any individual who has been convicted of a criminal violation of 18 USC 1956 or 1957 may not own or control an insured depository institution, or participate in its affairs for a minimum of 10 years after the conviction [12 USC 1829(a)]. After that period, the individual may only participate with the prior approval of the FDIC.

758. When conducting their due diligence, the financial banking agencies scrutinize the backgrounds of persons who are the organizers, senior executive officers, directors or principal shareholders of the bank. These individuals are investigated to determine whether they have the appropriate experience, competence, integrity, character, and financial ability to direct and/or manage a bank's affairs in a safe, sound and legal manner. On 22 January 1988, the FFIEC issued the "Joint Statement of Guidelines on Conducting Background Checks and Change in Control Investigations." This provides guidance regarding conducting checks on individuals seeking either to establish new depository institutions or holding companies, or to effect changes in control. The guidance details the steps that these agencies will take in investigating the accuracy and completeness of the information submitted by such individuals. All signatories currently perform background investigations in accordance with the guidelines. In 2003, the background check process was enhanced and now generally requires the submission of fingerprints from individuals who are subject to background checks in the applications process (SR letter 03-10, 28 May 2003). Particular attention is paid to any person who was previously associated with a failed or problem financial institution or other situation that may bring into question the person's personal or fiduciary integrity.

759. Requests for background investigations are forwarded to the FBI and other federal agencies, including, but not limited to, the U.S. Customs Service, IRS, DEA, the State Department, Interpol and the Central Intelligence Agency. In some instances, requests for background investigations may be sent to foreign law enforcement or regulatory authorities. Checks are also made through internal agency databases and the FinCEN database of persons named in SARs. The agencies may also access a variety of other databases, many of which are publicly available. These include Lexis/Nexis for legal proceedings and news, company financial reports from such providers as Dun & Bradstreet Business Information Reports, and public records such as bankruptcy filings, tax liens, and judgments.

Supervisory Procedures

760. The supervision and regulation of U.S. banking organizations by the Federal and State Banking Agencies for safety and soundness purposes is accomplished through a combination of off-site reviews and on-site examinations.

761. Off-site supervision involves continual surveillance and assessment of information from a variety of sources, including the supervised institution, external auditors, and other supervisors, both foreign and domestic. The information includes standard regulatory reports, reports of recent examinations and inspections, internal management and internal and external auditor reports, reports filed by public companies (e.g. 10-Qs and 10-Ks) application materials, and publicly available material (e.g. information published in the financial press and elsewhere). The number and the type of report forms that must be filed depend on the size of an institution and the scope of its operations. Examiners also routinely conduct a review of the FinCEN databases of SARs and CTRs (to which they have online access) to determine if a banking organization that is about to be examined has filed such reports and that they appear complete and timely.

762. On-site examinations of banks, thrifts, credit unions and the U.S. branches and agencies of foreign banking organizations are required by regulation to occur once every twelve to eighteen months (e.g. 12 FR 208.64) for entities subject to federal oversight. The agencies make risk assessments with respect to the banking organization's operations, and those that are deemed to present higher compliance risks or have a history of compliance problems may be examined more frequently than the norm. For larger organizations, the Federal Banking Agency maintains resident on-site examiners who provide continuous supervision of the institution and at least quarterly updates on the institution's condition and risk assessment. Examination areas for all depository institutions include any cross-border operations.

763. Between 1 October 2004 and 30 September 2005, the Federal Banking Agencies and the IRS (with respect to its responsibilities for depository institutions) undertook a total of 10,409 BSA/AML examinations and put in place a total of 71 formal enforcement actions due to BSA violations. The following table provides the numbers of examinations conducted and formal enforcement actions taken by each agency:

Federal Regulator	BSA/AML Exams conducted in FY 2005	Formal Enforcement Actions* taken in FY 2005
FDIC	2,755	16
Federal Reserve	682	9
NCUA	4,715	0
OCC	1,530	32
OTS	722	14
IRS	5	0
Total	10,409	71

*A formal enforcement action is a supervisory action used to compel a bank to address egregious violations of the law. Examples of these types of actions are Orders to Cease and Desist and Civil Money Penalties. Formal actions generally are public. In addition, the regulators took in excess of 2,000 "informal" enforcement actions, which relate primarily to technical violations of the BSA requirements.

764. In on-site examinations, supervisory staff generally: (1) evaluate the soundness of the institution's assets and the effectiveness of its internal operations, policies, and management; (2) analyze key financial factors such as the institution's capital, earnings, liquidity, and sensitivity to interest rate risk; (3) assess the institution's exposure to off-balance-sheet risks; (4) check for compliance with banking laws and regulations; and (5) determine the institution's overall soundness and solvency. A key component of the AML part of the examination, under the delegation from FinCEN as well as on safety and soundness grounds, is to ensure that the banking organization has properly implemented a BSA/AML compliance program.

765. In terms of the application of supervisory measures to assess compliance with AML/CFT obligations, the federal and state banking regulators have adopted the FFIEC Manual, which was issued in June 2005. This FFIEC manual (over 300 pages) provides a detailed description of the objectives and processes to be applied when conducting onsite examinations for AML compliance. It establishes minimum procedures that are to be used in every examination, and provides core and

expanded procedures to review and test the individual components of a bank's AML Program. The FFIEC Manual focuses attention on the need for examiners to identify how risk is identified and managed within institutions, and to assess the effectiveness of risk management by a review of the systems and controls, and by mandatory transaction testing. While the FFIEC Manual was developed primarily as an examiners' tool to ensure consistency in the AML examination procedures across the entire banking sector, it has also been structured to provide extensive guidance to the industry on its AML responsibilities in general, and on risk management in particular. The FFIEC Manual has been formally published and is available in its entirety to the banking sector and wider public.

766. Examiners are required, first, to determine whether the institution has included BSA/AML procedures in all of its operational areas, including retail operations, credit, private banking, and trust, and has adequate internal audit procedures to detect, deter and report money laundering activities, as well as other potential financial crimes. In addition, examiners will review a banking organization's fraud detection and prevention capabilities, and its policies and procedures for cooperating with law enforcement (whether through responding to subpoenas, acting on information requests under the USA PATRIOT Act, or otherwise). Transaction testing (including the SAR reporting arrangements) is a core part of the examination process.

767. Examinations carried out by state banking agencies under the cooperative agreements with the federal authorities are conducted in accordance with the FFIEC Manual and procedures used by the federal authorities.

768. The federal regulatory agencies also undertake special examination projects that are designed to address identified or emerging risks on a regional or national level. These would typically involve examining a group of banks, along a common theme (e.g. foreign correspondent banking), in order to establish industry practice and the risks posed. Such special examinations are undertaken in full consultation with the institutions selected for the process, and will often be used as the basis for providing additional guidance to the industry as a whole.

769. The production of the FFIEC Manual has been universally welcomed by the banks, as has been the outreach program by the regulators to alert the industry to the details of the document. The banks have expressed the view that this process leads to a more informed review of their overall systems and controls, rather than a narrow focus on individual breaches of the detailed regulations. They are expecting that the regulators will now take a longer term view of the effectiveness of compliance procedures. As a result, they feel that the quality of examinations has improved significantly in recent months, particularly with respect to the consistency of the messages that are being delivered. However, they have expressed some concerns that the FFIEC manual does not fully grasp the complexities of some of the situations, and that, over time, there may be a tendency to convert into mandatory requirements those issues that are indicated as being "for consideration" in the manual.

770. The Federal Banking Agencies have broad statutory authority to examine all books and records of any financial institution that they regulate. In addition, the USA PATRIOT Act also requires that financial institutions respond to requests for information and account documentation for any account opened, maintained, administered or managed in the U.S. by the financial institution within 120 hours after receiving the request from a Federal Banking Agency [31 USC 5318(k)(2)]. The Federal Banking Agencies also have investigation authority, separate from examination authority, permitting them to take sworn testimony and issue subpoenas for the production of documents from third parties [12 USC 1818(n) and 1784(b); and 12 USC 1820(c) and 1786(p)].

771. In addition, the USA PATRIOT Act provides that the Secretary of the Treasury or the Attorney General may issue a subpoena to any foreign bank that maintains a correspondent account in the U.S. and may request records related to such correspondent account, including records maintained outside of the U.S. relating to the deposit of funds into the foreign bank [31 USC 5318(k)(3)].

772. Since the federal banking agencies undertake BSA/AML examinations under delegated authority from FinCEN, all the agencies have entered into a common MOU with FinCEN, signed in September 2004. The MOU provides for the regular passage of information from the agencies to FinCEN on the number and scope of examinations undertaken, the resources applied to the process (including details of the training program), and the number and types of violations identified. In exchange, FinCEN is committed to providing regular information on its enforcement actions and on its analytical products, specifically those derived from the data provided by the banking agencies. The federal banking agencies have also entered into information-exchange MOUs with those state banking agencies that undertake BSA compliance examinations.

Securities sector

Regulatory Framework

773. As with the banking sector, there are several players in the regulatory framework for the securities industry. The SEC administers the U.S. securities laws, and adopts rules implementing those laws. It also oversees and examines market participants, including broker-dealers and mutual funds, and has the authority to take civil enforcement actions against persons and entities suspected of violating the securities laws. Section 19(g) of the Securities Exchange Act of 1934 and implementing rules have delegated some examination and enforcement authority to securities SROs (such as the NYSE and NASD). In addition, NFA's examination and enforcement authority is derived from 7 USC 7(b), 7(d), 12c and 21. However, the federal regulators retain and exercise the authority to: (i) approve SRO rules; (ii) review the examination, compliance and enforcement procedures of the SROs; (iii) take action against the SROs if they are deemed to be inadequately fulfilling these functions; (iv) examine supervised entities either independently or jointly with the SRO; and (v) enforce SRO rules directly against registered entities. This arrangement is consistent with the IOSCO Core Principles (see Principles 6 and 7). Mutual funds must register directly with, and be examined by, the SEC, as there is no SRO for this sector.

774. The SEC also generally regulates investment advisers with over USD 25 million in assets under management, multi-state investment advisers, advisers to registered investment companies, and non-U.S. investment advisers. The states generally regulate investment advisers with less than USD 25 million in assets under management. Although state-registered advisers are governed primarily by state law, several provisions of the Investment Advisers Act (Advisers Act) and SEC rules apply to them. For example, among other provisions, section 206 of the Advisers Act, which prohibits fraudulent conduct, applies to state-registered advisers. The SEC has authority to bring enforcement actions against state-registered advisers for fraud under this section.

775. The CFTC is responsible for the regulation of futures commission merchants and introducing brokers in commodities. However, much of the day-to-day examination work is delegated to the NFA. As an oversight agency, the CFTC has the authority to review NFA's examination, compliance and enforcement procedures, and is authorized to take action against NFA if it deems that NFA has inadequately fulfilled these functions. In summary, the respective responsibilities of the various regulatory authorities are shown in the following table.

Type of institution	Registration	Supervision
Broker-dealer	SEC, NASD, NYSE	SEC, NASD, NYSE
Mutual fund	SEC	SEC
Futures commission brokers	CFTC, NFA	CFTC, NFA
Introducing brokers in commodities	CFTC, NFA	CFTC, NFA
Investment advisers	SEC, state	SEC, state

Market Entry

776. Securities broker-dealers register with the SEC by filing a Form BD, which elicits information about the background and anticipated business of the broker-dealer and its principals, controlling persons, and key employees. The broker-dealer must meet statutory requirements involving defined professional standards and become a member of at least one SRO, such as the NYSE or NASD, both of which have extensive due diligence procedures in their membership application process. Moreover, a broker-dealer must comply with all applicable state requirements, and its "associated persons" must satisfy applicable examination, licensing and qualification requirements. Associated persons are individuals who work for a registered securities broker-dealer as an employee, an independent contractor, or otherwise. Although associated persons usually do not have to register separately as securities broker-dealers with the SEC, securities broker-dealers are required to supervise associated persons with a view to preventing violations of the federal securities laws.

777. SRO rules also require their members to establish, maintain, and enforce a system of supervisory control policies and procedures that, for example, test and verify that the member's supervisory procedures are reasonably designed to achieve compliance with applicable securities laws and regulations and applicable SRO rules. Firms also may be required to create additional supervisory procedures or amend existing ones if such a need is identified by the testing and verification.

778. Registered persons who are found to have violated securities rules and regulations face the following sanctions that jeopardize their continued employment in the securities industry:

(a) bar from the securities industry;

(b) suspension for a specific period of time, often only being re-admitted after paying fines and/or re-qualifying by passing specified qualification examinations; and

(c) fines and, in certain situations, orders to make restitution if customers were harmed financially.

779. In addition, persons who have engaged in certain types of misconduct are ineligible to serve or act in the capacity of employee, director, member of an advisory board, investment adviser or depositor of any registered investment company (e.g. mutual funds). Although investment advisers are not yet subject to AML Program requirements, it is helpful to note that the SEC may deny registration to persons who have engaged in certain misconduct that are seeking to become investment advisers and may bar, suspend, or place limitations on the activities of persons who are, or are seeking to become, associated with an investment adviser if those persons have engaged in certain misconduct.

780. A person who is subject to a statutory disqualification resulting from an arrest or conviction for certain financial-related crimes and other regulatory actions must undergo a rigorous application process when seeking employment in the securities industry. Re-admission would only be approved if the employer agrees to subject that person to special supervision and the SRO and the SEC determines that investor protection concerns are satisfied.

781. There are similar registration requirements placed on persons engaged in the futures and commodities industry. With certain exceptions, all persons and organizations that intend to do business as futures professionals must register with the CFTC pursuant to the Commodity Exchange Act (CEA). The primary purposes of registration are to screen an applicant's fitness to engage in business as a futures professional and to identify those individuals and organizations whose activities are subject to federal regulation. In addition, all individuals and firms that wish to conduct futures-related business with the public must apply for membership with the NFA. The CFTC has broad, specific power to bar criminals and alleged criminals from being involved in the futures industry. The CFTC is specifically authorized to refuse to register persons convicted of certain crimes, and to suspend or modify the registration of any person registered that is charged with certain crimes [CEA Sections 8a(2), (3) and (11)].

Supervisory Procedures

782. The SEC and CFTC resources dedicated to combating money laundering are integrated into their major program areas, and a risk-based approach forms an integral part of the SEC's and CFTC's strategy to meeting their money laundering responsibilities. In the securities and futures industries, the SROs examine their members for compliance with BSA/AML requirements, as well as with other federal securities regulations and their own rules and regulations (including AML-related rules).

783. The NYSE and NASD have examination cycles designed to address the regulatory concerns posed by different categories of firms. Accordingly, firms with substantial capital, investor or market exposure or, in some instances, a history of regulatory problems, are examined annually. Other firms, which present less public exposure and risk, generally are examined less frequently. The examination programs are reviewed by the SEC. The SEC covers BSA compliance in every oversight examination where it reviews the SROs' examination processes and findings. In addition, SEC staff selects several firms nationally each year to be the subject of "full-scale" AML examination, based on certain risk factors. These examinations provide data regarding national trends, and are designed to oversee the work of the SROs. As a matter of routine, the SEC, NASD, NYSE and FinCEN hold quarterly meetings to share information on the examination process, and to establish guidelines for examiners, where necessary. In addition, the SEC has sought to move to greater standardization of BSA examination procedures to help ensure consistency. The following table shows the recent record of examinations by the various agencies.

FY 2005				
	Exams completed	AML included	AML deficiencies	Formal enforcement
SEC broker-dealers	745	381	220	-
NYSE broker-dealers	484	173	50	5
NASD Broker-dealers	1,750	1,676	710	74
SEC mutual funds	526	136	23	-
SEC transfer agents	55	37	4	-

784. NFA has responsibility to examine members for compliance with AML, financial integrity, financial reporting, sales practice, recordkeeping, and other requirements. These examinations are conducted pursuant to an examination module that it has developed in consultation with the CFTC. NFA employs risk-based auditing guidelines, whereby the frequency and scope of the examination will be based on NFA's overall assessment of the financial and operational risk posed by the particular firm. However, such examinations must occur every nine to eighteen months for futures commission merchants, and every three years for introducing brokers in commodities. In 2003, NFA conducted 365 examinations, all of which included assessment of AML compliance. The NFA advised the assessment team that, to date, none of its formal enforcement actions have related to non-compliance with AML/CFT measures. The CFTC was also of the opinion the implementation of the new AML/CFT requirements has posed no substantial problems for this part of the securities sector.

785. Pursuant to Sections 17(a) and (b) of the Securities Exchange Act [15 USC 78(q)(a) and 78(q)(b)], there are no restrictions upon examiner access to the books and records of broker-dealers. SEC examiners also have unlimited access to the books and records of mutual funds that are required under the federal securities laws (15 USC 80a-30). In addition to these rules granting the SEC general access to the books and records requirements of regulated entities, all securities broker-dealers must also comply with the reporting, recordkeeping, and record retention requirements of regulations adopted pursuant to the BSA (17 CFR 240.17a-8).

786. For examination purposes, section 17(a) of the Securities Exchange Act provides authority for the SEC to request all records of registered broker-dealers, transfer agents and other entities, including but not limited to required records, to be made available for examination by an SEC representative. In general, this provision enables the SEC to examine all records, regardless of whether or not the SEC requires the record to be kept by the entity. In addition to being able to examine any of a registrant's records without limitation, pursuant to section 17(b), the SEC is authorized to examine a registrant any time it deems appropriate, as often as it deems appropriate, and according to whatever type of cycle it wishes. The SEC has taken the position that its examination authority is unconditional except for the requirement that any such record examination be reasonable. To be sure firms understand the extent of the authority granted by the various securities laws and the firm's rights thereunder, SEC representatives provide Form 1661 (which identifies and explains, in general, the rules to which the firms are subject) to firms prior to an examination.

787. The SEC need not conduct a formal examination to obtain copies of registrants' books and records. For example, the SEC may issue subpoenas pursuant to section 21(b) of the Exchange Act to obtain documents from both regulated and unregulated persons and entities in connection with investigations of any violations of the federal securities laws. The SEC may issue subpoenas without giving notice that the target is under investigation.

788. The securities firms generally are of the opinion that the quality of examinations has improved over the last two years. They feel that examiners are now adding value through the BSA compliance program, and are responsive in providing guidance. However, contrary to the practice adopted by the banking regulators, the securities regulators' examination procedures have not been made available to the industry. This is consistent with current practice in all areas of securities regulation, not just BSA compliance.

789. It should be noted that since investment advisers and commodity trading advisers have no AML Program requirements at present, examination procedures for these institutions do not cover BSA compliance.

Insurance sector

Regulatory Framework

790. The insurance industry in the U.S. is currently subject to state rather than federal regulation, primarily for safety and soundness rather than AML purposes. States vary in their regulatory and supervisory approach, in particular with respect to the structure of examinations, frequency of examinations and training of examiners. In some states, insurance companies are already subject to AML statutes, currency reporting requirements, and/or suspicious activity reporting requirements under state law. According to an unpublished survey, conducted by the National Association of Insurance Commissioners (NAIC), of state statutes or rules applicable to insurance companies, 38 states have money laundering statutes, 21 have currency reporting requirements and one has a suspicious activity requirement.[75] However, state regulators are not involved in the examination of life insurers of covered insurance products for BSA purposes. This function has been delegated to the IRS.

791. In the case of banks that sell insurance products, the Federal Banking Agencies will play a supervisory role. Insurance products are typically sold to bank customers through networking arrangements with an affiliate, an operating subsidiary, or other third party insurance providers. Banks also provide cross-selling opportunities for customers by expanding the insurance products they offer. The types of insurance products sold may include life, health, property and casualty, and fixed or variable annuities. In this regard, the FFIEC Manual describes the examination techniques that will be employed to assess the adequacy of a bank's systems to manage risks associated with insurance sales and the management's ability to implement effective monitoring and reporting.

[75] It should be noted that, although a copy of this survey was requested by the assessment team, it was not made available.

Market Entry

792. As insurance is a state matter, it is not appropriate to describe in this report all the licensing processes adopted by all state insurance regulators. Therefore, this section on market entry will only address the processes and procedures of the California Department of Insurance in admitting and licensing insurers to operate in the state of California. California has been selected because it is one of the five states with the most premiums written in all lines of insurance. While the assessment team has been led to understand that state licensing procedures are broadly similar, there are no assurances that the following reflects what takes place in other states.

Case study – California

The applicant proposing to form and operate an insurance company in California is required to apply to the Insurance Commissioner requesting approval of the name under which he/she intends to transact its business (s.881, California Insurance Code). Name approval requests for domestic companies in the process of formation must be accompanied by a disclosure of the company's principals. The applicant must also file articles of incorporation with the Secretary of State. After the corporation has been formed and duly qualified, it may apply to the Department of Insurance for an organizational permit so that it can raise the necessary capital to commence its operations. The permit application is an important step in the qualification of the insurer in that it requires detailed biographical information concerning the officers and directors, the contemplated plan of operation of the corporation, a projection of anticipated income and disbursements for a substantial period of years, and other essential data.

The admission procedure involving the licensing of a new insurer is detailed and time-consuming. It requires detailed actuarial and financial studies and projections indicating the company's anticipated income and disbursements over a period of five years; detailed field investigation of the background of each officer, director, and key management personnel of the applicant so as to determine their fitness and capability to engage in the insurance business; and detailed description and analysis of the applicant's proposed plan of operation in California, including samples of the contracts which it intends to issue, methods to be employed in the training and recruitment of its sales force, description of the method by which its accounting and bookkeeping records will be maintained so as to provide the periodic statements required by the Department of Insurance.

The California Insurance Code also sets out the minimum capital and surplus requirements for every insurer admitted to transact business in California (whether organized under the laws of the State of California or another jurisdiction). Section 2275, Article 1 of Subchapter 3 of the California Code of Regulations provides that the Insurance Commissioner will, in considering an applicant insurer for admission to transact business in California, determine each case largely upon its individual merits as to operating record and financial condition, and a reasonable surplus sufficient to meet all ordinary contingencies will be required in every case in addition to the minimum capital requirements specified in the statutes. The applicant must establish that its financial condition is such that the policyholders and creditors with which it will deal will be reasonably safe. Compliance with the minimum capital requirements does not guarantee admission of the applicant. Each application for admission is determined after a consideration of all of the qualifications of the applicant.

A foreign insurer (including an insurer operating in another U.S. state) also has to submit its most recent Report of Examination by, together with an original certification from, its domiciliary state insurance regulatory agency if it does not meet all of the following requirements:

(a) Such insurer has transacted insurance business under the same corporate name and management for at least five years immediately preceding the date of its application for

the admission to the State of California. Such insurer is, and for at least five years immediately preceding the date of its application for admission to the State, has been, authorized to transact insurance business in not less than five states.

(b) Such insurer, through its duly authorized officers who have full knowledge of the facts, files a verified statement under oath that it has never been denied admittance in any state and that its certificate of authorization to transact business in any state has never been revoked or suspended.

(c) Such insurer has been officially examined by the insurance commissioner or similar official of its home state as of a date not more than two years preceding the date of its application for admission to California.

(d) Such insurer, in addition to all other papers required to be filed, files with the Department of Insurance a certified copy of the last report of such examination.

(e) Such insurer has a cash capital of not less than USD 500,000 and a surplus over all liabilities of not less than USD 250,000.

The foregoing regulation 2276, Article 1 of Subchapter 3 is not to be construed as waiving the statutory right of the Insurance Commissioner to make or cause to make such examination in the case of any foreign insurer who meets all of the foregoing requirements.

Supervisory Procedures

793. At the time of the on-site visit, the IRS had yet to commence its AML/CFT examination of the insurance sector. This is because insurers have been given until 2 May 2006 to implement the AML Programs and begin filing SARs as required by the new final rules. In the meantime, the IRS is taking the following action (in consultation with FinCEN): (1) developing and adding to its Standard Examination Manual a new Part for examining the insurance sector for AML compliance; (2) including the examination of the insurance sector in its next annual examination work plan for fiscal year commencing 1 October 2006 to 30 September 2007; and (3) assigning examiners for the insurance sector depending on its available resources. Examinations will include the review of policies, procedures, books and records and sample transaction testing of SARs.

794. In the case of banks that sell insurance products, the Federal Banking Agencies will apply the following examination procedures (set out in the FFIEC Manual) for assessing a bank's sale of insurance policies.

(a) Review the policies, procedures, and processes related to insurance sales. Evaluate the adequacy of the policies, procedures and processes given the bank's insurance sales activities and the risks they present. Ensure that controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

(b) Review the contracts and agreements for the bank's networking arrangements with affiliates, operating subsidiaries, or other third-party insurance providers conducting sales activities on bank premises on behalf of the bank.

(c) Depending on the bank's responsibilities as set forth in the contracts and agreements, review management information system (MIS) reports (e.g. large transaction reports, single premium payments, early policy cancellation records, premium overpayments and assignments of claims) and internal risk rating factors. Determine whether the bank effectively identifies and monitors insurance product sales.

(d) Depending on the bank's responsibilities as set forth in the contracts and agreements, determine whether the bank's system for monitoring insurance products for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.

(e) If appropriate, refer to the OFAC procedure.

(f) If the bank or its majority-owned subsidiary is responsible for the sale of direct monitoring of insurance, then examiners should perform transaction testing procedures. On the basis of the bank's risk assessment of its insurance sales activities, as well as prior examination and audit reports, select a sample of insurance products. From the samples selected, perform the following procedures:

- review account opening document and on-going due diligence information;

- review account activity, compare anticipated transactions with actual transactions; and

- determine where activity is unusual or suspicious.

(g) On the basis of procedures completed, including transaction testing, examiners form a conclusion about the adequacy of policies, procedures, and processes associated with insurance sales.

(h) Examiners are also guided on the insurance documents that they should review during their on-site visits.

Money Services Business sector (including money remitters and foreign exchange)

795. The regulatory framework as it applies to MSBs, including foreign exchange operations is described in section 3.11 of this report.

Credit Card Operators

796. Responsibility for the oversight of BSA compliance by the credit card operators has been delegated to the IRS. For a description of the IRS regulatory structure and procedures (see section 3.11 below). Examinations of credit card operators started in the course of 2005, but no information was available on levels of compliance within this sector. The operators are also examined by the FFIEC (as an umbrella for the various functional regulators) on the basis of the systemic importance of the integrity of its data processing service, but there does not appear to be an AML element to this inspection program.

Enforcement and Sanctions

General—FinCEN

797. While examination authority for BSA compliance has been delegated to the Federal Banking Agencies, the same does not apply to enforcement powers under the BSA, which remain with FinCEN. However, the banking agencies have their own enforcement powers under Title 12 provisions (12 USC 1786 and 1818) which cover violations of "any law or regulation" (including the BSA). Under the BSA (31 USC 5311 et seq.) and its implementing regulations (31 CFR Part 103), FinCEN may bring an enforcement action for violations of the reporting, recordkeeping or other requirements of the BSA. For example, civil money penalties may be assessed for recordkeeping violations under 31 CFR 103.29, for reporting violations for failing to file a CTR in violation of 31 CFR 103.22, for failing to file a suspicious activity report in violation of 31 CFR 103.21, or for failing to have an adequate AML Program in place, in violation of 31 CFR 103.120.

798. Civil money penalties for willful violations of the BSA range from USD 25,000 per violation (or per day that an entity fails to have an adequate anti-money laundering program in place) to the actual amount involved in the violation, not to exceed USD 100,000 per violation under 31 CFR 103.57. Additionally, under 31 USC 5321(a)(7), civil money penalties equal to but not less than two times the amount of the transaction, but not greater than USD 1,000,000 may be imposed on institutions that violate special international counter money laundering provisions of the BSA codified under 31 USC 5318(i), 31 USC 5318(j), or 31 USC 5318A. Finally, under 31 USC 5321(a)(6)(b), civil money penalties up to USD 50,000 may be imposed on any financial institution or non-financial trade or business that engages in a pattern of negligent violations of the BSA.

799. The factors taken into account by FinCEN in determining any civil money penalty amount include.

(a) severity of the violations (number, time-span, rate of failure);

(b) nature of violations (cause, repetitive/isolated, program breakdown);

(c) method of discovery (internal audit, supervisory examination, law enforcement tip);

(d) corrective action taken (immediate, comprehensive, management supervised);

(e) other law enforcement/supervisory agency actions;

(f) year of violations; and

(g) size and financial health of institution.

800. Once FinCEN's Office of Enforcement has determined that there is a case to answer, it will issue a charging letter to the entity listing the grounds for possible enforcement action. The issuance of a charging letter usually results in a process of negotiation with the institution to agree on the level at which a civil money penalty should be applied. In circumstances where the entity does not consent to the assessment of a civil money penalty, FinCEN may consider passing the matter to the DOJ for possible criminal litigation, with Treasury as the plaintiff. However, in the vast majority of cases, the entity will prefer to consent to the assessment of a civil money penalty for a regulatory violation, since criminal prosecution for a money laundering offense would have a potentially fatal impact on the entity.

801. FinCEN has separate authority to assess a civil money penalty against a financial institution or non-financial trade or business, and a partner, director, officer, or employee of a financial institution or non-financial trade or business, or individual for willful violations of the BSA or FinCEN regulations issued thereunder (31 USC 5321, 31 CFR 103.57). A civil penalty may be levied not to exceed the greater of the amount (up to USD 100,000) involved in the transaction or USD 25,000 (31 CFR 103.57). Other sanctions are available to FinCEN to resolve civil enforcement matters include letters of warning or caution; injunctions in the appropriate U.S. District Court; and the imposition of consent orders. The following chart provides data on the enforcement measures taken by FinCEN in fiscal years 2003, 2004 and 2005.

Regulatory activity	2003	2004	2005
Compliance matters referred to FinCEN for possible enforcement action reviewed by FinCEN pursuant to its enforcement authority	49	52	229
Assessments of civil money penalties	4	2	3
Civil money penalties assessed	USD 24.45 million	USD 25.01 million	USD 34.7 million

802. Generally, criminal penalties for violations of the BSA (prosecuted by the DOJ) are available under 31 USC 5322. Persons convicted of violating the BSA may be subject to up to five years' imprisonment, and a criminal fine of up to USD 250,000. Persons convicted of engaging in a pattern of illegal activity involving more than USD 100,000 in a twelve-month period may be subject to up to ten years' imprisonment and a criminal fine of up to USD 500,000. Criminal penalties for violations of the structuring and bulk cash smuggling statutes are prescribed within the respective statutes. The first criminal prosecution against a bank for money laundering was brought in 2002 in the case of Broadway National Bank, on the grounds that it had no compliance program in place and persistently failed to monitor and report suspicious transactions. Subsequent convictions were achieved against Banco Popular de Puerto Rico in 2003 and AmSouth Bank in 2004.

803. The following chart summarizes the civil and criminal penalties for willful and negligent violations of the BSA.

BSA Civil Penalties (Willful violations)

Currency Transaction Reports (CTRs)	USD 25,000 to USD 100,000 per violation
Suspicious Activity Reports (SARs)	USD 25,000 to USD 100,000 per violation
AML Compliance Program	USD 25,000 per day
Record-keeping	USD 1,000 per violation
Report of Foreign Financial Accounts (FBARs)	USD 25,000 to USD 100,000 per violation
Structuring	Dollar Amount Involved in Transactions
USD 10,000 Received by Trade or Business (Form 8300s)	USD 25,000 to USD 100,000 per violation
International Counter-Money Laundering Provisions	2X Transaction Dollar Amount to USD 1 million
BSA Civil Penalties (Negligent)	
Negligence	USD 500 per violation
Pattern of negligent activity	USD 50,000
BSA Criminal Penalties	
General	5 Years Imprisonment USD 250,000 Fine
Pattern of Illegal Activity	10 Years Imprisonment USD 500,000 Fine

Banking sector—Federal Banking Agencies

804. The Federal Banking Agencies have broad authority under their own statutory authority to take informal and formal administrative sanctions against the financial institutions that they supervise. In general, AML/CFT problems that give rise to enforcement actions relate to compliance with the four-part BSA/AML compliance program rule and with SAR filing requirements. In cases where examiners have identified a violation of the BSA/AML compliance program requirement, the Federal Banking Agencies are required by law to take enforcement action requiring the financial institution to correct the problem [12 USC 1818(s)]. The provisions of each such action are tailored to address the particular violations and weaknesses identified by the examiners. Generally, banking organizations consent to the issuance of formal enforcement actions and move quickly to implement the required remedial measures. Depending on the degree of non-compliance, a regulatory agency can issue written orders, that impose remedial actions, impose civil money penalties, reprimand individuals or bar them from employment within the industry, restrict or suspend the operation of the institution, revoke the license of the institution, refer the matter to DOJ for possible criminal penalties, and/or refer the matter to FinCEN for possible civil money penalties.

805. The most serious administrative sanction that the Federal Banking Agencies may impose is to terminate the activities of a financial institution that has been found guilty of any of certain criminal offenses relating to money-laundering. These offenses are: laundering of monetary instruments (18 USC 1956); engaging in monetary transactions in property derived from specified unlawful activities (18 USC 1957); and the willful violation of certain provisions of the BSA or regulations issued thereunder (31 USC 5322). For domestic U.S. banking organizations, the FDIC may be appointed as a receiver of any insured depository institution that has been found guilty of the enumerated criminal offenses [12 USC 1821(c)(5)(M)].

806. Various statutes authorize individual Federal Banking Agencies to take specific action. Separately, the FDIC may terminate the deposit insurance of any state-chartered insured depository institution that has been convicted under 18 USC 1956 or 1957 [12 USC 1818(w)]. The OCC may revoke the charter of any national bank that has been convicted of the crimes described in 18 USC 1956 or 1957, or 31 USC 5322 or 5324 [12 USC 93(d)]. For branches and agencies of foreign banks, the Federal Reserve, the OCC, or the FDIC, as appropriate, may commence termination proceeding against a branch or agency of a foreign bank guilty of a money laundering offense [12 USC 3105(i); 12 USC 93(d); 12 USC 1821(c)(5)(M)]. The OTS has authority to revoke the charter of any Federal savings association [12 USC 1464(w)]. The NCUA has authority to appoint

itself conservator of any insured credit union or terminate the deposit insurance of any insured credit union [USC 1786(h)(1)(C) and (v)].

807. The Federal Banking Agencies are authorized to take formal administrative action against any officer, director, employee, controlling stockholder or agent of any financial institution, and, in certain cases, any independent contractor (collectively "institution-affiliated party") of any financial institution [12 USC 1813(u) and 1818(b), (c), (e), (g), and (i)]. Such actions include: (1) Cease and Desist Orders; (2) Orders of Suspension, Removal, or Prohibition; and (3) Civil Money Penalty Assessments.

808. By law, the Federal Banking Agencies must make formal enforcement actions public. Several banks in recent years faced severe criminal and civil penalties as a consequence of BSA lapses (see also the data under Recommendation 32). The number of formal enforcement actions taken by each of the banking agencies in the period 2001-2005 is tabulated below.

Agency	Number of formal actions
Federal Reserve	37
FDIC	47
NCUA	1
OCC	76
OTS	38

809. Typically, these enforcement actions would result in cease and desist orders, civil money penalties, prohibition orders or supervisory agreements. The table below describes some examples of recent enforcement actions taken by the U.S. authorities for violations of BSA requirements.

NAME AND DATE	PENALTY	DESCRIPTION OF THE VIOLATION
March 2004 Riggs Bank, N.A.	USD 25 million	• Willful violation of the AML Program requirement of the BSA. • Deficiencies in designing a program tailored to the risks of its business that would ensure appropriate reporting, implementing the procedures it did have, and responding to classic "red flags" of suspicious conduct. • Failure to correct the violations and implement an adequate BSA program in a timely manner.
October 2004 AmSouth Bank of Birmingham	USD 10 million	• Failure to establish an adequate AML Program • Failure to file accurate, complete and timely SARs • Systemic defects in its program with respect to internal controls, employee training, and independent review that resulted in failures to identify, analyze and report suspicious activity.
December 2005 ABN AMRO Bank, N.V.	USD 80 million	• Unsafe and unsound practices • Systemic defects in its internal controls to ensure compliance with U.S. AML laws and regulations which resulted in failures to identify, analyze and report suspicious activity • Participation in transactions that violated U.S. sanctions laws
April 2006 BankAtlantic	USD 10 million	• Failure to maintain an AML Program • Failure to detect, identify and report suspicious transactions

810. In addition to the formal action procedures described above, the federal banking agencies are able to take "informal action" with respect to more technical violations of the AML requirements. These typically might involve agreements between the regulators and the institutions that certain measures will be taken to address deficiencies within a defined period. According to data collated for a recent GAO study, in fiscal year 2005, over 2,000 such informal actions were taken.

Securities sector—SEC, CFTC and the SROs

811. The SEC may investigate and impose its full range of sanctions against any person that violates the federal securities laws (15 USC 78u, 15 USC 78u-2, and 15 USC 78u-3). In addition, the SROs may suspend or otherwise sanction members (and their associated persons) that fail to comply with the federal securities laws or the SRO's own rules. AML-related infractions of the BSA or the rules promulgated under the BSA may constitute violations of the federal securities laws, and accordingly could serve as a basis for SEC- or SRO-initiated enforcement actions (17 CFR 240.17a-8 and 17 CFR 270.38a-1). Securities Exchange Act Rule 17a-8 requires all securities broker-dealers to comply with the reporting, recordkeeping and record retention requirements of regulations adopted under the BSA. The SEC could assess a civil money penalty against, or otherwise sanction, a securities broker-dealer that fails to comply with those requirements. Similarly, Investment Company Act Rule 38a-1 requires all mutual funds to adopt and implement policies and procedures reasonably

designed to prevent violation of the federal securities laws, including applicable provisions of the BSA. Under this rule, mutual funds must also designate a chief compliance officer to be responsible for administering the fund's policies and procedures. The SEC could assess a civil monetary penalty against, or otherwise sanction, a mutual fund for failure to comply with those provisions.

812. Enforcement remedies available to the SEC include (1) cease and desist orders; (2) injunctions obtained by court order; (3) censures or suspensions or bars from the securities industry; (4) agreements with regulated entities to undertake specific activities to correct deficient behavior; and (5) the assessment of civil monetary penalties. Separate from enforcement action, the SEC may issue deficiency letters under its examination program, and the SROs may also take formal enforcement actions against their members or may pursue informal remedies. NASD issues Letters of Caution and holds Compliance Conferences and the NYSE issues Letters of Admonition. The SEC and SROs also inform registered entities to take corrective action to address weaknesses in their AML Programs. Securities broker-dealers and mutual funds are required to demonstrate that the issues raised in the deficiency letters have been addressed. The SEC and SROs generally hold exit conferences with registered entities at the conclusion of an on-site examination to discuss their initial concerns.

813. Under Section 15(b)(4) of the Exchange Act, the SEC may censure, suspend, or revoke the license of a securities broker-dealer that fails to reasonably supervise a person subject to his supervision in this manner. In addition, under SRO rules, securities broker-dealers must adopt and implement written policies and procedures reasonably designed to prevent violation of the federal securities laws and designate a chief compliance officer to be responsible for administering the policies and procedures. Securities broker-dealers' supervisory personnel may be sanctioned for failure to supervise subordinates.

814. The NFA has the authority to file disciplinary complaints against futures commission merchants and/or introducing brokers in commodities that are found to have BSA deficiencies. Such action is taken in consultation with the CFTC, with which it also holds quarterly meetings (sometimes involving law enforcement) to discuss experience with the examinations. In its role as an oversight authority, the CFTC conducts rule enforcement reviews of NFA, and would take action against NFA if it were inadequately enforcing future commission merchant and IB compliance with their AML obligations.

815. In addition, the CFTC may take direct enforcement action against future commission merchants and/or introducing brokers in commodities for failure to comply with the CFTC's rules including its rule requiring firms to comply with their BSA obligations (17 CFR 42.2). The CFTC has broad sanction authority, including the imposition of civil monetary penalties, for violations of CFTC rules.

816. In 2005 (through September), the NASD identified 710 cases of AML deficiencies in the 1,676 AML examinations that it undertook of broker-dealers. Of these, 100 were referred to the enforcement division, resulting in 74 enforcement actions. Generally, these enforcement actions were brought against smaller firms with a limited risk profile. For example, most of these firms had few clients, few registered representatives, and no branches. The firms engaged in application-way mutual fund sales, non-ERISA retirement account transactions and other similar types of business at lower risk for money laundering. The firms that engaged in a general securities business did not execute large numbers of trades per month. From the 173 AML examinations undertaken in the same period by the NYSE, 50 found cases of deficiencies, with nine resulting in formal enforcement action. In the mutual funds sector, the SEC undertook 136 AML reviews, leading to 23 adverse findings.

817. As a result of the 365 direct examinations of futures commission merchants and introducing brokers in commodities that were conducted in 2003, the NFA issued 238 audit reports, 54 of which identified AML deficiencies by nine futures commission merchants and 39 introducing brokers in commodities. The reports cited deficiencies that included failure to have adequate AML procedures in place, failure to follow AML procedures, and failure to have senior management approve the AML procedures. But the primary deficiencies cited were failures to comply with the annual audit and training requirements. NFA usually communicates deficiencies to a firm during the audit process,

thereby providing the firm the opportunity to correct the deficiency. Deficiencies that are not resolved may result in the filing of a disciplinary complaint. The deficiency reports issued during 2003 have resulted in filing of two NFA disciplinary complaints against IBs that included charges of AML violations indicative of a firm's overall failure to supervise as prescribed by NFA rules.

818. Since 2002, the NYSE has examined all of its members at least once for compliance with AML/CFT obligations. In that time, seven disciplinary actions have been taken and an additional 22 are pending. Most of these related to failure to detect suspicious activity, file SARs in a timely manner or conduct continuing education programs. As part of an examination, the NYSE may conduct random transaction testing in relation to SAR filings and hits on the OFAC list. The NYSE conducted 484 examinations overall between 1 October 2004 and 31 October 2005, of which 173 had an AML component. Of these, 50 examinations identified AML/CFT deficiencies, mostly in relation to implementation of AML Programs. Five of these were referred to a formal disciplinary group.

819. Overall, for the securities sector, implementation of AML/CFT requirements is still in the early days. For instance, although some firms have been found to have uncured BSA violations, the CFTC has deferred to SRO enforcement and has not yet had cause to take direct action beyond that taken by the SRO.

Money Services Business sector (including money remitters and foreign exchange)

820. Sanctions in the MSB sector (including money remitters and foreign exchange) are discussed in section 3.11 of this report.

Insurance sector—FinCEN and the IRS

821. Each state insurance regulator has the power to supervise and sanction its respective insurance sector for safety and soundness in the interest of the insuring public but does not monitor life insurers transacting covered life insurance products for AML compliance.

822. Although FinCEN has delegated examination authority for BSA compliance to the IRS, it has retained the enforcement powers under the BSA. The measures available to FinCEN are described above. Since the effective date of the insurance AML rule is 2 May 2006, FinCEN has not yet exercised its sanction powers against insurers.

Guidance for financial institutions (other than on SARs)

FinCEN

823. FinCEN, in conjunction with the federal financial regulators, provides various types of guidance to domestic financial institutions in complying with AML/CFT requirements. All such guidance is posted on FinCEN's website. FinCEN's guidance materials include the following:

(a) letter rulings explaining those BSA requirements that apply to specific facts and circumstances;

(b) answers to frequently asked questions about BSA requirements; and

(c) advisories and bulletins on: (1) specific ML/FT schemes; (2) jurisdictions with seriously deficient AML/CFT regimes; and (3) institutions or individuals who may be engaged in fraudulent activities or be deemed to be of a high ML/FT risk.

824. FinCEN also maintains a separate website specifically dedicated to providing guidance to MSBs. The website contains interactive guides for assisting a business in determining whether it is a covered financial institution, answers to frequently asked questions about requirements applicable to MSBs, reference guides that have been specifically prepared to educate MSBs on their responsibilities under the BSA generally and SARs specifically, and links to Issue 4 of FinCEN's SAR Bulletin, a publication that provides information on detecting financial transactions indicative of terrorist funding.

825. In addition to creating a special website to provide guidance to MSBs, FinCEN hired a contractor to prepare guidance materials for MSBs. These free materials include guidance pamphlets, training videos and CD-ROMs, and materials that MSBs can display in their place of business, or provide to their customers, to explain why MSBs are required to obtain customer identification with respect to certain transactions. Posters are available in several foreign languages including Spanish, Arabic, Chinese, Korean, Spanish and Vietnamese, and FinCEN is implementing plans to translate existing guidance materials into a number of other languages.

826. In order to better ensure that money services businesses continue to operate within the regulated financial sector, on 26 April 2005, FinCEN and the Federal Banking Agencies issued "Interagency Guidance on Providing Banking Services to Money Services Businesses Operating in the U.S." The guidance outlines with specificity BSA compliance expectations when banks open and maintain accounts for money services businesses. FinCEN also issued a concurrent "Advisory to Money Services Businesses on Obtaining and Maintaining Banking Services" to emphasize the BSA obligations of money services businesses and to notify those businesses of the types of information they would be expected to provide to a banking organization in the course of opening or maintaining account relationships. This guidance and future advisories may be obtained from FinCEN's web site.

Federal Banking Agencies

827. The FFIEC Manual, published in June 2005, provides comprehensive guidance to the banking sector. Following its publication, conference calls were held by the FDIC, FRB, OCC, and OTS to provide an introduction and overview of the FFIEC Manual for the banking industry. Approximately 8,200 persons participated in these calls. Additionally, the FDIC, FRB, OCC, and the OTS conducted regional banker outreach and examiner training events in five large metropolitan cities in which approximately 2,800 individuals attended. One outreach event was broadcast via the Internet, and approximately 12,400 people viewed this broadcast. FinCEN and OFAC participated in all these events.

828. Outreach programs are also in place, whereby the Federal Banking Agencies, in partnership with FinCEN, conduct symposiums for banking industry representatives to discuss current issues, trends, regulatory requirements, challenges, and coordination with law enforcement. On a day-to-day basis, the Federal Banking Agencies provide interpretive guidance to banking organizations subject to their supervision regarding AML regulations through formal and informal methods. This is promulgated through Supervision and Regulation (SR) letters, bulletins, advisories and other forms of notification, all of which are readily accessible on the agency websites.

Securities regulators and SROs

829. The SEC and, with respect to securities broker-dealers, the SROs provide various types of guidance and feedback to assist securities broker-dealers and mutual funds in implementing and complying with their AML/CFT obligations.

830. The SEC has issued letters to industry representatives (called no action letters) advising them of certain aspects of BSA regulations. The SEC maintains a webpage specifically dedicated to providing guidance to regulated firms' about their anti-money laundering obligations. It has also published guidance, often jointly with Treasury, and has prepared a webcast together with a Securities Industry Association informing securities broker-dealers of their anti-money laundering obligations and the SEC's AML/CFT exam process. Among other things, the guidance has addressed specific questions and answers relating to the customer identification program.

831. SROs provide guidance to their members by issuing Notices to Members (NASD) or Information Memos (NYSE). For example, NASD has issued several Notices to Members on AML obligations, including Special Notice to Members 02-21 (Anti-Money Laundering: NASD Provides Guidance to Member Firms Concerning Anti-Money Laundering Programs Required by Federal Law), Notice to Members 02-47 (Treasury Issues Final Suspicious Activity Reporting Rule for

Broker/Dealers) and Notice to Members 03-34 (Treasury and SEC Issue Final Rule Regarding Customer Identification Programs for Broker/Dealers). More recently, in February 2006, NYSE issued NYSE Information Memo 06-04 and NASD issued NtM 06-07 discussing recent changes to their respective AML program rules. These Notices to Members advised members about their obligation to adopt and implement an AML Program, suspicious activity reporting, customer identification requirements, and about members' other AML/CFT obligations. NASD has also published a comparison of the differing legal obligations for customer identification and record-keeping between the BSA and the SEC rules. In order to assist, specifically, the smaller firms within its membership, NASD has developed a "small firms template", which provides a model for the written policy for an AML Program. NASD also created a web-page dedicated to providing securities firms with AML information and guidance. NASD has also created an AML web cast (AML: Do You Know Your Customer?) and several on-line AML training courses that are available to member firms to assist in training and educating their associated persons. Approximately 90,000 persons have taken NASD's on-line AML courses.

832. The CFTC and NFA have adopted a multi-level approach to educate futures commission merchants and introducing brokers in commodities regarding their AML obligations. For example, the CFTC maintains a webpage outlining the AML responsibilities of its financial institutions. The CFTC has published guidance, often jointly with Treasury, advising futures commission merchants and introducing brokers in commodities with respect to specific AML compliance issues (e.g. on the CIP). Both CFTC and NFA also seek to educate futures commission merchants and introducing brokers in commodities through participation in futures industry seminars, conferences, training sessions and conference calls.

Insurance regulators and industry bodies

833. FinCEN has initiated outreach initiatives with insurance trade associations to provide guidance to the sector before and after 2 May 2006, the effective date of the regulations. In addition, The following are some of the initiatives of the NAIC in preparing the insurance sector for its AML obligations:

(a) established an Ad Hoc (Government Affairs Executive Committee) Task Force on the USA PATRIOT Act with the objective to consider policy issues, develop and coordinate appropriate examination standards, and coordinate with state and federal regulators regarding the USA PATRIOT Act AML amendments to the BSA;

(b) invited FinCEN to present its rules on AML Program and SAR requirement at the NAIC Winter 2005 National Meeting in Chicago on 5 December 2005 that was attended by insurance supervisors from various states and jurisdictions; and

(c) published FinCEN's "AML Program and SAR Requirements for Insurance Companies" FAQ in the NAIC website to assist insurers in understanding the scope of the final rules.

834. During the on-site visit, the American Council of Life Insurers (ACLI) informed that it has established a working group to create a uniform template to integrate agents, including certification that the agents subscribe to a certain company's training focus on core AML policies and procedures for gathering the same kind of information required by the authorities that every agent needs to know. Training for agents will identify areas that are vulnerable to money laundering, and establish procedures and guidance to agents to forward the relevant information to their insurers, which will relay the information to the authorities. The Life Insurance Management Resources Association (LIMRA) has AML training for agents that includes the processes that will certify that the agents have completed their AML training.

ICE Cornerstone initiative

835. The mission of the ICE's Cornerstone initiative is to develop private sector partnerships with industries involved in financial, trade, transportation and immigration-related areas and to identify and

eliminate vulnerabilities in the systems that are subject to exploitation by criminal and terrorist organizations. ICE alerts industry partners to "red flag" items that indicate a vulnerability within a particular industry and provides training for industry on the same. ICE maintains over 100 specially trained Cornerstone field liaisons throughout the U.S. Additionally, the Cornerstone program publishes a quarterly report that highlights significant investigations, "red flags", and other useful information for the private sector. It also maintains a website for the public to visit, which contains useful information and guidance. Cornerstone also produces the "The Cornerstone Report", a quarterly newsletter provided to the financial, manufacturing, and trade sectors to address emerging trends, patterns, and typologies in the money laundering arena.

3.10.2 Recommendations and Comments

836. The U.S. regulatory framework for the banking sector is complex, but overall there are considerable resources applied to the task, undertaken by well-trained examiners in a number of federal agencies, usually working in cooperation with state agencies. The legal authority of the regulators to conduct examinations, to acquire information and to conduct enforcement proceedings against financial institutions and their employees for AML compliance failures is broad, and there is clear evidence that these powers are used extensively and on a regular basis. The publication, in June 2005, of the FFIEC Manual seems to have been a watershed in the understanding between the regulators and the banks as to the latter's expectations of what constitutes an effective AML regime, and this move can be expected to help improve the levels of compliance considerably. On the basis of the response in the banking industry to this document, it is strongly recommended that additional guidance be issued to the securities and insurance sectors. The SEC, NYSE, and NASD have advised that they have reached out to the securities sector to identify areas of BSA compliance where further guidance would be helpful.

837. There are, however, two areas of potential concern. The first relates to the approximately 400 uninsured state-chartered banks and other depository institutions which are currently not subject to AML Program requirements. FinCEN intends to amend its regulations to eliminate this regulatory anomaly to bring uniformity to the banking sector.

838. The second issue relates to resources. The delegation of responsibilities to the IRS to conduct BSA examinations of the privately insured, state-chartered credit unions gives that agency a critical task for which it does not appear to have the appropriate resources. This comment is made in the context of the extensive responsibilities that the IRS has also been given to conduct oversight of the MSB and the non-financial businesses. This indicates that their resources will be pressed extremely thinly, although IRS-SBSE is in the process of hiring an additional 90 examiners. Nevertheless, it is recommended that consideration be given to providing more and better resources to examining AML compliance in the privately insured credit union sector.

839. IRS-SBSE representatives have met with FinCEN, the SEC, and the Federal Banking Agencies to discuss the overlapping jurisdiction and the need for consistency. FinCEN has issued a tentative listing of insurance companies impacted by the regulation that fall under IRS-SBSE jurisdiction. IRS-SBSE is working with FinCEN to develop an implementation and examination strategy. A basic outline of draft examination procedures has been developed; these procedures parallel established guidelines issued by the FFIEC.

840. The sanctions regime in the U.S. is wide-ranging in terms of the options available, and the penalties are applied without reticence and the general implementation appears to be effective. This is clearly acting as an incentive to institutions to implement effective AML/CFT procedures. Institutions that have been found to be deficient have faced severe financial penalties. However, the scope of the AML/CFT requirements does not yet address all of the sectors in the financial industry that have been determined to pose a lower risk of money laundering. With respect to the insurance industry, its enhanced obligations did not come into force until May and, therefore, the sanctions regime for the new

measures only recently came into force and cannot yet be measured for effectiveness. In addition, the investment advisers and commodity trading advisers currently have no AML Program obligations and, therefore, the broader sanctions currently do not apply to them, although those sectors have been considered by the U.S. to pose a lower risk of money laundering than other sectors to which BSA AML/CFT obligations have been applied. There are also concerns about the availability of resources within the IRS to undertake comprehensive examinations of the large number of institutions for which it is responsible. This may have an effect upon the degree to which these sectors are properly sanctioned for AML/CFT compliance, particularly in view of the wide perception among U.S. law enforcement agencies that the MSB sector has a high level of non-compliance (see the discussion in section 3.11).

841. The U.S. has extended considerable efforts towards providing guidance to the financial sector and there are clear signs that it will continue to do so as and when new institutions are brought within the AML/CFT framework.

3.10.3 Compliance with Recommendations 23, 29, 17 & 25

	Rating	Summary of factors relevant to s.3.10 underlying overall rating
R.17	LC	• Some banking and securities participants are not subject to all AML/CFT requirements and related sanctions at the federal level. • The effectiveness of the measures in the insurance sector can not yet be assessed. • There are concerns about how effectively sanctions are applied in the MSB sector given the current level of the IRS's resources.
R.23	LC	• Some securities sector participants are not subject to supervision for AML/CFT requirements. • The effectiveness of the measures in the insurance sector can not yet be assessed. • Concerns about IRS examination resources.
R.25	C	• This Recommendation is fully observed.
R.29	C	• This Recommendation is fully observed.

3.11 Money or value transfer services (SR.VI)

3.11.1 Description and Analysis

842. This section must be read in conjunction with the relevant descriptions, elsewhere in the report, of the obligations imposed on MSBs, specifically in relation to CDD, monitoring for, and filing of, SARs, and internal control procedures.

Definition of a money transmitter (money or value transfer service provider)

843. Money or value transfer services provided in the U.S. by non-bank financial institutions are included in the category of money services businesses, defined under the BSA regulations [31 CFR 103.11(uu)] as: "Each agent, agency, branch, or office within the U.S. of any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the capacities listed in paragraphs (uu)(1) through (uu)(6) of this section." The listed capacities include a currency or exchange dealer, a check casher, an issuer or seller of travelers' checks, money orders or stored value, and a money transmitter. The term "money services business" does not include a bank, nor a person registered with, and regulated or examined by, the SEC or the CFTC.

844. Money transmitters and are defined to mean:

(A) "Any person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution, a

Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both, or an electronic funds transfer network; or

(B) Any other person engaged as a business in the transfer of funds."

845. Whether a person "engages as a business" is a matter of facts and circumstances. Generally, the acceptance and transmission of funds as an integral part of the execution and settlement of a transaction other than the funds transmission itself (for example, in connection with a bona fide sale of securities or other property) will not cause a person to be a money transmitter.

846. FinCEN has adopted a broad interpretation of the BSA regulations with regard to their application to money transmitters. Also, the definition of money transmitter was amended by section 359(a) of the USA PATRIOT Act to clarify that the term includes "any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institution system." Therefore under U.S. law, all money transfer services, both formal and informal systems, are considered money services businesses (MSBs) under the law, and are subject to any BSA requirement applicable to any money transmitter, including registration as an MSB with FinCEN, the establishment of an AML Program, appropriate record keeping, and the reporting of suspicious activity.

Registration requirements

847. As of 5 April 2006, 24,884 MSBs had registered with FinCEN. As indicated in section 1 of this report, a 1997 study by Coopers & Lybrand suggested that the total number of such business in the U.S. at that time could have exceeded 200,000. This figure includes agents, which are exempted by registration due to primary MSB requirements to maintain lists of all agents with/through which they transact/conduct business, U.S. postal service offices, and MSBs that are solely seller/issuers/redeemers of stored value. Since the Coopers & Lybrand study was issued, the regulations as amended by the USA PATRIOT Act have made more comprehensive the definition of an MSB for purposes of registration, and the application as a covered institution for purposes of compliance with the BSA.

848. Authorities continue to believe that there may potentially be many MSBs that continue to be unregistered, or unlicensed in the U.S.. Identifying and tracing unregistered MSBs poses a major challenge to the authorities and their drive to bring them within the law will have significant resource implications for the regulators.

849. FinCEN Form 107, Registration of Money Services Business, requires that the registrant provide contact information, identify its owner or controlling person, provide a governmentally-issued identification number for that person, and identify the business' primary transaction account (used to provide money services). The registrant is also required to indicate if any part of the money services business is an informal value transfer system. Not all MSBs are required to register; those exempt from registration are:

(a) money services businesses that are MSBs solely because they are agents of another MSB;

(b) branches of an MSB;

(c) money services businesses that are MSBs solely because they are issuers/sellers/redeemers of stored value; and

(d) U.S. Postal Service, federal or state government agencies.

850. MSBs established after 31 December 2001 that are required to register, are required initially to register within 180 days after the date of establishment, and their registration renewal (or two-year update) is due on or before 31 December, of the second calendar year of their initial registration period.

851. A money services business is required to re-register when one or more of the following events occur:

(a) the MSB must be re-registered under state law due to change in ownership or control;

(b) more than 10% transfer of equity interest; and

(c) more than 50% increase in agents.

852. An MSB Registration List has been published by FinCEN, pursuant to FinCEN's BSA rules at 31 CFR 103.41. A registered MSB that has agents must also prepare and maintain a list of those agents (31 CFR 103.41). This list must be updated by January 1 of each year. An MSB must make its list of agents available to FinCEN, as well as other appropriate law enforcement agencies, including the IRS, upon request. Generally, the agent list must include:

(a) the name of the agent, including any trade names or doing-business-as names;

(b) the address of the agent, including street address, city, state, and ZIP code;

(c) the type of MSB services the agent provides on behalf of the MSB maintaining the list;

(d) a listing of the individual months in the 12 months preceding the date of the agent list in which the agent's gross transaction amount, for financial products or services issued by the MSB maintaining the agent list, exceeded USD 100,000;

(e) name an address of any depository institution at which the agent maintains a transaction account for any of the funds received in or for the MSB services the agent provides on behalf of the MSB maintaining the list;

(f) the year in which the agent first became an agent of the MSB; and

(g) the number of branches and sub-agents the agent has, if any.

State licensing

853. In addition to the federal registration process through FinCEN, 46 states have MSB licensing requirements, but they are not uniform. Some license only money transmitters and/or check cashers. In the Money Laundering Suppression Act of 1994, the U.S. Congress recommended that the States enact uniform laws to regulate MSBs. In response, the National Conference of Commissioners on Uniform State Laws (NCCUSL) has promulgated a model law regulating MSBs, which it recommended that all States enact. However, this has not been universally adopted, and MSBs reported that, when they operate across state lines, some of the legal requirements conflict between states.

854. Title 18 USC 1960 makes it a federal offense to operate a money transmitting business in the absence of compliance with any applicable state licensing requirements or failure to register as a MSB with FinCEN or to transport or transmit funds that are known to the defendant to have been derived from a criminal offense or intended to be used to promote or support unlawful activity. The USA PATRIOT Act specifically provides that a conviction for failure to comply with a state licensing requirement does not require proof that the defendant knew of the state licensing requirement. Prior to its amendment, this section had only applied to money transmitting businesses intentionally operating without an appropriate state license. The penalty for knowingly conducting, controlling, managing, supervising, directing or owning all or part of an unlicensed money transmitting business is a fine or five years imprisonment [18 USC 1960(a)].

Regulatory Framework

Internal Revenue Service

855. The IRS is integrated into the National Money Laundering Strategy. Due to the IRS' separate budget from Congress, it remains autonomous from undue influence from the DOJ and from Treasury.

This permits the IRS to allocate resources to assist in implementing the AML/CFT laws within the scope of its primary mission to administer the U.S. tax laws. In terms of AML compliance, the IRS has been delegated a responsibility for examining those institutions that do not otherwise have a federal financial regulator, including MSBs. To assist in this goal, the IRS has assigned responsibilities to two of its five compliance divisions:

(a) **Small Business and Self Employed (IRS-SBSE):** The IRS-SBSE is responsible for ensuring that MSBs register with FinCEN, and for conducting compliance examinations – including for AML/CFT – of MSBs, insurance companies, non-federally regulated credit unions, and credit card operators, as well as casinos, card clubs and jewelers in the non-financial sector. It is also responsible for inspections of any trade or business that has an obligation to file CTRs (Form 8300). The BSA function of the IRS-SBSE now forms a standalone structure within the IRS-SBSE division, which has a total of 315 examiners in the field. A full description of these IRS resources is in Section 7 of this report.

(b) **Criminal Investigation (IRS-CI):** The IRS-CI is responsible for investigating possible criminal violations of the money laundering laws, the BSA, and terrorist financing laws, (including violations of the BSA by MSBs). These investigations can be initiated from referrals. The authorities mentioned that approximately 50% of their 4,000 investigations each year are devoted to proceeds of criminal activities.

856. IRS examinations include a review of the examined entity's policies, procedures, books and records, and sample testing of relevant currency transactions to ensure a form has been correctly filed. IRS has two methods to compel the production of records—the administrative summons (which is not predicated upon a court order) or the grand jury subpoena (which can only be issued during the course of a criminal investigation). IRS is able to issue the administrative summons itself, and the grand jury subpoena is obtained from the prosecuting U.S. Attorney's Office.

857. The IRS-SBSE examines both the corporate headquarters of MSBs and their agents which, according to the BSA, are MSBs in their own right. The IRS completed 3,712 BSA examinations in Fiscal Year 2005 and will undertake approximately 6,400 BSA compliance examinations in FY 2006 across the range of businesses for which it is responsible, including MSBs. In addition, for FY 2006, it plans to conduct approximately 2,600 examinations for Form 8300 compliance. In FY 2005, 2,366 Form 8300 examinations were completed. Unlike the federal banking and securities regulators, the IRS is not obligated to undertake examinations on any particular cycle. Its program is largely determined on a risk basis and by the relative size of the institutions for which it is responsible. Large MSBs are examined as a matter of course with the IRS performing a centralized examination of the MSBs corporate headquarters. Smaller MSBs are targeted for an audit if they have been identified as high risk, including for terrorist financing, as determined by leads from other federal or state agencies and their SAR filing history. The IRS-SBSE reports that, given their limited resources, they must rely on a risk-based approach when formulating their examination schedule. Work is underway to refine the risk assessment process.

Regulators

858. The primary federal regulator for MSBs is the IRS. To date, 35 states have signed MOUs with the IRS-SBSE for information sharing. The primary purpose of these MOUs is to enhance interagency cooperation in BSA matters They are also intended to foster the flow of information between the IRS-SBSE and the states in a manner that avoids undue regulatory duplication, conserves regulatory resources, and better ensures consistency in the application of the regulatory provisions of BSA. The scope of activities covered by these MOUs includes:

- sharing BSA and AML examination information, including upcoming examination schedules;
- sharing lists of MSBs and other Non-Bank Financial Institutions (NBFIs) and providing access to certain information maintained on the State Regulator databases;

- sharing MSB and other NBFI information available from the State Regulator, including, but not limited to, the status of licenses or charters granted by the State Regulator to MSBs and other NBFIs;
- training and orientation of IRS examiners and examiners for the state regulator; and
- sharing Program Documents such as examination manuals and policy directives.

859. Although most states have licensing requirements, seven states do not regulate MSBs at all and the statutes of nine states prevent them from entering into a MOU (Alaska, Arkansas, Colorado, Hawaii, Iowa, Montana, South Carolina, New Hampshire, and New Mexico). Even where licensing requirements exist, only about 12 states conduct onsite examinations (including California, Florida, Maryland, New York, Ohio, Pennsylvania and Texas). Where this occurs, it is not uncommon for the regulators to look at BSA compliance, as well as state requirements, since the state legislation normally requires compliance with federal law as a condition of licensing. Where MSBs operate across several states they will be subject to multiple examinations by individual state regulators. Typically, this takes place at headquarters level, irrespective of the state in which it is physically located, and larger MSBs have reported having 6 to 10 separate examinations by different state authorities in any one year, all using different methodologies. The MTRA has established a committee to consider formulating standardized examination procedures, but it is understood that several states are reluctant to move away from their existing procedures.

860. In the case of those states that license MSBs but do not examine as a matter of routine, the regulatory response is triggered only as a response to customer complaints or other external factors. The private sector is calling for more coordination amongst state regulators; however, it will probably be another two to three years before this is fully implemented. Currently, those states that belong to the MTRA and have signed the cooperative agreement exchange examination reports, albeit on an infrequent basis except in the case of the largest MSBs. MTRA would ideally wish to move towards the concept of joint examinations.

861. From discussions with the state authorities, it appears that the level of cooperation and coordination in the examination process between the IRS and state regulators has been limited. Joint state/federal examinations do not take place. However, MOUs between FinCEN, states and IRS provide for information sharing on examination and compliance issues.

MSBs and their agents

862. While the licensing/registration process at both federal and state level applies to the MSB itself, the majority of such businesses operate through extensive networks of independent agents whose primary business is unrelated to financial services (e.g. grocery stores, gas stations, etc). The possible multiplier effect of this relationship may be illustrated by a case in Arizona where there are 56 registered MSBs with a total of 7,288 authorized agents, although Arizona may not be representative of the U.S. as a whole.

863. In most cases, there is an obligation on the MSB to require its agents to implement appropriate systems and controls, and to have effective oversight of the agents' implementation of such systems. It is not the practice to impose an independent obligation on agents. It is recognized that the level of compliance by some agents in certain geographical areas is relatively low, and that the ability/willingness of some MSBs to expend resources on ensuring compliance is limited.

864. While, in most cases the regulators have the right to conduct examinations of the agents (and in some states, such as Maryland, a limited number of on-site inspections of agents are conducted), they typically do not have any direct enforcement authority over them, since any action can only be taken against the MSBs themselves. Moreover, given the very large number of agents, the regulators cannot realistically undertake anything other than a very limited sampling of the agents. Consequently, the focus is more often on the MSB's own internal audit programs and supervision of its agents.

Applicability of the FATF Recommendations

865. The limitations identified under Recommendation 5, 8, 13 and SR.IV with respect to the MSB sector (as discussed previously in Section 3 of this report) also affect compliance with Special Recommendation VI.

Enforcement and Sanctions

866. FinCEN is responsible for bringing civil enforcement actions and assessing civil money penalties with respect to violations of the BSA regulations by MSBs. Enforcement of criminal penalties is under the jurisdiction of the DOJ.

867. Any MSB that fails to register with FinCEN (under 31 USC 5330), or files false or incomplete information in the registration statement, is subject to civil penalties of USD 5,000 per day, while the violation continues. In addition, under 18 USC 1960, any person who knowingly conducts, controls, manages, supervises, directs or owns all or part of an unlicensed money transmitting business, may be subject to criminal fines, imprisonment of not more than five years, or both. For purposes of 18 USC 1960, the term "unlicensed money transmitting business" means a money transmitting business that is operated without an appropriate state license (in a state where operation without an appropriate license is punishable as a misdemeanor or a felony under state law), whether or not the defendant knew that the operation was required to be licensed or knew that operation without such license was a criminal offense, or fails to comply with the registration requirements under the BSA, or otherwise involves the transportation or transmission of funds that are known to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity.

868. The following statistics show the cases that were prosecuted in relation to operating a money remittance business without a license.

Number of...	Fiscal year 2004
Cases	45
Defendants	68
Successful charges	40
Terminated defendant count	40
Guilty	27

869. To help identify/uncover informal value transfer systems (or alternative remittance systems), FinCEN is participating in an Interagency IVTS Working Group with other federal law enforcement and regulatory agencies. FinCEN is also working with banks and state licensing departments, analyzing Internet, printed media, and other advertising as well as SARs and CTRs that have been filed, and consulting with registered MSBs with respect to their unregistered or unlicensed competitors. As part of an awareness raising campaign, FinCEN has continued its industry training and public presentation efforts, issuance of guidance on its website, and working with the IRS-SBSE, which is responsible for examining MSBs for their compliance with BSA regulations, and with the IRS Communications, Liaison and Disclosure Division to conduct enhanced outreach efforts. FinCEN has also made the list of registered MSBs publicly available on its website. These efforts are described in greater detail below. Additionally, some states such as Maryland and New York have dedicated some resources to proactively seeking out unregistered/unlicensed money remitters; however, most states do not have such programs in place due to a lack of resources.

870. In terms of compliance with general BSA requirements (e.g. AML Program, record keeping, and reporting), the sanctions available FinCEN are as described generally in section 3.10 above. The IRS has only limited civil enforcement powers in its own right. In cases where it identifies deficiencies that are not significant, it may issue a "letter 1112" which defines the issues and provides notice of follow-up action to assess the corrective measures taken by the entity. A total of 1,368 such letters were issued

in 2005 (again for all businesses, not simply MSBs). All cases of more egregious non-compliance must be referred to FinCEN. There were nine such referrals in FY 2005. If the examiner believes the deficiencies are criminal in nature, the information is also referred to IRS-CI for possible investigation.

871. From discussions with the state regulators who examine for compliance with state law rather than BSA requirements, the sense is that the level of compliance within the MSB sector is relatively low. The weaknesses most commonly identified were a lack of skilled resources within the businesses and poor control environments. This typically leads to poor standards of customer identification and failures to file SARs and CTRs. As indicated above, the problems often lie with the agents rather than the MSBs themselves, although a lack of adequate oversight of the agents by the MSBs may be the root cause.

Outreach Efforts

872. See section 2.5 for a discussion of some of the general outreach efforts that FinCEN has taken in relation to the MSB sector. FinCEN has indicated that it will continue to improve its ability to provide information to the regulated MSB community to help identify potential terrorist financing activity, in particular, by:

(a) educating segments of the MSB industry most vulnerable to terrorist abuse, which include small businesses that typically offer money remittance services, check cashing, money orders, stored value products and other IVTS; and

(b) providing training on how terrorists have used and continue to use MSBs; the reason for and importance of the MSB registration requirement; and the importance of complying with the reporting requirements of the BSA, especially suspicious activity reporting.

873. To enhance outreach and compliance efforts with money/transfer services providers, and to balance enforcement efforts with outreach needs, an Interagency MSB Informal Value Transfer System (IVTS) Working Group was formed with the goal of identifying and locating IVTS (such as hawalas) and ascertaining MSB and alternative remittance systems (ARS) understanding of their compliance obligations and assessing the level of their compliance with the BSA. The Working Group consists of representatives from IRS-CI, IRS-SBSE, ICE, FBI, DEA, CIA and Treasury/FinCEN. To facilitate conducting targeted outreach to IVTS nationwide, FinCEN is contracting for translation of its currently existing MSB regulatory materials that explain requirements in Arabic, Hindi and Persian, among other languages.

Case study--Arizona

A disproportionate volume of wire transfers goes through the state of Arizona. Law enforcement reporting indicates that a large amount of illicit funds laundered through money transmitter services are sent to the southwest border of the U.S.—particularly southern Arizona, where USD 12 is received for every USD 1 sent. This is accounted for in bulk cash movements south of the border. There are only three sizeable licensees in Arizona that engage in received transactions. (This is in contrast to the situation in some areas, such as south Florida, New York and south Texas which have large networks of small and unauthorized MSBs.)

All MSBs doing business in the state of Arizona must register itself and a list of its agents with FinCEN. Additionally, the MSB must be licensed with the state of Arizona.

The relationship between the principal MSB (the licensee) and its agents is different in Arizona than it is in many other states. Agents have an "agent/delegate" relationship with the licensee. They are not "stand alones" and do not have to register separately with FinCEN—unless they are performing another service (other than remittance) that requires registration. (In such cases, the registration of the licensee will not cover that activity and the agent/delegate will have to register separately.) Likewise, the agent/delegate does not have to comply with state licensing requirements. The

licensee remains liable for all of the activities of its agent/delegates. Consequently, enforcement actions are taken against the licensee (not against the agent/delegate directly).

At the state level, Arizona has a USD 1,000 threshold for reporting and recording transactions. Additionally, MSBs operating in Arizona must comply with the federal reporting and recording requirements which apply to transactions above the USD 3,000 threshold.

MSBs are supervised the federal level (by the IRS) and at the state level (by the State of Arizona Department of Financial Institutions). A licensee may be subject to license responsibility if there is a pattern of negligent supervision or may lose its license in the case of a widespread pattern of abuse. Additionally, there is close cooperation between law enforcement agencies and the private sector.

At the law enforcement level, Arizona has focused on identifying and stopping wire transfers of proceeds through the state. The Arizona Task Force (ARS) (which was created in 2001) is an independent task force that monitors wire transfers through MSBs (including transfers that fall well below the state reporting threshold of USD 1,000). The ARS proactively analyzes this information with a view to identifying and stopping the movement of proceeds of crime. The Arizona authorities have a wide range of tools that facilitate stopping such flows, including geographic targeting orders (GTO) and sweep warrants. This work has resulted in seizures of about USD 16 million and hundreds of arrests. The ARS reports that recently, as a result of these efforts, the number of wire transfers of wire transfers being sent through Arizona has been decreasing and the number being sent through neighboring states been increasing accordingly. The ARS is working to take its model and share it with other states in the country, particularly with neighboring states such as California, New Mexico and Texas.

3.11.2 Recommendations and Comments

874. The U.S. has introduced a federal registration system which also includes a requirement to maintain a list of agents for each registered MSB. It has also introduced a regulatory and oversight system. However, the size of the MSB sector poses a major challenge to the authorities in implementing an effective oversight system and, although the IRS is seeking to take up the challenges, its resources seem wholly inadequate. The current registered sector exceeds 24,000 businesses with an extremely large number of agents and the authorities recognize that there is probably an even greater number of MSBs that remain unregistered – making registration and subsequent assessments for compliance a key issue. To tackle this overall issue, the IRS has approximately 315 examiners in the field, although it is currently in the process of hiring another 90 examiners. Moreover, these examiners have responsibility for examining compliance in numerous other sectors. The IRS has adopted a risk-based approach to examination, but recognizes that there will be a very significant number of MSBs that may not be examined at all in the foreseeable future. This situation could, in part, be alleviated by greater coordination between the IRS and the state authorities that license and examine MSBs and the U.S. authorities are strongly recommended to pursue this line as a matter of urgency. However, this alone would not resolve the problem, and the steps below highlight the enhanced coordination efforts the IRS has been undertaking to specifically address this issue. Associated with this, it is recommended that further efforts are made to standardize the AML examination procedures both between the states, and between the individual states and the IRS.

875. It is recommended that a thorough review be undertaken of the workload and resources of the IRS in the area of BSA compliance to ensure that the allocation of responsibilities is delivering the most effective and efficient results (i.e. are other agencies better placed to take on some of these responsibilities?). Irrespective of any reallocation of responsibilities, it is clearly the case that the IRS needs to be allocated significantly more resources simply to address the MSB sector. This is particularly important since there is common acknowledgement that a major problem of compliance exists among MSB agents which are currently only examined on a sample basis albeit using a risk-

based approach. The problem is partly due to a failure by the operators to exercise effective oversight over the agents. If the system of regulatory oversight is to be effective, it seems necessary to extend the examination program for agents quite extensively.

3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	LC	• The limitations identified under Recommendation 5, 8, 13 and SR.IV with respect to the MSB sector also affect compliance with Special Recommendation VI. • Major concerns with respect to resources of the IRS for monitoring of this sector.

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

876. Since the enactment of the USA PATRIOT Act in October 2001, but in some cases even prior to that point, some of the entities defined as DNFBPs by the FATF have been subject to some of the requirements of the BSA. As a result, Treasury and FinCEN have promulgated regulations that impose certain of the reporting, recordkeeping, and/or AML Program requirements of the BSA on these entities.

Scope of application of the BSA obligations in the DNFBP sectors

877. The current position of each of the DNFBP under the BSA is addressed below. With the exception of the casino sector (which files CTRs), all of the following DNFBPs have a responsibility to file Form 8300 as a minimum requirement under the BSA. See section 3.7 of this report for a description of CTR and Form 8300 filing requirements respectively.

Accountants

878. Accountants in the U.S. are not defined as "financial institutions" under the BSA, and accordingly they are not currently subject to most of the AML requirements under the BSA (other than the obligation to file Form 8300s). Since accountants have access to companies' operations and financial records, there have been discussions in Congress on how existing accounting standards can incorporate AML safeguards. During the first on-site visit, the team was informed that accountants in one state have met with the government authorities to discuss and prepare for any possible additional BSA obligations.

Casinos

879. The BSA defines a "casino" as being a gaming establishment with a gross annual revenue that exceeds USD 1 million. Casinos (as defined in the BSA) are subject to the following BSA requirements: suspicious transaction reporting (31 CFR 103.21); reporting of transactions in currency [31 CFR 103.22(b)(2) and (c)(3)]; record keeping (31 CFR 103.36); and establishing AML Programs (i.e. internal controls) [31 CFR 103.64(a) and 120(d)]. Gaming establishments with a gross annual revenue of USD 1 million or less do not fall within the BSA's definition of "casino" and are, therefore, not subject to these requirements.

880. Financial services available at casinos are similar and, in some cases, identical to those generally provided by banks and other depository institutions and by other financial services providers (check cashers, money transmitters, issuers, sellers and redeemers of money orders and traveler's checks, and currency dealers and exchangers) and can include customer deposit or credit accounts, facilities for transmitting and receiving funds transfers directly from other institutions, and check cashing and currency exchange services. Because of this, state-licensed gambling casinos whose gross annual gaming revenues exceeded USD 1 million were generally made subject to the BSA by

regulation in 1985 [50 FR 5069 (6 February 1985)]. The Money Laundering Suppression Act[76] explicitly added casinos (both state-licensed and tribal), or other gaming establishments (e.g., card clubs), to the list of financial institutions specified in the BSA statute. In the case of state-licensed casinos, the applicable state legislation contains, in some cases, requirements that are substantially similar to those encompassed in the BSA and its regulations.

881. Gambling casinos authorized to do business under the Indian Gaming Regulatory Act became subject to the BSA, by statutory amendment in 1994 and by regulation in 1996 [61 FR 7054 – 7056 (23 February 1996)], and the class of gaming establishments known as "card clubs" became subject to the BSA by regulation in 1998 [63 FR 1919 - 1924 (13 January 1998)]. Thus, the BSA requirement applies to state-licensed casinos (both land-based and riverboat), tribal casinos and state-licensed and tribal card clubs.

882. Although casinos conduct many financial transactions at their cage operations, they may contract out certain services. For example, many tribal casinos in the U.S. typically contract out their check cashing to third party check cashing operators. These casinos lease space within the facilities to these check cashing operators. If these operators cash checks totaling more than USD 1 000 for one person in any one day [31 CFR 103.11(uu)(2)] they are deemed to be an MSB and must comply with MSB requirements such as 31 CFR 103.22(b)(1), 103.38, 103.41, and 103.125. Similarly, many large to mid-size casinos offer wire transfer services to customers and typically contract out to private agents of MSB issuers for these services. These casinos lease space within the casinos to MSB money transfer agents of MSB issuers, and these agents operate the money transfer services. Since these private agents conduct money transfers [31 CFR 103.11(uu)(5)] they must comply with the same MSB requirements, as well as the SAR requirement in 31 CFR 103.20 .

883. The U.S. prohibits internet gaming or operating an internet casino in the U.S. This includes using the telephone or telecommunications to conduct an illegal gambling business [18 USC 1084].

Dealers in precious metals and stones

884. Although a dealer in "precious metals, stones, or jewels" has long been defined as a financial institution under the BSA, FinCEN had not previously defined the term or issued regulations regarding the dealers. On 29 April 2002 (four days after section 352 of the USA PATRIOT Act came into force), FinCEN deferred the AML Program requirement contained in 31 USC 5318 (h) that would have applied to dealers. The deferral was to allow FinCEN time to study the industry and to consider how AML controls could be best applied to them.

885. The U.S. reviewed, analyzed and discussed (with input from both industry representatives and law enforcement) the extent to which the industry may be used by money launderers or terrorist financiers, and assessed the money laundering risks posed by the business, and the overall risks posed by the business. Although these dealers do not perform the same functions as depository institutions, the review concluded that this industry presents identifiable money laundering risks. Precious metals, stones or jewels are easily transportable, highly concentrated forms of wealth and can be highly attractive to money launderers and other criminals, including those involved in the financing of terrorism.

886. FinCEN has issued an interim final rule requiring certain dealers in precious metals, stones, or jewels to establish an AML Program pursuant to the provisions of section 352 of the USA PATRIOT Act of 2001 [70 FR 33702 (9 June 2005)]. The rule was issued as an interim final rule because FinCEN is seeking additional public comment regarding issues such as whether silver should be removed from the definition of the term, "precious metal," whether "precious stones" and "jewels" should be defined more specifically, for example, by reference to a minimum price per carat, etc. FinCEN has received comments on these issues but indicated that these comments would not result in

[76] Title IV of the Riegle Community Development and Regulatory Improvement Act of 1994 – Pub. L 103-325.

any major changes to the rule. However, the rule became effective 1 January 2006 and the requirements are now in place.

Lawyers

887. Lawyers and other legal professionals in the U.S. are not defined as "financial institutions" under the BSA and are not currently subject to most of the AML requirements under the BSA (other than the obligation to file Form 8300s). Representatives of the American Bar Association (ABA) Task Force on Gatekeeper Regulation and the Profession (ABA Gatekeeper Task Force) stated that the ABA has no objection in principle to the application of certain AML requirements on lawyers, as long as they do not conflict with established ethics requirements and the attorney-client privilege. The ABA represents more than 400,000 lawyers in the United States. FinCEN is reviewing the status of attorneys under the BSA,[77] particularly with respect to their involvement in certain real estate transactions and corporate formation capacities.

Real Estate Agents

888. Although the BSA defines "persons involved in real estate closings and settlements" as a type of financial institution, for which the Treasury should consider applying AML and other BSA requirements, the U.S. has not yet adopted a final rule relating to such persons. The U.S. recognizes that the real estate industry and persons involved in the industry could be vulnerable to money laundering and other financial crime because of the high value of the product. In light of these potential vulnerabilities, FinCEN issued an advance notice of proposed rulemaking (ANPRM) in April 2003 to solicit public comments on four main questions: (1i) what are the money laundering risks in this sector; (2) how should "persons involved in real estate closings and settlements" be defined; (3) should there be any exemptions for any category of persons; and (4) how should the AML Program requirement be structured. In terms of the definition, the NPRM recognizes that the term is undefined in the BSA itself, and that, in principle, it could encompass a range of participants well beyond the real estate agent. Nothing further has been published by FinCEN on this sector following the NPRM.

Trust and company service providers

889. Trust companies that are authorized to act in a fiduciary capacity are defined as financial institutions under the BSA. They are chartered and regulated at either federal or state level, on a basis similar to that for banks, and are mostly subject to the same AML requirements (see section 3). The business of acting as an agent in the formation and administration of companies is not similarly defined, and so such businesses are not currently subject to AML requirements. In its most recent threat assessment (January 2006), the U.S. identified the formation of shell companies within certain states as a serious cause for concern. However, to date no proposals have been published with respect to bringing the company formation agents within the AML framework. For ease of reference throughout this section, unless otherwise specified, the term TCSP is used only to refer to the activities of trust and company service providers where that activity is not carried out by a licensed trust company.

[77]Also, the ABA Section of International Law and Practice, Ad Hoc Task Force on Professional Responsibilities Regarding Money Laundering, and the ABA Gatekeeper Task Force have been established to monitor the issue of imposing an AML regime on lawyers

4.1 Customer due diligence and record-keeping (R.12)

(Applying R.5, 6 & 8-11)

4.1.1 Description and Analysis

Applying R.5 (Customer identification)

Casinos

890. The customer identification obligations described below are triggered when a customer conducts a financial transaction in a casino.

891. The BSA does not permit casinos to keep anonymous accounts or accounts in fictitious names involving deposits and credits. There is no systematic identification of customers who enter casinos in the U.S. However, casinos are required to collect and verify customer identification information when there is:

(a) a deposit of funds, account opened or line of credit extended. In such cases, the name, permanent address and social security number of the person involved (or a passport number, in the case of a non-resident alien), as well as similar information for other persons having a financial interest in the account, regardless of residency must be obtained and verified [31 CFR 103.36(a)];

(b) a transaction for or through a customer's deposit or credit account [31 CFR 103.36(b)(1)];

(c) an extension of credit in excess of USD 2,500 [31 CFR 103.36(b)(4)];

(d) an advice, request or instruction with respect to a transaction involving persons, accounts or places outside the U.S., regardless of residency [31 CFR 103(b)(5)];

(e) a transaction with a face value of USD 3,000 or more, including transactions involving personal checks (excluding instruments which evidence credit granted by a casino strictly for gaming, such as markers); business checks (including casino checks); official bank checks; cashier's checks; third-party checks; promissory notes; traveler's checks; or money orders conducted with a customer, regardless of whether currency is involved [31 CFR 103.36(b)(9)]; and

(f) transmittals of funds in excess of USD 3,000 [31 CFR 103.33(f) and (g)].

892. The customer identification obligations that apply to casinos require them to verify and record the customer's name, address and social security number; however, it is not deemed to be in violation of these obligations "in the event that a casino has been unable to secure the required social security number" provided that it has made reasonable efforts to obtain the number and maintains a list of the names and addresses of those persons from the number could not be obtained. This list must be available for inspection by the competent authorities upon request [31 CFR 103.36(a)].

893. Casinos do not have to obtain information on the purpose and intended nature of this business relationship unless customers are opening credit or check cashing accounts. For credit or check cashing accounts, casinos must conduct ongoing due diligence reviews of the business relationships with such customers.

894. Customer identification and verification for casinos under the BSA requires the use of reliable, independent sources, documents, data or information (identification data) for both deposit and credit accounts and for filing FinCEN Form 103, CTR by Casinos (CTRC)s. Acceptable forms of identification include a driver's license, military or military/dependent identification card, passport, alien registration card, state issued identification card, cedular card (foreign), or a combination of other documents that contain an individual's name and address and are normally acceptable by financial institutions as a means of identification when cashing checks for persons other than established customers. Reportable currency transactions include both financial transactions and gambling transactions.

895. For casino customers with accounts for credit, deposit, or check cashing, or on whom a CTRC has been filed, acceptable identification information previously obtained and maintained in the casino's internal records may be used for purposes of completing a CTRC, as long as the following conditions are met:

(a) the customer's identity is re-verified periodically;

(b) any out-of-date identifying information is updated in the internal records; and,

(c) the date of each re-verification is noted on the internal record.

> *Case study—One Arizona tribal gaming casino*
>
> In 2005, a typical Arizona tribal gaming casino filed 881 CTR-C and no SARC forms. Typically, the customer identification includes recording the client's social security number when the client's cash in/cash out transactions exceed USD 3,000 or USD 10,000 per day. "Cash in" refers to currency the casino receives from the clients (e.g. in exchange for chips or playing tokens, or when exchanging currency). "Cash out" refers to currency the casino gives to the patron for exchange of chips or other gaming instruments (like redemption of chips or other gaming instruments, payment on jackpots, cashing of negotiable instruments including casinos checks).
>
> Some CDD is undertaken if a client opens a player account (which is the case for only of 32% of the clients in the mentioned example). In such instances, the identification will be limited to the name and address. If a client does not want to open a player account, the casino will sometimes try to perform limited CDD. This may involve a casino employee asking the client to provide his/her name so that it can be written down on a invitation for a free meal. No PEP identification and no OFAC lists screening requirements had been implemented by the casinos that were visited by the assessment team.

Accountants, dealers in precious metals and stones, lawyers, real estate agents and TCSPs

896. These businesses and professions have no customer identification obligations beyond the Form 8300 reporting requirement.

Applying R.6-9 and 11 (PEPs, payment technologies, introduced business and unusual transactions)

897. No regulations have been introduced extending any of the specific obligations under Recommendations 6, 8, 9 or 11 to any category of DNFBP.

Applying R.10 (Record keeping)

Casinos

898. Casinos are required to maintain and retain the original or a copy of certain records for a period of five years, including:

(a) records of each deposit of funds, account opened or line of credit extended, including a customer's identification and the verification of that identification as well as similar information for other persons having a financial interest in the account, regardless of residency [31 CFR 103.36(a)];

(b) records showing transactions for or through each customer's deposit or credit account, including a customer's identification and the verification of that identification, regardless of residency [31 CFR 103.36(b)(1)];

(c) other records pertaining to each customer's deposit and credit accounts [31 CFR 103.36(b)(2)-(b)(3) and (b)(6)]; and

(d) records of extensions of credit in excess of USD 2,500, including a customer's identification and the verification of that identification, regardless of residency [31 CFR 103.36(b)(4)].

899. Further, casinos are required to record transactions with a face value of USD 3,000 or more, including a customer's name and address, involving personal checks (excluding instruments which evidence credit granted by a casino strictly for gaming, such as markers); business checks (including casino checks); official bank checks; cashier's checks; third-party checks; promissory notes; traveler's checks; or money orders conducted with a customer, regardless of whether currency is involved [31 CFR 103.36(b)(9)]. In addition, casinos are required to maintain records of transmittals of funds in excess of USD 3,000, verify customer identification, and provide for retrievability and reporting of this information to other financial institutions in the payment chain [31 CFR 103.33(f) and (g)].

900. For customer gambling transactions, the BSA also requires a casino to maintain and retain the original or a copy of records prepared or used to monitor a customer's gaming activity (e.g., player rating records, currency multiple transaction logs, etc.) [31 CFR 103.36(b)(8)]. However, the BSA does not define the information that must be contained in these records. Casinos maintain gambling transaction records, in the ordinary course of business as follows. Some casinos use a manual system to track customer gambling activities at the gaming tables based on physical observations by casino employees. Others use a computerized slot data system to track customer gambling activities at slot machines or video lottery terminals through the use of "membership cards" inserted into the machines. Both of these systems provide a broad estimate of the funds placed by individual players. The customer's computerized player rating account record or slot account record typically contains the customer's name, permanent address, date of birth, sometimes other identification information, as well as the player's gaming activity. In addition, the player rating system will include the amount of currency received from a customer for the purchase of chips or cash bets, chip buy-in amount, credit buy-in amount, as well as other information such as average bets, estimated win or loss, etc. The player rating system reflects all rated player cash activity recorded on player rating cards (regardless of the amount) that has occurred on the gaming floor. As a corollary, the slot data systems will include customers' coin-in/number of credits played (i.e. total play), currency placed in the bill acceptor, wins/losses, jackpot wins, electronic funds transfer (EFT/AFT) processing, ticket ins, tickets outs, etc.

901. Additionally, a casino must maintain any supporting documentation or business record equivalents with its copy of the filed SAR form for five years from the date of filing. Documentation may include canceled checks, credit bureau reports, credit slips/vouchers, deposit/withdrawal slips, multiple transaction logs, player rating records, slot club player records, identification credentials, spreadsheets, photographs, surveillance audio and/or video recording media and surveillance logs. Upon request, the casino or card club must make the SAR, along with any supporting documentation to FinCEN and any other appropriate law enforcement or supervisory agencies (including the IRS in its capacity as BSA examination authority) [31 CFR 103.21(d)].

902. The BSA regulations require in 31 CFR 103.38(d) the retention for five years of the source records (either originals or copies or reproductions of the documents) of all records required to be retained by 31 CFR Part 103 (e.g., 31 CFR 103.36 requires detailed casino and card club recordkeeping) and, if made, casino computer records, source documentation and related programs, of all the records described in 31 CFR 103.32, 103.33 and 103.36. Also, these records must be filed or stored in such a way as to be accessible within a reasonable period of time.

903. A casino that inputs, stores, or retains, in whole or in part, for any period of time, any records required to be maintained under BSA regulations at 31 CFR 103.33 or 103.36(a) and (b) on computer disk, tape, or other machine-readable media also is required to retain these records in such media. In addition, a casino is required to maintain the indexes, books, file descriptions and programs that would enable a person readily to access and review these computer records [31 CFR 103.36(c)].

904. Additional checks, controls and requirements are imposed on casinos under state, tribal or local laws. For example, most casinos maintain multiple transaction logs, which are used to record currency transactions above a given threshold, usually USD 2,500 to USD 3,000. Generally, casinos record on these logs customers' purchases of chips or tokens with currency, redemption of chips or tokens for currency, currency exchanges, and wagers in currency.

Accountants, lawyers, dealers in precious metals and stones, real estate agents and TCSPs

905. These categories of DNFBP are required to maintain the information collected for the purpose of meeting their Form 8300 reporting requirements for five years.

4.1.2 Recommendations and Comments

906. Casinos are subject to customer identification and record keeping requirements that meet several of the requirements of Recommendation 5, and meet Recommendation 10. The existing obligations seem to be implemented effectively. However, some of the components of Recommendation 5 are missing. In particular, casinos are not explicitly required to perform enhanced due diligence for higher risk categories of customers, nor is there a requirement to undertake CDD when there is a suspicion of money laundering or terrorist financing. The U.S. should make casinos subject to these obligations. There is very limited application of Recommendations 5 and 10 to accountants, dealers in precious metals, stones and jewels, lawyers and real estate agents. Customer identification and record keeping requirements only apply to these sectors in relation to their obligation to file Forms 8300. The U.S. should extend customer identification, record keeping and account monitoring obligations that are consistent with FATF Recommendations to these sectors as soon as possible.

907. DNFBPs are not subject to obligations that relate to Recommendations 6, 8 or 11, with the exception of casinos which are subject to suspicious activity reporting and are thus responsible for monitoring of unusual transactions (Recommendation 11).

908. In the short term, a proposed final rule should be issued to expedite the introduction of AML obligations for "persons involved in real estate closings and settlements." Additionally, the U.S. should prepare an advanced notice of proposed rulemaking in the near future in relation to the TCSP sector—especially in light of the views that were expressed in the January 2006 threat assessment. This proposal should extend both the AML Program and CIP requirements to this sector.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	NC	• Casinos are not required to perform enhanced due diligence for higher risk categories of customer, nor is there a requirement to undertake CDD when there is a suspicion of money laundering or terrorist financing (R.5). • Accountants, dealers in precious metals and stones, lawyers and real estate agents are not subject to customer identification and record keeping requirements that meet Recommendations 5 and 10. • None of the DNFBP sectors is subject to obligations that relate to Recommendations 6, 8 or 11 (except for casinos in relation to R.11).

4.2 Monitoring transactions and other issues (R.16)

(applying R.13-15 & 21)

4.2.1 Description and Analysis

Applying R.13 (Suspicious transaction reporting)

Casinos

909. As part of its required AML Program, a casino must have procedures for filing a report of any activity when there is a suspicion of money laundering or terrorist financing at the required reporting threshold [31 CFR 103.21(a)(1)]. This suspicious activity reporting obligation applies to all casinos and card clubs with gross annual gaming revenues of USD 1,000,000 or more, including those in the state of Nevada (31 CFR 103.21). It is expected that casinos will follow a risk-based approach in monitoring for suspicious transactions, and will report all detected suspicious transactions that involve USD 5,000 or more in funds or other assets. A well-implemented AML compliance program should reinforce a casino's efforts in detecting suspicious activity.

910. Casinos must file a report of any suspicious transaction that it believes is relevant to the possible violation of any law or regulation that is conducted or attempted by, at, or through a casino, and involves or aggregates at least USD 5,000 in funds or other assets, and the casino knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

(a) Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;

(b) Is designed, whether through structuring or other means, to evade any requirements of this part or of any other regulations promulgated under the BSA, Public Law 91-508, as amended, codified at 12 USC 1829b, 12 USC 1951-1959, and 31 USC 5311-5332;

(c) Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the casino knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or,

(d) Involves use of the casino to facilitate criminal activity [31 CFR 103.21(a)(2)(iv)]. This pertains to transactions involving legally derived funds that the casino knows, suspects or has reason to suspect are being used for a criminal purpose, such as money laundering or terrorist financing.

911. Casinos are required to report transactions that appear, for whatever reason, to be conducted for an unlawful purpose. Additionally, casinos may voluntarily file suspicious transaction reports in situations in which mandatory reporting is not required, such as transactions that fall below the USD 5,000 reporting threshold. As well, casinos can contact FinCEN's Financial Institutions Hotline (1-866-556-3974), to voluntarily to report to law enforcement suspicious transactions that may relate to terrorist activity. Casinos reporting suspicious activity by calling the Financial Institutions Hotline must still file a timely FinCEN Form 102, Suspicious SARC, to the extent required by 31 CFR 103.21.

912. On 16 October 2000, the state of New Jersey imposed a suspicious activity reporting requirement on casinos in that state (P.L. 1977, which amended the New Jersey's "Casino Control Act"), which was in effect before the BSA's casino suspicious activity reporting requirement (31 CFR 103.21) took effect nationwide for all applicable casinos and card clubs, on 25 March 2003.

913. FinCEN publishes statistics concerning the rate of casino SAR reporting twice annually in "The SAR Activity Review-By The Numbers", which is available on FinCEN's website and covers the periods

1 January to 30 June and 1 July to 31 December. The statistics included in the publication include number of filings by U.S. states and territories, by violation reported, by type of establishment (state licensed, tribal licensed, card club, other and unspecified) and by year and month of filing. The following chart shows the number of SARs filed by casinos or card clubs for the calendar years 2001 through 2005.

YEAR	NUMBER OF SARs FILED
2001	1,377
2002	1,827
2003	5,095
2004	5,754
2005	2,827

Accountants, dealers in precious metals and stones, lawyers, real estate agents and TCSPs

914. These categories of DNFBPs are not required at this time to file SARs. They are permitted to report suspicious transactions voluntarily. However, as discussed below, because they are defined as "financial institutions" under the BSA, only dealers in precious metals, stones and jewels, and persons involved in real estate closings and settlements, are protected from liability for making a disclosure to appropriate authorities. More generally, all persons subject to Form 8300 reporting (including accountants and TCSPs) may complete Item 1 of the Form that has a box for reporting a "suspicious transaction". In this context, a "suspicious transaction" is defined as "a transaction in which it appears that a person is attempting to cause Form 8300 not to be filed, or to file a false or incomplete form. The term also includes any transaction in which there is an indication of possible illegal activity." (For a detailed description of the Form 8300 requirements, see section 3.7 of this report).

Applying R.14 (Protection from liability and tipping off)

Casinos

915. Casinos, and any directors, officers, employees, or agents of such casinos, like other financial institutions, enjoy broad protection from civil liability for making reports of suspicious transactions (whether such reports are required by 31 CFR 103.21 or made voluntarily) [31 USC 5318(g)(3) and 31 CFR 103.21(e)]. Persons filing suspicious activity reports are prohibited from disclosing that a report has been prepared or filed, except to appropriate law enforcement and regulatory agencies [31 USC 5318(g)(2) and 31 CFR 103.21(e)].

Dealers in precious metals and stones

916. Any financial institution (as defined under the BSA, and which includes dealers in precious metals, stones and jewels, as well as persons involved in real estate closings and settlements) that chooses to file a suspicious transaction report is prohibited from notifying the subject of the report that the transaction has been reported [31 USC 5318(g)(2)]. The business is also protected from liability for making a disclosure or failing to notify the subject of the disclosure or any other person identified in the disclosure [31 USC 5318(g)(3)].

Accountants, lawyers, and TCSPs

917. Since they are not defined as "financial institutions" under the BSA, accountants, lawyers, and TCSPs are not covered by the voluntary disclosure provisions and protections of 31 USC 5318(g). The protection from liability and tipping off provisions do not apply to businesses that complete the suspicious transaction box on Form 8300. (For a detailed description of the Form 8300 requirements, see section 3.7 of this report).

Applying R.15 (Internal controls)

Casinos

918. BSA statute and regulation require each financial institution (including a casino or card club) to develop an effective AML compliance program [31 USC 5318(h) and 31 CFR 103.64(a) and 103.120(d)]. Each program must be commensurate with the risks posed by the products and financial services provided by the casino and card club. An effective program is one that is developed, implemented, maintained and reasonably designed to prevent the casino and card club from being used to facilitate money laundering or terrorist financing. At a minimum, each AML Program must be in writing and must have, among other things:

(a) System of internal controls to assure ongoing compliance with the BSA's suspicious and currency reporting, identification, recordkeeping, record retention, and compliance program requirements;

(b) Internal and/or external independent testing for compliance with a scope and frequency commensurate with the money laundering and terrorist financing risks posed by the products and services provided;

(c) Training of casino personnel (e.g., providing education and/or training of appropriate personnel), including training in the identification of unusual or suspicious transactions, to the extent that the reporting of such transactions is required;

(d) Designation of an individual or individuals (e.g., a compliance officer) responsible for day-to-day compliance with the BSA and the program;

(e) Procedures for using all available information to determine:

- when required, the name, address, social security number, and other information, and verification, of a person, and
- the occurrence of any transactions or patterns of transactions required to be reported as suspicious; and

(f) For casinos that have automated data processing systems, the use of computers to aid in assuring compliance.

Dealers in precious metals and stones

919. FinCEN has issued an interim final rule (IFR) requiring certain dealers in precious metals, stones, or jewels to establish an AML Program [70 FR 33702 (9 June 2005)]; after issuance of a notice of proposed rule making in 2003 [68 FR 8480 (21 February 2003)]. Dealers in covered goods who are required to comply with the rule must develop AML Programs by 1 January 2006. At a minimum, the AML Program must be comprised of the following four elements:

(a) Policies, procedures and internal controls, based on the dealer's assessment of the money laundering and terrorist financing risk associated with its business;

(b) A compliance officer who is responsible for ensuring that the program is implemented effectively;

(c) Ongoing training of appropriate persons concerning their responsibilities under the program; and

(d) Independent testing to monitor and maintain an adequate program.

920. The IFR covers manufacturers, refiners, wholesalers, certain retailers considered dealers, and any other entity engaged in the business of purchasing and selling jewels, precious metals, precious stones, or jewelry.

921. The IFR applies to "dealers" that have purchased and sold at least USD 50,000 worth of "covered goods" during the preceding year. FinCEN has defined the term "dealer" as it is commonly understood: A person who both purchases and sells covered goods. Additionally, FinCEN has included dollar thresholds in the definition of "dealer": A person must have purchased at least USD 50,000 and sold at least USD 50,000, worth of covered goods during the preceding year. The dollar threshold is intended to ensure that the rule only applies to persons engaged in the business of buying and selling a significant amount of items rather than small businesses, occasional dealers and persons dealing in such items for hobby purposes. For example, the rule excludes the buying or selling of value-added fabricated goods containing minor amounts of precious metals or gemstones, such as dealers in computers or drills with industrial diamond cutting tools or other goods containing minor amounts of precious metals or gemstones used for their strength.

922. Significantly, the interim rule distinguishes between a "dealer" and "retailer" of covered goods. FinCEN has defined the term retailer as a person engaged within the U.S. in sales of covered goods, primarily to the public. Based on the risk assessment conducted, FinCEN determined that retailers, as defined, do not pose the same level of risk for money laundering as do dealers. Thus, most retailers will not be required to establish AML Programs. "Covered goods" include jewels, precious metals, and precious stones, and finished goods (including but not limited to, jewelry, numismatic items, and antiques) that derive 50% or more of their value from jewels, precious metals, or precious stones contained in or attached to such finished goods.

923. A dealer's AML Program must incorporate policies, procedures, and internal controls based upon the dealer's assessment of the money laundering and terrorist financing risks associated with its line(s) of business [31 CFR 103.140(c)(1)]. Policies, procedures, and internal controls must also include provisions for complying with applicable BSA requirements. Thus, a dealer's program must address its obligation to report on Form 8300 the receipt of cash or certain non-cash instruments totaling more than USD 10,000 in one transaction or in two or more related transactions. If dealers become subject to additional BSA requirements, their AML Programs will need to be updated accordingly.

924. For purposes of making the required risk assessment, a dealer must consider all relevant factors, including the specific factors contained in the rule, which require a dealer to:

(a) assess the money laundering and terrorist financing risks associated with its products, customers, supplies, distribution channels, and geographic locations;

(b) take into consideration the extent to which the dealer engages in transactions other than with established customers, or sources of supply, or other dealers subject to this rule; and

(c) analyze the extent to which it engages in transactions for which payment or account reconciliation is routed to or from accounts located in jurisdictions that have been identified as vulnerable to terrorism or money laundering.

925. The rule is intended to give a dealer the flexibility design its program to meet specific money laundering and terrorist financing risks presented by the dealer's business, based on the dealer's assessment of those risks [31 CFR 103.140(c)(1)(i)].

926. A dealer's policies, procedures, and internal controls must be reasonably designed to detect transactions that may involve use of the dealer to facilitate money laundering or terrorist financing [31 CFR 103.140(c)(1)(ii)]. In addition, a dealer's program must incorporate procedures for making reasonable inquiries to determine whether a transaction may involve money laundering or terrorist financing. A dealer that identifies indicators that a transaction may involve money laundering or terrorist financing should take reasonable steps to determine whether its suspicions are justified and respond accordingly, including refusing to enter into, or complete, a transaction that appears designed to further illegal activity. However, the dealer is not required to report such a suspicious transaction to FinCEN as there is no SAR requirement for the dealer.

927. The obligation on dealers in precious metals and stones to implement AML Programs is very recent. Consequently, the obligation is in the early stages of being implemented. Additionally, industry associations such as the Jewelers' Vigilance Committee (JVC) and Manufacturing and Jewelers Suppliers of America (MJSA), who reach a combined membership of over 12,000 members, are working with their members to make them aware of their obligations. This includes providing them AML packages and templates that will assist them in developing effective internal controls. However, these efforts are challenged by the diverse characteristics of the sector and the fact that many participants do not belong to any industry association. The situation is further complicated because most of these businesses have never been subject to regulation before. FinCEN has published guidance [e.g. Frequently Asked Questions: Interim Final Rule – Anti-Money Laundering Programs for Dealers in Precious Metals, Stones, or Jewels (3 June 2005); FinCEN Ruling 2006-1 – Anti-Money Laundering Programs for Dealers in Silver (30 December 2005)].

Accountants, lawyers, real estate agents and TCSPs

928. There are currently no AML internal control obligations imposed on these categories of business.

Applying R.21 (Countries that insufficiently apply the FATF Recommendations)

Casinos

929. As part of their required AML Programs, casinos must have procedures for reviewing country advisories issued by FinCEN that urge enhanced scrutiny of financial transactions with countries that have deficient AML controls.

Accountants, lawyers, real estate agents and TCSPs

930. FinCEN has issued country advisories urging enhanced scrutiny of financial transactions with countries that have deficient AML controls (see detailed discussion in section 3.10.1). These advisories are generally available and can be accessed by DNFBPs. However, no specific obligations have been imposed on accountants, lawyers, real estate agents or TCSPs in this regard.

4.2.2 Recommendations and Comments

931. Although casinos are required to report suspicious transactions, there is a threshold on that obligation. This threshold should be removed because Recommendation 13 requires that all suspicious transactions should be reported, regardless of amount. As well, the obligation to report suspicious transactions should be extended to all other DNFBP sectors.

932. Accountants, lawyers, real estate agents and TCSP should be made subject to the "tipping off" provision and should be protected from liability when they choose to file a suspicious transaction report. They should also be required to implement adequate internal controls (i.e. AML Programs).

933. Continued work is needed to ensure that dealers in precious metals and stones are aware of their obligation to establish AML Programs and are implementing them effectively.

934. The U.S. should obligate accountants, lawyers, real estate agents and TCSPs to give special attention to the country advisories that FinCEN has issued and which urge enhanced scrutiny of financial transactions with countries that have deficient AML controls.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	NC	• Casinos are the only DNFBP sector that is required to report suspicious transactions; however,

		there is a threshold on that obligation. • Accountants, lawyers, real estate agents and TCSPs are not subject to the "tipping off" provision or protected from liability when they choose to file a suspicious transaction report. • Accountants, lawyers, real estate agents and TCSPs are not required to implement adequate internal controls (i.e. AML Programs). • Dealers in precious metals, precious stones, or jewels are required to implement AML programs; however, the effectiveness of implementation cannot yet be assessed. • There are no specific obligations on accountants, lawyers, real estate agents or TCSPs to give special attention to the country advisories that FinCEN has issued and which urge enhanced scrutiny of financial transactions with countries that have deficient AML controls.

4.3 Regulation, supervision and monitoring (R. 17, 24 & 25)

4.3.1 Description and Analysis

Recommendations 24 (Regulation and supervision of DNFBP)

Casinos

935. In the U.S., gambling regulation is primarily a matter of state/territory law, reinforced by federal law in the case of AML laws or where the presence of interstate or foreign elements might otherwise frustrate the enforcement policies of state law. Where duly licensed or authorized to do business, casinos and card clubs are regulated, in differing degrees, by various state, local and tribal governmental agencies, and federally for compliance with AML/CFT requirements.

936. For U.S. commercial casinos (i.e., non-tribal), each must apply for gambling licenses from casino commissions located in relevant states/territories. The state gaming commissions require that each of these commercial gaming establishments be a separate business and therefore grants each a separate casino license. The focus of these non-federal requirements are typically investigating the qualifications of each applicant seeking a gaming license (owners and principal shareholders, key casino employees and, in some cases, all casino employees), issuing casino licenses, promulgating regulations (e.g., on the types of games offers, the integrity of the games and consumer protection issues, internal controls, etc.), investigating violations of these gaming regulations, initiating regulatory compliance actions against licensees, hearing and deciding licensing cases, and interaction with other regulators and law enforcement agencies.

937. A casino that is duly licensed or authorized to do business as such, and has gross annual gaming revenue in excess of USD 1 million, is a "financial institution" under the BSA [31 USC 5312(a)(2)(X) and 31 CFR 103.11(n)(5)(i) and (n)(6)(i)]. While the statutory definition is written to include casinos or other types of gaming establishments, the regulatory definition, at this time, applies to duly licensed or authorized casinos which includes state/ territory -licensed casinos (both land-based and riverboat), tribal casinos, and card clubs, which includes state/territory and tribal card clubs.

938. The key AML/CFT requirements which are applicable to casinos are contained in the BSA rules (31 CFR Part 103). Specifically, casinos must meet the following requirements:

(a) the reporting of suspicious activity when a casino knows, suspects or has reason to suspect that the transaction or pattern of transactions is both suspicious and involves USD 5 000 or more (31 CFR 103.21);

(b) the reporting of each transaction in currency, involving either "cash in" or "cash out", of more than USD 10 000 in a gaming day [31 CFR 103.22(b)(2) and (c)(3)];

(c) detailed recordkeeping (31 CFR 103.36); and

(d) a written compliance program [31 CFR 103.64 and 103.120(d)].

939. In addition to the casino specific requirements, there are other reporting, general recordkeeping, and special rules under the BSA that apply to all financial institutions, including casinos and card clubs, such as:

(a) reports of transportation of currency or monetary instruments (31 CFR 103.23);

(b) reports of foreign financial accounts (31 CFR 103.24);

(c) filing of timely and complete reports (31 CFR 103.27);

(d) identification required (31 CFR 103.28);

(e) records and identification required for purchase of certain monetary instruments with USD 3,000 to USD 10,000 in cash (31 CFR 103.29);

(f) records by persons having financial interests in foreign financial accounts (31 CFR 103.32);

(g) records of transmittals of funds in excess of USD 3,000 requiring recordkeeping, verification of identity, retrievability and reporting of this information to other financial institutions in the payment chain, regardless of the method of payment [31 CFR 103.33(f) and (g)];

(h) nature of records and retention period (31 CFR 103.38); and

(i) structured transactions (31 CFR 103.63).

940. FinCEN is responsible for administering the BSA. FinCEN is accountable for ensuring compliance with the BSA, but does not itself directly examine financial institutions for compliance with that law. Instead, FinCEN has delegated examination responsibility to the IRS for state/territory licensed casino gaming operations, other than Nevada gaming operations, as well as tribal casinos [31 CFR 103.56(b)(8)]. The National Indian Gaming Commission (in the case of Indian gaming operations) will examine some tribal casinos pertaining to BSA casino recordkeeping and CTRC reporting requirements as part of its efforts to ensure compliance with its Minimum Internal Control Standards (25 CFR 542). Where duly licensed or authorized to do business, casinos are also regulated by various state, local and tribal governmental agencies. The following table seeks to draw out which authorities examine for BSA compliance.

Type of gaming operations	BSA examination authority has been delegated by FinCEN to:
State/territory "commercial" licensed casino gaming operations, other than Nevada gaming operations, as well as tribal casinos	IRS-SBSE
Nevada gaming operations	Nevada Gaming Commission, NGC (whereby both FinCEN and IRS are allowed to accompany NGC personnel during certain examinations. Relating to SARs, the authority to examine Nevada casinos compliance belongs not to the NGC but in full to FinCEN and the IRS.
Indian gaming operations pertaining to casino recordkeeping and CTRC reporting requirements	National Indian Gaming Commission and Tribal Gaming Commission (established at States level in the frame of State Compacts). IRS-SBSE

941. IRS conducts examinations of casinos to ensure they are complying with their obligations under the BSA, including their Form 8300 filing obligations (which require them to file reports for currency received in excess of USD 10,000) (31 USC 5331 and 26 USC 6050I). This includes approximately 845 casinos or other gaming organizations located in some 34 states and territories and on tribal lands.

942. Since 1999, FinCEN has provided to the IRS detailed written guidance to assist it in developing effective programs and procedures for examining casinos. IRS personnel educate gaming operations as to their responsibilities under the BSA, provide information concerning the specific reporting, identification, recordkeeping, record retention, and compliance program requirements, and provide practical information on the discharge of these responsibilities. These education and outreach efforts

are important to keep these gaming operations informed of their BSA compliance obligations. Also, the IRS may provide a copy of 31 CFR Part 103 along with the applicable reporting forms and other informational documents.

State/territory-licensed casino gaming operations

943. State/territory-licensed casino gaming operations are found in fourteen jurisdictions, each of which has a gaming regulator.

944. State-licensed gambling casinos whose gross annual gaming revenues exceeded USD 1 million were generally made subject to the Bank Secrecy Act (BSA) by regulation in 1985 [50 FR 5069 (6 February 1985)]. Special BSA regulations relating to casinos were issued in 1987, and amended in 1989 and (more significantly) in 1994 [52 FR 11443 (8 April 1987), 54 FR 1165 (12 January 1989), and 59 FR 61660 (1 December 1994) (modifying and putting into final effect the rule originally published at 58 FR 13538 (12 March 1993)]. The Money Laundering Suppression Act (Title IV of the Riegle Community Development and Regulatory Improvement Act of 1994 – Pub. L 103-325) explicitly added casinos (both state-licensed and tribal), or other gaming establishments (e.g., card clubs), to the list of financial institutions specified in the BSA.

945. The state gaming commissions typically investigate the qualifications of each applicant seeking a gaming license, issue casino licenses, promulgate regulations (e.g., on the types of games offered, the integrity of the games and consumer protection issues, internal controls, etc.), investigate violations of these gaming regulations, initiate regulatory compliance actions against licensees, hear and decide licensing cases, and interact with other regulators and law enforcement agencies.

946. It is common for many state regulators also to impose internal control standards on the casinos that they license. Although these state standards vary somewhat from each other, they typically include procedures for handling table games, rules of the game, electronic gaming devices, casino cashiering and credit, check cashing, casino accounting, internal audit, surveillance, security, etc. Several of these regulators also have internal control procedures for CTRC reporting (e.g., Colorado, Illinois, Indiana, Louisiana, Michigan, and Missouri). It is normally within a state's CTRC reporting internal control standards that one finds the requirement to prepare currency multiple transaction logs.

Nevada gaming operations

947. Nevada legalized gaming 1931 and was the first U.S. state to do so. The oversight of the Nevada casinos and of the administration of the state laws and regulations that govern gaming is exercised by the Nevada Gaming Commission (NGC). The NGC is comprised of 5 part-time persons and by the State Gaming Control Board (which is comprised of 3 persons serving in a full time capacity). The Gaming Board has a staff of more than 350 people who are assigned to 7 divisions. It has offices in 6 locations (Las Vegas, Carson City, Elko, Laughlin and Reno).

948. The Nevada Gaming Commission ("Commission") and State Gaming Control Board ("Board") control who may have a gaming license. Specifically, the Commission determines if a person is qualified to receive a gaming license and to be qualified the Commission, pursuant to Nevada Revised Statutes ("NRS") 463.170, must be satisfied that the applicant for a licensee is:

> "(a) A person of good character, honesty and integrity;
>
> (b) A person whose prior activities, criminal record, if any, reputation, habits and associations do not pose a threat to the public interest of this State or to the effective regulation and control of gaming or charitable lotteries, or create or enhance the dangers of unsuitable, unfair or illegal practices, methods and activities in the conduct of gaming or charitable lotteries or in the carrying on of the business and financial arrangements incidental thereto; and

(c) In all other respects qualified to be licensed or found suitable consistently with the declared policy of the State."

949. Further, the Board, pursuant to NRS 463.1405, must "investigate the qualifications of each applicant" before any gaming license is issued. Also, Commission Regulation 3.110 allows for the Commission to require that any key employee (e.g. management personnel) be licensed.

950. As far as AML/CFT requirements are concerned, Nevada Regulation6A (Regulation 6A) is a key requirement. The Secretary of the Treasury may exempt [31 CFR 103.55(c)] from the BSA's CTRC reporting and recordkeeping requirements for casinos any state whose regulatory system contains substantially similar requirements. On 8 May 1985, the Secretary of the Treasury entered into a Memorandum of Agreement with the State of Nevada, through its Gaming Commission and Gaming Control Board (the Nevada exemption agreement). The agreement, among other things, granted Nevada casinos an exemption from certain record keeping and reporting requirements of the BSA. Specifically, the agreement exempts Nevada casinos, subject to Nevada Gaming Commission Regulation 6A, from the requirement to file the standard "CTR by Casinos" form. The agreement did however require Nevada to maintain its own CTRC reporting system that is required to be substantially similar to the BSA.[78] Nevada has implemented its system through Nevada Gaming Commission Regulation 6A.

951. Nevada Gaming Commission Regulation 6A, "Cash Transactions, Prohibitions, Reporting and Recordkeeping," was adopted in 1985, amended in 1997, and currently requires certain Nevada casinos to report currency transactions in excess of USD 10,000, to keep records of certain casino transactions, to maintain appropriate internal controls, and to maintain written compliance programs. Under that system, Nevada casinos are required to file CTRs with FinCEN on FinCEN Form 103-N "CTR by Casinos – Nevada." Also, the Nevada Gaming Control Board has on-line access to Form 103-Ns, pursuant to an interagency agreement with FinCEN.

952. As a result of the Nevada exemption agreement and Regulation 6A, neither FinCEN nor the IRS has authority to examine Nevada casinos for compliance with CTRC-N reporting requirements under Nevada law. However, FinCEN may request that Nevada conduct an examination of a casino at any time and both FinCEN and the IRS are authorized to accompany Nevada personnel during such an examination. Finally, because of the agreement, FinCEN has no authority to take civil enforcement action against a Nevada casino for failing to file the CTRC-Ns because the Nevada casino has no obligation to file under the BSA or FinCEN's regulations.[79] Nonetheless, the Nevada regulator has authority to penalize Nevada casinos for non-compliance with Regulation 6A. In addition to the Regulation 6A requirements, all Nevada casinos with gross annual gaming revenues of USD 1,000,000 or more are subject to the following BSA requirements: (1) the requirement to establish and maintain a written anti-money laundering program [31 CFR 103.64(a) and 103.120(d)]; and (2) the requirement to report suspicious activity when a casino knows, suspects or has reason to suspect that the transaction or pattern of transactions is both suspicious and involves USD 5,000 or more (31 CFR 103.21). Further, Nevada casinos that are not subject to Regulation 6A, but that have gross annual gaming revenues in excess of USD 1,000,000, are subject to all of the provisions of the Bank Secrecy Act applicable to casinos generally (31 CFR Part 103). Nevada casinos are subject to federal regulation under the BSA relating to the filing of SARs because Nevada Regulation 6A does not have a similar requirement. Consequently, the IRS has the authority to examine Nevada casinos

[78] Nevada Gaming Commission Regulation 6A, "Cash Transactions, Prohibitions, Reporting, and Recordkeeping," was adopted in 1985, amended in 1997, and currently requires certain Nevada casinos to report to FinCEN and the Gaming Control Board currency transactions in excess of USD 10,000, to keep records of certain casino transactions, to maintain appropriate internal controls, and to maintain written compliance programs.

[79] Nevada casinos are subject to federal regulation under the BSA relating to the filing of SARs because Nevada Regulation 6A does not have a similar requirement. Consequently, FinCEN and the IRS have the authority to examine casinos for compliance with, and take enforcement action with respect to, suspicious activity reporting requirements. See 31 CFR 103.21.

for compliance with, and FinCEN has the authority to take enforcement action with respect to, SAR requirements [31 CFR 103.21, 103.64(a), and 103.56(b)(8)].

953. The Nevada exemption agreement implementing the exemption acknowledges, and is contingent upon, the existence and continuance of a state casino regulatory regime that is substantially similar to the federal standards. With respect to compliance and enforcement, the agreement, along with Nevada Regulation 6A, holds Nevada responsible for assuring compliance with the reporting and record keeping obligations of casinos under Nevada rules. The agreement further provides that Nevada must maintain sufficient safeguards to assure compliance with obligations of the state requirements and take appropriate action to administer, enforce and examine for compliance with Nevada Regulation 6A.

954. Although pursuant to the Nevada exemption agreement, Nevada casinos are exempt from the CTRC reporting and certain record keeping requirements of the BSA, the exemption is contingent on Nevada's regulation remaining substantially similar to the BSA's regulation. For instance, the Nevada Gaming Commission has issued for its Regulation 6A, detailed minimum internal control standards for CTRC-N reporting and recordkeeping.

955. In some respects, Regulation 6A has been revised to keep it in line with the revisions of the BSA's provisions and in order to provide reporting path to the IRS. However, Regulation 6A does differ from the BSA in some respects—namely relating the threshold of USD 1 million or more of gross revenue. This threshold is based on a risk assessment that the Nevada authorities, working with FinCEN, did in 1997. The risk assessment concluded that the BSA threshold definition of a "casino" was too low, and captured places such as a bar or grocery store with 20 slot machines manned by a person who does nothing more than sell change. The Nevada authorities advised FinCEN that they did not see these establishments as posing a money laundering risk. In 1997, FinCEN finally agreed that these small places probably should not be subject to Regulation 6A and accepted the threshold being moved to USD 10 million. However, in November 2003 the Nevada Gaming Control Board submitted to FinCEN an extensive survey of about 145 smaller Nevada casino licensees that identified about 50 of the larger ones that offered a variety of cage financial services to customers other than just gambling (e.g. deposit and credit accounts, check cashing, currency exchange, money transfers). There are now about 114 casinos which fall into the exemption. An additional 145 casinos have less than USD 10 million but more than USD 2 million in gross revenue. Another significant difference between Nevada Regulation 6A and the BSA is in prescribing when multiple currency transactions that aggregate to more than USD 10,000 in a single gaming day must be reported, with the BSA requirements being more inclusive [31 CFR 103.22(c)(3)] than Nevada Regulation 6A.040(2). Nevada casinos currently report to FinCEN using CTRN forms which are somewhat close in substance to the forms used by all non-Nevada casinos and which must also be filed with the IRS (Detroit Computing Center)), except the types of transactions and the currency aggregation requirements under Regulation 6A is more limited than under the BSA (discussed above). In addition, all casinos subject to the BSA's suspicious transaction reporting requirement, including those in Nevada, report to FinCEN using Form 102 (SARC). Moreover, Nevada casinos that are not subject to Regulation 6A, but that have gross annual gaming revenues in excess of USD 1,000,000, are subject to all of the provisions of the Bank Secrecy Act applicable to casinos generally (31 CFR Part 103).

956. In May 2003, FinCEN advised the Nevada Gaming Control Board that its regulation no longer "substantially meets" [31 CFR 103.55(c)] the BSA's regulation. Given the discrepancies between the Nevada Regulation 6A and the BSA regulation, and in light of the importance of consistency among the many jurisdictions permitting gaming, FinCEN has discussed with the Nevada Gaming Control Board the outstanding issues between the two casino regulatory systems in an effort to resolve the variances. In May 2005, the Nevada Gaming Control Board recommended to the Nevada Gaming Commission that it repeal Regulation 6A. With the repeal of Regulation 6A, all BSA examination and enforcement of the Nevada casino industry would become the responsibility of the IRS and FinCEN.

As of August 2005, FinCEN is still discussing with the Nevada Gaming Control Board how an orderly transition of these responsibilities could occur.

957. The Nevada legislature has legalized interactive gambling, pending the adoption by the Gaming Commission of corresponding regulations. However, as long as no such regulations exist, internet gaming is not legal in Nevada and such operations would be prosecuted.

Indian gaming operations

958. Tribal government-sponsored gaming is an evolution dating back to the late 1970's. After the Supreme Court confirmed (in 1987) the right of the tribal governments to establish gaming operations, Congress passed in 1988 the Indian Gaming Regulatory Act (IGRA) (25 USC 2701) which recognized, but limited, the right of tribes "to conduct gaming operations" and embodies a compromise between state and tribal interest. According to the IGRA, the states are given a voice in determining the scope and extent of tribal gaming by requiring tribal-state compacts for all forms of casinos style gambling—so called Class III, Class II (bingo style games) is jointly regulated by tribes and the National Indian Gaming Commission. Class I (traditional Indian gaming involving minimal prizes) is regulated exclusively by tribes.

959. Gambling casinos authorized to do business under the Indian Gaming Regulatory Act became subject to the BSA, by amendment in 1994 and by regulation in 1996 [61 FR 7054 – 7056 (23 February 1996)], and the class of gaming establishments known as "card clubs" became subject to the BSA by regulation in 1998 [63 FR 1919-1924 (13 January 1998)]. The same gross annual gaming revenue threshold of in excess of USD 1 million applies to these gaming establishments.

960. Tribal Gaming is present in 27 states across the U.S. The 307 tribal casinos are located in the following states: Alabama (3), Arizona (22), California (52), Colorado (2), Connecticut (2), Florida (6), Idaho (3), Iowa (3), Kansas (5), Louisiana (3), Michigan (17), Minnesota (18), Mississippi (2), Montana (5), Nebraska (1), New Mexico (14), New York (6), North Carolina (1), North Dakota (5), Oklahoma (50), Oregon (9), South Dakota (10), Texas (1), Washington State (27), Wisconsin (17), and Wyoming (2).

961. The IGRA establishes the jurisdictional framework that governs Indian gaming. The IGRA created certain classes of gaming. The two that are relevant to the BSA are Class II tribal card clubs and all forms of Class III gaming, which is comparable to casino gaming. Class II gaming is jointly regulated by the Tribes and the National Indian Gaming Commission. Class III gaming is lawful on Indian lands only if such activities are, among other things, conducted in conformance with a tribal-state compact entered into by an Indian tribe and a state and approved by the Secretary of the Interior. The National Indian Gaming Commission has recognized that the Treasury has established unique AML requirements when it promulgated Minimum Internal Control Standards [64 FR 590, (5 January 1999)] for Class II and III tribal gaming operations which require that such operations establish standards which shall comply with 31 CFR Part 103.

962. The IGRA also created the National Indian Gaming Commission (NGIC) as an independent federal regulatory agency whose primary mission is to regulate gaming activities on Indian lands for the purposes of shielding Indian tribes from organized crime and other corrupting influences, ensuring that Indian tribes are the primary beneficiaries of gaming revenues, and assuring that gaming is conducted fairly and honestly by both operators and players.

963. The National Indian Gaming Commission is authorized to: conduct background investigations of primary management officials and key employees of a gaming operation, conduct audits, review and approve tribal gaming ordinances and management contracts, promulgate federal regulations, investigate violations of these gaming regulations, and undertake enforcement actions (including the assessment of fines and issuance of closure orders). The NGIC maintains six field offices (Washington DC, Portland, Sacramento, Phoenix, St.-Paul and Tulsa) that assist tribes in developing compliance with the law, monitoring Indian gaming operations, conducting background investigations

of individuals and companies seeking approvals of management contracts. Since it became operational in 1993, the NGIC has been submitted 233 management contracts. A large number have been withdrawn or modified one or more times

964. Additionally, many tribal gaming commissions have been established to oversee tribal gaming and are typically semi-autonomous or independent agencies of tribal governments. The primary purpose of a tribal gaming commission is to regulate and oversee Class II and Class III gaming operations consistent with rules and procedures established under tribal gaming ordinances. However, there is potential for a lack of clear and sufficient separation between the tribal commissions and the tribal nations themselves.

965. Tribal governments are required to submit their gaming ordinances or resolutions (including a copy of the tribal-state compact for Class III gaming) as well as any management contracts for the operation of gaming activities to the National Indian Gaming Commission for approval (25 USC 2710). The ordinance submitted to the National Indian Gaming Commission may define how a tribe is operating its gaming establishments (i.e., are they identified as separate operations or one operation). Tribes also have authority to regulate and oversee Class III gaming operations pursuant to tribal-state compacts, which typically recognize and require various degrees of tribal regulation on the gaming enterprises.

> *Case Study – Arizona Tribal Gaming*
>
> According to the Indian Gaming Regulatory Act 1988, Tribes must negotiate with the states in the form of a Compact concerning the conditions at which casinos can be operated in a given State. In the state of Arizona, 22 casinos are set that way. In Arizona, the Arizona Department of Gaming exercises oversight over gaming activities and conducts a yearly audit performed with field examiners. The size of the casinos, the types of games authorized and the betting limits vary significantly. A small/medium sized in Arizona will have, for example, according to the Compact, a USD 500 betting limit.

Dealers in precious metals and stones

966. While FinCEN is responsible for administering the BSA and is accountable for ensuring dealers in precious metals, stones, and jewels comply with the BSA, it does not itself directly examine them for compliance with that law. FinCEN has delegated examination responsibility to the IRS, which examines dealers in precious metals, stones, and jewels to ensure they are complying with their obligations under the BSA, including their Form 8300 filing obligations (which require them to file reports for currency received in excess of USD 10,000) (31 USC 5331 and 26 USC 6050I).

967. Dealers in precious metals, stones and jewels must implement their AML Program by 1 January 2006 [s.103.140(d)] or six months after the date they become subject to the provisions of the IFR. The IRS has indicated that it will commence AML compliance examination of dealers in precious metals, stones and jewels six months after that date. It is unclear, however, whether the IRS will have sufficient resources to manage this new responsibility.

968. The Jeweler's Vigilance Committee (JVC) is an industry organization that handles legal compliance for the sector. Most applicable legal requirements relate to trade practices; however, the JVC has been very proactive in educating its members about the new requirements and helping them to develop AML/CFT programs. Of the existing trade associations, the JVC has the broadest reach into the industry, representing a cross-section of manufacturers, wholesalers and retailers at the national and international level. Moreover, the JVC is the only industry association that promotes compliance with legal requirements, although some others promote ethics. The JVC monitors the trade practices of its members and, in appropriate cases, will impose sanctions which may include

delisting the member. However, the JVC only covers about one third of the sector nationwide. Many dealers do not belong to any trade association or read any trade publications, so they may be completely unaware of the BSA obligations that now apply to them. Nevertheless, most of the biggest players in each part of the industry do belong to the JVC.

Other DNFBP

969. FinCEN has delegated authority to IRS to examine all business and trades (including all the categories of DNFBPs) for compliance with Form 8300 reporting requirements. IRS conducts examinations of such businesses to ensure they are complying with their Form 8300 filing obligations (which require them to file reports for currency received in excess of USD 10,000) (31 USC 5331 and 26 USC 6050I). By end-2005, the IRS had conducted 2,366 such examinations. In other respects there are no oversight procedures for compliance with AML obligations by accountants, lawyers, real estate agents and TCSPs, since no such specific obligations have yet been introduced. However, general conduct of business oversight does exist for some of the businesses and professions, as follows.

Accountants

970. Accountants are subject to Codes of Professional Conduct and state licensing and accreditation. Certified public accountants in the U.S. were solely subject to oversight by a state governmental entity that has the authority to revoke the accountant's license for improper conduct, until July 2002, when the U.S. Congress enacted the landmark Sarbanes-Oxley Act (hereinafter "Sarbanes-Oxley") (15 USC 7201). Public accountants are now subject to oversight by the Public Company Accounting Oversight Board (PCAOB), a federal entity which was created by Sarbanes-Oxley to oversee the auditors of public companies in order to, among other things, ensure preparation of fair and impartial audit reports, strengthen auditor independence rules, increase accountability of officers and directors, and enhance the timeliness and quality of financial reports of public companies.

Lawyers

971. Legal professionals in the U.S. are currently subject to substantial regulation by primarily state, and to a more limited extent, federal entities, as well as self regulatory organizations, in a way that has a bearing on AML concerns. A legal professional's professional and, in some cases, nonprofessional activities are regulated by state rules of professional conduct. A lawyer who litigates before any state or federal court is subject to that court's rules. In addition, some federal agencies impose limitations and due diligence requirements on the professional activities of lawyers practicing before those agencies. Those agencies can sanction lawyers who engage in proscribed activities. Finally, lawyers are subject to criminal and civil sanctions (including disbarment) and liability arising from federal, state, and local laws, regulations, and rules that apply to other citizens. As well, the ABA Section of the International Law and Practice, Committee on Anti-Money Laundering and Professional Ethics, and the ABA Task Force on Gatekeeper Regulation and the Profession ("ABA Gatekeeper Task Force") have been established to, among other things, monitor the issue of imposing an AML regime on lawyers and promote understanding within the ABA and legal profession of AML and CFT requirements. The ABA represents approximately 400,000 of the estimated 1.1 million attorneys in the U.S.

972. The regulation of lawyers, including the licensing, is done by the states. Each state sets its own competency requirements for lawyers which may include passing a bar examination and the successful completion of continuing legal education requirements. In the U.S., legal professionals who are not lawyers may operate or practice only under the supervision or oversight of a lawyer and, as a result, are subject to the same regulatory regime as lawyers. Once a lawyer is duly licensed to practice in a jurisdiction, he/she is allowed to engage in any business activity in that jurisdiction as long as the activity is within the parameters of federal and state law, and the activity adheres to the guidelines set forth in the Model Rules of Professional Conduct issued by the American Bar Association (ABA) and each state bar. These requirements generally mandate that lawyers must maintain the integrity and competence of the profession, exercise independent judgment and avoid improper conduct.

973. Legal ethics involve many responsibilities which, while obligatory, are rooted in non-legal or quasi-legal concerns, such as morality and professional tradition. Conduct rules such as the Code of Professional Responsibility or the Rules of Professional Conduct, once adopted as positive law in a jurisdiction, become a dominant source of binding rules in that jurisdiction. Many of the norms applicable to lawyers are self-designed by private bar associations and then adopted by courts and other governmental agencies. The most obvious example is the adoption of the Model Rules of Professional Conduct by courts in the various jurisdictions, after the rules were proposed by the ABA. Even though the Model Rules of Professional Conduct do not have the force of law, they are widely followed and cited by courts as establishing rules of conduct for lawyers in the U.S. Forty-one states and the District of Columbia have adopted the Model Rules as rules for the conduct of lawyers. Violation of any Model Rule or other law is professional misconduct under Model Rule 8.4(a) and could result in disbarment of a duly licensed lawyer. Since private bar associations, other governmental agencies and, particularly, the courts, are dominated by lawyers, regulation may be said to be largely self-imposed. In most situations the rules are activated and self enforced by individual lawyers. When serious violations of the rules are alleged, enforcement also is through the profession and its members, including ultimately members of the judiciary (Enforcement mechanisms; see s.104).

974. Engaging in money laundering activities or knowingly assisting a client in money laundering activities violates every state's rules of professional conduct and could subject the lawyer to severe sanctions, such as disbarment, and the loss of the privilege to practice law. Model Rule 1.2(d) makes it clear that a "lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent". Violating that rule would subject the lawyer to action by the disciplinary authority. It also is professional misconduct to "commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness, or fitness as a lawyer in other respects" or to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation" or conduct "that is prejudicial to the administration of justice" (Model Rule 8.4). Finally, rules of professional conduct require a lawyer not to represent a client, or to withdraw from the representation, where representing the client will result in the lawyer violating rules of professional conduct or other law.

Real estate agents

975. In large part, real estate agents are governed by state law. State real estate boards (which usually have regulatory authority over real estate agents) establish licensing requirements which may include coursework and passing an examination.

Trust and company service providers

976. TCSPs that are not licensed with fiduciary powers under federal or state law,[80] are not "financial institutions" under 31 USC 5312(a)(2), and are not required by law or regulation to comply with BSA requirements, such as establishing AML Programs or filing SARs. Although there is no clearly defined sector within the U.S. that provides the company formation services usually associated with TCSPs, the company laws in certain states create an environment where such services have developed significantly. Delaware, Nevada and Wyoming are the prime examples. Since the activities of such TCSPs are inextricably linked with the corporate law framework in these states, detailed discussion of this sector is addressed under section 6 below (Legal Persons and Arrangements), which contains case studies on Delaware and Nevada.

[80] *e.g. In re Lee*, 75 A.2d 1034 (D.C. 2000) (disbarring attorney who conspired to launder drug trafficking proceeds); *In re Calhoun*, 492 S.E.2d 514 (Ga.1997) (disbarring attorney who participated in a scheme to launder proceeds of client's illicit drug business through the purchase of real estate); In re Berman, 769 P.2d 984 (Cal. 1989) (disbarring attorney who proposed scheme to undercover agents that would result in the laundering of money that would have been obtained through drug sales); In re Ciardelli, 514 N.E.2d 1006 (Ill. 1987) (three-year suspension of attorney who assisted a client in laundering proceeds of illegal activity by borrowing such proceeds for real estate purchase and who encouraged another attorney to do the same); In re Rech, 1995 Calif. Op. LEXIS 14, 3 Cal. State Bar Ct. Rptr. 310 (1995) (recommending disbarment of attorney who admitted to assisting his client in concealing drug proceeds through investments in two real estate ventures).

Applying R.17 to the DNFBP sector

977. The civil and criminal penalties outlined in the BSA and in FinCEN regulations are applicable to all "financial institutions" covered by the BSA and apply to any violations of the BSA and implementing regulations that meet the threshold requirements for imposition of those sanctions. However, since the broad implementing regulations have not been extended to any category of DNFBP, other than casinos and dealers in precious metals and stones sanctions may only be applied in relation to the customer identification and record-keeping requirements associated with the filing of Form 8300.

978. Under certain circumstances, businesses can be held criminally liable for the acts of their employees. Criminal penalties for violating a BSA requirement is a fine of up to USD 250,000 or a term of imprisonment of up to 5 years, or both. These penalties can be doubled if another federal law is violated or the illegal activity pattern exceeds USD 100,000 in a 12-month period.

979. IRS personnel conduct periodic examinations of non-bank financial institutions to assess their overall effectiveness in complying with these requirements. In instances of ineffective or unsuccessful BSA compliance procedures/program or when reporting and recordkeeping violations have occurred, IRS personnel prepare referral reports for FinCEN's disposition, including for consideration of civil money penalties or other sanctions. These reports to FinCEN are made based on referral guidelines established by FinCEN. If the examiner believes the conduct is criminal in nature, it is referred to IRS-CI for investigation.

Casinos

980. Examples of BSA deficiencies that would normally prompt an IRS casino referral to FinCEN or IRS-CI may include: (1) failure to maintain or implement an effective AML compliance program, including any requirement of that program; (2) failure to file suspicious activity report by casinos forms when required; (3) significant failures to file CTR by casinos forms; (4) notable deficiencies in procedures for verification of customer identity and related filing of incomplete CTR by casinos forms; and/or (5) failure to preserve required records. If IRS examination referrals do not warrant a civil money penalty FinCEN may take lesser action by sending the casino a cautionary or warning letter. Also, FinCEN may seek: (1) a permanent injunction against future violations of the BSA pursuant to 31 USC 5230; (2) civil money penalties of not more than the greater of the amount (not to exceed USD 100,000) involved in the transaction or pursuant to 31 USC 5231(a)(1) and 31 CFR 103.57(f); and (3) other appropriate relief. In addition, FinCEN may seek civil money penalties of USD 25 000 a day per violation of any compliance program requirement under 31 CFR 103.64(a), pursuant to 31 USC 5231(a)(1). These civil sanctions for willful violations of the BSA may be applied to any casino that is subject to the BSA, or to any partner, director, officer, or employee of such gaming operations.

Dealers in precious metals and stones

981. Until BSA obligations were extended to this sector, it was primarily unregulated. As these measures are only newly in force, the IRS has not yet started conducting compliance examinations of this sector.

Lawyers

982. Although lawyers in the U.S. are currently not required to implement any AML regimes or adhere to the BSA obligations, it is noted that they are regulated to the extent that they themselves might engage in money laundering activities. In many cases, state bar associations have authority for regulating, supervising, and monitoring lawyers for the purpose of ensuring that they adhere to the applicable standards of professional responsibility. Courts and legislatures have created attorney disciplinary agencies to investigate and prosecute alleged breaches of the professional conduct rules. In some jurisdictions, the highest court has delegated this function to the state bar association, but those courts retain ultimate responsibility and authority. Charges against attorneys are investigated

and prosecuted at a hearing if they are found to have merit. Hearing committees composed of other attorneys and members of the general public serve as fact finders—in effect, jurors. The committees' decisions are reviewed by the highest court of the jurisdiction or by a separate disciplinary review board, established for that purpose. In some jurisdictions, the decision not to prosecute a matter can be reviewed as well. If appropriate, the hearing committee may recommend sanctions against a lawyer, but generally it is the court that ultimately decides the sanction to be imposed, ranging from a reprimand to disbarment.

983. Individual state bar associations can be aware of cases involving lawyers who violate the state rules of professional conduct by engaging in money laundering activities or knowingly assisting a client in money laundering activities. Individual state bar associations prosecute them. These organizations, supported by their respective state supreme courts, or the state's equivalent courts, have sometimes disciplined attorneys who assist clients with money laundering or who launder funds themselves.[81] In disciplinary proceedings administered by state regulatory officials, even when criminal conduct is not proven, severe penalties authorized by the appropriate set of rules have been imposed where money laundering has been involved. State bar disciplinary proceedings for money laundering activity can go forward even when criminal charges have not been brought.[82]

Recommendation 25 (Guidance for DNFBPs other than guidance on SARs)

984. FinCEN and the federal functional regulators provide guidance in numerous ways and various forms to financial institutions subject to the BSA to assist those financial institutions in implementing and complying with BSA requirements. In addition to issuing regulations to implement the provisions of the BSA, FinCEN and the federal functional regulators issue technical bulletins, advisories, interpretive rulings and opinions, and a variety of publications, as well as maintaining websites with BSA information, guidance, regulations, statutes and forms. These have been described in detail in the financial sector part of this report, and, although they may not all be directly relevant to the DNFBPs, they offer general guidance.

Casinos

985. With respect to issuing guidance, in July 1998, FinCEN published an initial casino guidance document entitled "Suspicious Activity Reporting & Casinos". In August 2000, FinCEN issued a SAR Bulletin indicating the use of wire transfers and cashier's checks to deposit funds into casino accounts, with little or no gaming activity, followed by cashing out. In December 2003, FinCEN released new Suspicious Activity Reporting Guidance for Casinos that supplements the FinCEN Form 102, Suspicious Activity Report by Casinos and Card Clubs, instructions and explains how to prepare a complete and sufficient "Narrative". Also, FinCEN has issued extensive guidance to the MSB industry that can be found its websites.

986. FinCEN has also issued guidance to casinos concerning how they will be examined by the IRS for compliance with the obligation to implement an AML Program. The guidance document states that IRS's "...compliance examinations will look at the whether a casino's written program is designed to address the money laundering risks of your particular business, whether the casino and its

[81] *e.g. In re Lee*, 75 A.2d 1034 (D.C. 2000) (disbarring attorney who conspired to launder drug trafficking proceeds); *In re Calhoun*, 492 S.E.2d 514 (Ga.1997) (disbarring attorney who participated in a scheme to launder proceeds of client's illicit drug business through the purchase of real estate); In re Berman, 769 P.2d 984 (Cal. 1989) (disbarring attorney who proposed scheme to undercover agents that would result in the laundering of money that would have been obtained through drug sales); In re Ciardelli, 514 N.E.2d 1006 (Ill. 1987) (three-year suspension of attorney who assisted a client in laundering proceeds of illegal activity by borrowing such proceeds for real estate purchase and who encouraged another attorney to do the same); In re Rech, 1995 Calif. Op. LEXIS 14, 3 Cal. State Bar Ct. Rptr. 310 (1995) (recommending disbarment of attorney who admitted to assisting his client in concealing drug proceeds through investments in two real estate ventures).

[82] *e.g. In re Belgrad*, 1999 Ill. Atty. Reg. Disc. LEXIS 96 (1999) (recommending suspension of attorney who misappropriated USD 900 from a client trust account and tried to disguise the transaction by writing a check from the account to his law partner and having the partner write a USD 900 check to the attorney's personal account).

employees are following the program, whether employees are being properly trained, whether the program is being audited and the results of that audit, and whether the casino responds to red flags and other indicia that the compliance program is deficient" [Suspicious Activity Reporting Guidance for Casinos (December 2003, p.4)].

Dealers in precious metals and stones

987. The interim final rule which requires certain dealers in precious metals, stones, or jewels to establish an AML Program [70 FR 33702 (9 June 2005) (Interim Final Rule); 68 FR 8480 (21 February 2003) (NPRM)] contains a series of Frequently Asked Questions that are designed to assist dealers in determining whether they are subject to the rule and, if so, in establishing their AML Programs.

Lawyers

988. During the last six years, the organized bars in the U.S. have performed nearly 50 AML educational conferences. The speakers have included federal governmental officials and national and local bar leaders knowledgeable about AML matters. The conferences tend to focus on compliance issues as well as the impact AML laws have on various practice disciplines (such as banking law, trusts and estates law, corporate law, international law, and real estate law). The specific AML Program offerings tend to grow. Most states have continuing legal education requirements that legal professionals must comply with to remain entitled to practice law, many legal professionals will necessarily be exposed educational programs non specifically devoted to AML issues.

989. The ABA, the American College of Trusts and Estates Counsel ("ACTEC"), the American College of Real Estate Lawyers ("ACREL") and other state and local bar groups have all produced AML and CFT educational programs. The educational efforts are thus national in scope, thereby ensuring that legal professionals throughout the U.S. have access to these types of course and program offerings. The efforts also entail varying program delivery methods, including in-person programs, teleconferences, on-line programs, and study materials. The nature and content of such educational training needs to take into account the circumstances of individual legal professionals, in terms of their practice specialties, the risk of money laundering activity in their client representations, the existing ethical rules to which they are subject, their economic circumstances, and the institutional structure of their practice.

990. In addition to these educational programs, legal practitioners and academics have published articles on AML issues and their impact on the attorney-client privilege and the duty of client confidentiality. These articles have been published in local, regional, and national publications, some of which have significant circulation levels within the bar. For example, the article on the USA Patriot Act recently published in the "Real Property Probate & Trust Journal" reached over 30,000 practitioners in the U.S. This Journal has the second highest circulation level of any law review-style publication in the U.S.

Real estate agents

991. No specific guidance has been issued by the authorities to the real estate sector, but the real estate industry itself has taken steps to identify potential money laundering vulnerabilities. For instance, the American Land Title Association has identified several potential ''red flag'' situations involving real estate transactions, including:

(a) Where a prospective buyer is paying for real estate with funds from a high risk country, such as a ''non-cooperative country or territory'' as designated by the FATF or a country designated by the Treasury Secretary as ''a primary money laundering concern'' pursuant to Section 311 of the USA PATRIOT Act;

(b) Where the seller requests that the proceeds of a sale of real estate be sent to a high risk country;

(c) Where a person is seeking to purchase real estate in the name of a nominee and has no apparent legitimate explanation for the use of a nominee;

(d) Where a person is acting, or appears to be acting, as an agent for an undisclosed party and is reluctant or unwilling to provide information about the party or the reason for the agency relationship;

(e) Where a person does not appear to be sufficiently knowledgeable about the purpose or use of the real estate being purchased;

(f) Where the person appears to be buying and selling the same piece of real estate within a short period of time or is buying multiple pieces of real estate for no apparent legitimate purpose;

(g) Where the prospective purchaser or seller seeks to have the documents reflect something other than the true nature of the transaction; and

(h) Where the person provides suspicious documentation to verify his or her identity.

4.3.2 Recommendations and Comments

992. The regulatory regime applied to the casino sector generally appears to be working effectively. However, the work to further harmonize Nevada's regulatory requirements with the BSA should continue as rapidly as possible. Accountants, lawyers, real estate agents and TCSPs[83] should be made subject to AML/CFT obligations and appropriate regulatory oversight. In the case of TCSPs a registration process should be introduced for agents engaged in the business of providing company formation and related services (perhaps with a *de minimis* threshold to ensure that single company agents are not required to register). In view of the threat clearly identified in the latest U.S. threat assessment, work on addressing the TCSP issue should have a higher priority than appears to be the case currently (see discussion under section 5.1).

4.3.3 Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	PC	• There is no regulatory oversight for AML/CFT compliance for accountants, lawyers, real estate agents or TCSPs. • The supervisory regime for Nevada casinos is currently not harmonized with the BSA requirements.
R.25	C	• The Recommendation is fully observed.

4.4 Other non-financial businesses and professions

Modern secure transaction techniques (R.20)

4.4.1 Description and Analysis

Dealers in high value goods

993. In February 2003, FinCEN issued an advanced notice of proposed rulemaking (68 FR 8568) seeking public comment on a wide range of questions pertaining to imposing the AML and customer identification program requirements of the Bank Secrecy Act to businesses engaged in vehicle sales, including automobile, airplane, and boat sales, which are defined as "financial institutions" under the BSA. The NPRM also sought comment on the money laundering risks that are posed by these businesses, whether these businesses should be subject to these requirements, and if so, how the requirements should be structured. The business of vehicle sellers encompasses various segments,

[83] As indicated above, this relates only to TCSPs acting as company formation agents, since trust companies are already subject to the BSA requirements on the same basis as banks.

including sellers of: (1) new land-based vehicles, such as automobiles, trucks, recreational vehicles, and motorcycles; (2) new aircraft, including fixed wing airplanes and helicopters; (3) new boats and ships; and, (4) used vehicles (as well as those who broker the sale of used vehicles). There appears little likelihood that BSA obligations will be imposed on this sector in the foreseeable future.

Automated teller machines

994. While most ATMs are owned and/or controlled by regulated financial institutions, there is a growing industry in the leasing of such machines to non-financial businesses wishing to provide an incidental service to their customers. Typically, this might be in small convenience stores, shopping malls, bars or other locations where there is a volume of passing trade. Many of the ATMs are owned by large-scale operators, but it is also possible for then to be purchased outright by the businesses where they are located. In the majority of states there is no requirement to register ownership of ATMs and there is no oversight of their use.

995. Law enforcement and regulatory authorities in the U.S. have identified privately-owned ATMs as a material money laundering risk, particularly where the owner is directly responsible for replenishing the cash, rather than this being contracted out to a professional vault currency provider. They are also seen as posing particular risks of fraud and identity theft. The ATMs are linked to a transaction network which routes the data on customer withdrawals to the customer's bank (for debit to his/her account) and to the owner's account (for corresponding credit). Some, but not all, the transaction networks require an owner to be sponsored by a bank, and for such cases the banking regulators have specified due diligence standards that they expect to be followed in such circumstances (FFIEC Manual pp.126-128). However, these measures do not address all the risks, and law enforcement reports high levels of abuse in some parts of the U.S. U.S. authorities are now considering appropriate measures and control with respect to privately-owned ATMs. It is important that the authorities undertake further action, possibly with the objective of introducing a registration and monitoring system for the owners of ATMs.

Terrorist financing over the internet

996. The Treasury and DOJ have established a working group that focuses on terrorist financing on the Internet. In addition, recently, the U.S. presented a white paper to the FATF to address the need for countries to implement real measures to address, through regulation, these new payment methods and Internet cyber currency.

4.4.2 Recommendations and Comments

997. The authorities are engaged in considering the need to extend BSA requirements to a number of key areas, and this work should clearly proceed as quickly as possible. On the basis of comments by law enforcement, the money laundering risk appears to have been appropriately identified; however, insufficient AML/CFT measures been implemented to address the risk for these businesses, although they are subject to Form 8300 reporting under the BSA, as are all trades and businesses operating in the U.S.. The U.S. should take additional action to address this issue as soon as possible.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	C	• This Recommendation is fully observed.

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANIZATIONS

5.1 Legal Persons – Access to beneficial ownership and control information (R.33)

5.1.1 Description and Analysis

998. In preventing the use of legal person for illicit purposes, the U.S. government primarily relies on an investigatory approach.[84]

Federal laws

999. The U.S. uses a combination of the following mechanisms to comply with Recommendation 33:

(a) corporate reporting requirements.

(b) general purpose compulsory powers available to certain law enforcement, regulatory supervisors and judicial authorities during an investigation; and

(c) a tax registration system for employers administered through the issue of Employer Identification Numbers (EIN)

SEC corporate reporting requirements for publicly traded companies

1000. The U.S. imposes reporting requirements at the federal level for companies (both domestic and foreign) that offer securities to the public, or whose securities are listed on a U.S. stock exchange. These account for approximately 10,000 of the over 13 million active legal entities registered in the U.S.

1001. For the purposes of investor protection and fair dealing, Section 13(d)(1) of the Securities Exchange Act requires any person who acquires either directly or indirectly the beneficial ownership of more than 5% of a class of equity security, (required to be registered with the SEC), to file a statement with the SEC and the issuer of that security within 10 days of acquisition. The statement must disclose the identity and amount of shares held by the beneficial owner. Rule 13d-1 made pursuant to this provision sets out the detail of the reporting requirements. Section 13(d)(2) requires any material change to the statements to be reported with the SEC. These forms are required to be submitted electronically and are made available immediately, so the public will be able to search for a report.[85]

1002. There are further reporting requirements imposed on beneficial owners by the SEC which are aimed at the prevention of illegal insider trading. "Insiders" under section 16(a) of the Securities Exchange Act includes not only directors and officers of the issuer, but also any person who is the beneficial owner of more than 10% of any class of equity security (other than an exempted security[86]) that is registered under the Securities Exchange Act. Such persons must disclose their holdings to the company and are required to file certain statements, known as "insider reports", with the SEC. Within 10 days of becoming a reporting person (officer, director or 10% beneficial holder), the beneficial owner must file a statement (Form 3) of the amount of all equity securities in that issuer which is beneficially owned by that person. The person is required to file a further statement (Form 4) when

[84] This is Option 3 in the OECD paper entitled "Behind the Corporate Veil" (2001) (see p.83-88).

[85] Certain exemptions from the 10 day reporting rule are permitted for institutional funds where they were not acquired for takeover reasons [17 CFR 240.16a-1(a)(1)]. Those funds exempted from the 10 day rule are still required to file a statement with the SEC by the end of the calendar year if, at the time of filing that statement, the fund is still a beneficial owner of more than 5% of the class of equity shares. However, if the fund owns more than 10% of the class of equity securities at the end of any month, the fund must file the statement within 10 days of the end of the month [17 CFR 240.13d-1(b)(2)]. Further, while non-institutional holders of more than 5% but less than 20% of the class of equity security, and without takeover intent, must file a statement within 10 days of acquisition, such holders may file the same abbreviated statement as the exempt institutional funds [17 CFR 240.13d-1(c)].

[86] Rule 3a12-3 (17 CFR 240) provides that securities registered by a foreign private issuer are exempt from Section 16.

there is any change in such ownership[87] indicating any changes. "Ownership" is broadly defined to include either investment control and/or voting interest.

1003. Certain securities are exempt from registration and therefore exempt from these reporting requirements. Categories exempt from registration are: private offerings to a limited number of persons or institutions, offerings of a limited size, intrastate offerings and securities of municipal, State and Federal governments. Further, a company is not required to file reports with the SEC in the rare case that it "goes private", or reduces the number of its shareholders to fewer than 300.

1004. The DOJ and other federal law enforcement entities (including DEA, FBI, and ICE), in addition to the IRS, SEC and CFTC have general purpose compulsory powers enabling them to obtain beneficial ownership and control information for legal persons created in, or operating in, the U.S. These powers are triggered when illicit activity is suspected.

Compulsory powers available during an investigation

1005. In criminal matters, federal law enforcement entities can utilize judicial processes in obtaining records of beneficial ownership. Information is generally obtained through the use of the Grand Jury Subpoena. This type of process involves the assistance of the Assistant United States Attorney (AUSA) assigned to the investigation. The AUSA represents the Grand Jury and authorizes the issuance of the subpoena.[88] The agent will then "serve" the subpoena upon the recipient (bank, title company, business, a registered agent, individual, etc.). AUSAs may subpoena witnesses, compel the attendance and testimony of witnesses, and require the production of any records (including books, papers, documents, and other tangible things which constitute or contain evidence) which the Attorney General finds relevant or material to the investigation. The attendance of witnesses and the production of records may be required from any place in any State or in any territory or other place subject to the jurisdiction of the United States at any designated place of hearing. Depending upon the type of record requested the length of time from service to compliance can vary. In most instances there is compliance by a date specified on the subpoena. There are other types of judicial process that can be used to obtain records/testimony, but the most common is the subpoena. Compliance with the subpoena is compulsory and is subject only to the constitutional bar against self incrimination. The privilege against self-incrimination does not extend to legal persons or legal arrangements.

1006. As part of any federal criminal investigation, the prosecutor can also apply to a federal court for the issue of a search warrant to be executed upon a legal person. The Constitutional requirements of due process mean that courts cannot automatically issue a search warrant. Evidence on oath, usually by affidavit, that the legal burden of suspicion of a felony has been met, is required.

1007. In some select types of investigations law enforcement has administrative subpoena authority. The scope of this authority, preconditions to its use and who can exercise this authority will depend on the particular statute. Some statutes, such as the Internal Revenue Code, use the term "administrative summons" rather than "subpoena". As with a grand jury subpoena the administrative subpoena generally has a compliance date, records are then provided by that date by the recipient of the subpoena. If the statute permits, the administrative subpoena can be immediately issued at the first line investigative supervisory level without the need for a court order.

[87] Statements are also required where the owner purchased or sold any security based swap agreement involving the equity security.

[88] *Subpoena duces tecum* - A process by which the court, at the instances of a party, commands a witness who has in his possession or control some document or paper that is pertinent to the issues of a pending controversy, requires production of books, paper and other things. *Subpoena ad testificandum* - Subpoena to testify. A technical and descriptive term for the ordinary subpoena.

1008. The SEC's subpoena powers under section 21(b) of the Securities Exchange Commission Act enable it to compel the production of documents or testimony from any person or entity anywhere within the U.S. where the SEC has reason to believe there has been a violation of federal securities laws.

Employer identification number

1009. The IRS uses an Employer Identification Number (EIN) as an information tool to identify taxpayers that are required to file various business tax returns. Title 26 IRC 6109, requires any "person," including a legal person, who is required to file a return to include a prescribed identification number in order to properly identify that person. Treasury regulation 1.6109-1(a)(ii)(c states that any person other than an individual ("such as corporations, partnerships, non-profit organizations, trust estates and similar non-individual persons") must use an employee identification number as prescribed identification number for the purposes of Title 26 IRC 6109. Information contained in the application forms for EINs is used as a tool to identify potential taxable accounts of employers, sole proprietors, corporations, partnerships, estates, trusts, and other entities.

1010. A legal person or arrangement must apply to the IRS for an EIN if any one of the following conditions applies:

(a) it has employees;

(b) it has a qualified retirement plan;

(c) it files returns for employment taxes, excise taxes or income taxes;

(d) it opens a checking, saving or brokerage account or applies for a safe deposit box.

1011. Apart from their tax responsibilities, BSA regulations also require that all persons other than individuals (such as a corporation, partnership or trust) must provide an EIN or other taxpayer identification number when opening an account.[89]

1012. EINs are obtained by filing Form SS-4 with the IRS, which requires the following information about the entity:

(a) the legal name and mailing address of the entity;

(b) the name and social security number (or other tax identification number) of the principal officer, general partner, grantor, owner or trustor;

(c) type of entity, including the state in which it is incorporated (if the entity is a corporation);

(d) the date that the business was started; and

(e) the type of business activity.

1013. IRS officials confirmed that it is possible that a legal arrangement may not need an EIN and that such situations would be rare. However, it should be noted that it is a common typology that a corporation would be established to hold assets (e.g. real estate) which would not require the use of an account at a financial institution or the employment of personnel and, therefore, there would be no requirement under U.S. law to apply for an EIN.

1014. The U.S. describes the requirement for legal persons to apply for an EIN as a "starting point" for acquiring beneficial or controlling ownership of that legal person in that entities are required to provide certain information in the application form (Form SS-4) which is filed with the IRS. This includes the entity's legal and trade names, its mailing address and, depending on the type of entity, the name of either the principal officer, general partner, grantor, owner, or trustor, as well as any other

[89] 31 CFR 103.121(2)(iii).

tax identifier number of this person. The principal officer is the individual who is to be the contact person for the IRS. This person could be a manager, director, employee or agent acting on behalf of the legal person and, therefore, may not be an adequate, accurate and timely source of information on the beneficial ownership and control of the legal person.

1015. The concept of ownership under the EIN regime is different from the concept of beneficial ownership under the FATF Recommendations. This is demonstrated by the EIN rules relating to "change of ownership" in the legal entity. A new EIN is required when there is a "change of ownership" in these legal persons or arrangements. For U.S. federal tax purposes, change of ownership does not mean change in beneficial ownership, but rather a change in the type of taxable organization or a change in the location of the organization.[90] Where there is a change of beneficial ownership or control of the particular legal entity, but no change in the type of taxable organization, there is no requirement to apply for a new EIN.

1016. The IRS is invested with compulsory powers to verify that the information placed on an EIN application is accurate. The IRS has four compliance divisions that can verify EIN information during the course of the audits of the legal persons. The IRS advises that very few legal entities would be audited to ascertain the accuracy of information contained in the application for an EIN.[91]

1017. Federal law enforcement entities are able to share information both domestically and internationally through mechanisms described elsewhere in this report. However, IRS-CI can only share this information directly with law enforcement agencies when conducting a money laundering or terrorist financing investigation jointly with a criminal tax investigation. Where there is no criminal tax investigation (and therefore no IRS-CI involvement) law enforcement agencies do not have direct access to the IRS Form SS-4s or the information contained therein. In such cases, law enforcement agencies can obtain this information by requesting an *ex parte* order from a U.S. Judge.[92] EIN information placed on the application form to the IRS is not authorized to be disclosed by the IRS to AML/CTF regulators.

State laws

1018. The formation, operation and dissolution of U.S. corporations are governed mostly by state law. Corporations and other types of licensed business entities in any state in the U.S. are also subject to certain federal criminal laws, and corporate or other business activity suspected of being illegal under federal law is subject to investigation and enforcement under federal jurisdiction. The Model Business Corporation Act (MBCA) is a model act originally developed by the American Bar Association in the 1980's to encourage uniformity within the corporation laws of each U.S. state. The MBCA is only a guide for state governments, but most states have adopted significant portions of the MBCA for their corporate laws. The corporate laws in each state have evolved quite differently, with some states promoting the concept of establishing corporations within the state for the purpose of conducting business outside the state.

1019. Ordinarily, forming a corporation is a simple process, much of which may be performed by a competent legal secretary. The actual mechanics of creating a corporation vary from state to state, although they are usually quite similar. Every state requires the filing of a corporate governance document (called the "articles of incorporation, "certificate of incorporation," or "charter") with a state official (usually the Secretary of State) together with the payment of a filing fee. The Office of the

[90] A trust becomes a corporation; an unincorporated association becomes a corporation; a corporation reincorporates in another state; a state corporation reincorporates under an Act of Congress; an individual/sole proprietor changes to a partnership; an individual/sole proprietor changes to a corporation; or a corporation becomes a partnership.

[91] Once a criminal investigation has commenced, IRS-CI will also become involved. During the course of a criminal investigation, IRS-CI can use an administrative summons, or a grand jury subpoena, or apply for a search warrant to compel the receipt of the records to prove true ownership of a legal person.

[92] 26 USC 6103(i).

Secretary of State reviews each filing to ensure that it meets the state's statutory requirements; however, the information contained in the filing is generally not verified. Thirteen states have additional filing requirements. Delaware, for example, requires local filing in the county in which the corporation's registered office is located in addition to filing in the state office. Twelve states, including Arizona, require that evidence be submitted that the statutory agent has accepted his/her appointment. Arizona, Georgia and Pennsylvania also require publication of the entity's formation by way of a notice in a local newspaper.

1020. The articles of incorporation must, generally, set forth the following information: (1) the name of the proposed corporation; (2) the period of its duration; (3) the purpose for its formation (a requirement which, in some states, may be satisfied by the very general statement of "for any lawful purpose"); (4) the amount of capital stock; (5) the address of the corporate office or place of business, and the name of its registered agent; (6) the number and names of the founding board of directors (who may, in some cases, only serve until the first annual shareholders meeting); and, (7) the names and addresses of the incorporator(s). All states provide that the incorporators must sign the articles of incorporation, and their signatures must, ordinarily, be verified. Additionally, some states require that duplicate originals of the articles of incorporation be filed with the secretary of state.[93]

1021. All states require that every corporation maintain a registered office within the state and a registered/statutory agent at that office. The registered office may, but need not be, the corporation's business office. One of the primary purposes of the requirements for a registered office and registered agent are to provide an agent for service of process and a place of delivery for legal/tax notices and other official communications. The original registered office and registered agent is specified in the articles of incorporation; if either is changed thereafter a statement describing the change must be filed with the secretary of state. Many attorneys suggest that they be designated as the registered agent and their office be designated as the registered office.

1022. The following case studies describe the situation in the states of Delaware and Nevada. The assessment team focused on these particular states since they actively promote the establishment of corporations by non-residents.

A Case Study – Delaware

Delaware is one of the leading states within the U.S. for the incorporation of business entities. There are currently some 695,000 active entities registered in Delaware, including approximately 50% of the corporations publicly traded on the U.S. stock exchanges. The state is considered to be particularly attractive for the undertaking of mergers and acquisitions. New business formations are currently running at about 130,000 per annum, with the majority being established in the form of "alternative entities" (i.e. non-traditional corporations). Many are formed for the purposes of a single transaction (e.g. structured finance), upon the completion of which the company may typically be allowed to lapse. Also, Delaware entities are widely used for asset protection purposes by private individuals. Possible legal structures include Stock Corporations, Non-Stock Corporations, Close Corporations, Foreign Corporations, Limited Liability Companies, Foreign Limited Liability Companies, General Partnerships, Foreign Partnerships,

[93] Subsequent to the on-site visits, in April 2006, the Government Accountability Office (GAO) published a document entitled "Company Formations: Minimal Ownership Information is Collected and Available" which states that "Most states do not require ownership information at the time a company is formed, and while most states require corporations and LLCs to file annual or biennial reports, few states require ownership information on these reports. Similarly, only a handful of states mandate that companies list the names of company managers on formation documents, although many require managers' information on periodic reports. States may require other types of information on company formation documents, but typically they do not ask for more than the name of the company and the name and address of the agent for service of process (where legal notices for the company should be sent). Most states conduct a cursory review of the information submitted on these filings, but none of the states verify the identities of company officials or screen names against federal criminal records or watch lists".

Statutory Trusts, Foreign Statutory Trusts, Limited Partnerships and Foreign Limited Partnerships.

The primary reasons commonly given for Delaware's popularity are that:

(a) Delaware's laws governing corporations, limited liability companies, limited partnerships and statutory trusts are among the most advanced and flexible laws in the nation.

(b) Jurisdiction over most questions arising under Delaware's corporation, limited liability company, statutory trust and partnership laws is vested in the Delaware Court of Chancery, which has developed over 200 years of legal precedent in corporation and business law, and is noted for its sophistication and its mediation between the rights of investors and managers.

(c) The Delaware State Legislature seeks routinely (on an annual basis) to update its laws, while maintaining a stable core.

Key Delaware corporate and other business legislation includes: the General Corporation Law, Revised Uniform Partnership Act, Limited Partnership Act, and Limited Liability Company Act. The concept of the Limited Liability Company (LLC) was first created in 1992, and since then it has become the vehicle of choice for the majority of businesses wishing to establish a Delaware entity. One of its primary attractions is the ability to combine a tax treatment similar to that of a partnership with the limited liability of a corporate structure. However, another key feature is that the LLC can dispense with most of the common trappings of a corporation (e.g. board meetings, minutes, etc), with the relationship between the shareholders and the management typically being defined in a written LLC agreement, and not in statute except for certain default rules that apply in the absence of an agreement.

The vast majority of Delaware corporations and LLCs are established by non-residents in order to do business outside the state. The only territorial obligation is that all entities must have a physical registered address within the State of Delaware for the service of process. Typically, such an address is provided by a registered agent (see below), many of whom cite as a particular attraction the fact that entities can be established without the principals having to go to Delaware. Incorporation is routinely possible within 24 hours, and the Delaware Division of Corporations offers a one-hour service on demand.

All information held on the corporate registry is available to the public. However, there is no obligation to file the name of any shareholder or beneficial owner when establishing either a corporation or an LLC. Section 102 of the General Corporation Law requires such information in principle, but notes that "if the powers of the incorporator or incorporators are to terminate upon the filing of the certificate of incorporation, the names and mailing addresses of the persons who are to serve as the directors until the first annual meeting of the stockholders or until their successors are elected" should be supplied. The initial directors may simply be appointees by the registered agents. Section 219 provides that a list of the stockholders eligible to vote must be drawn up by the company ten days before any meeting of the stockholders, but the substantial case law on the relative rights of nominee stockholders and beneficial owners clearly shows that the practice of using nominees is not unusual and is common practice in the United States where mutual funds hold a large percentage of all publicly-held stock. Bearer shares are expressly prohibited by section 158 of the Law.

In the case of LLCs there are no requirements to file the names of either the managers or members at formation. Section 18-201 of the Limited Liability Company Act requires the submission only of the name of the company, the registered address and "any other matters the members determine to include therein" (i.e. disclosure is entirely voluntary). Other features of both corporations and LLC are:

(a) one person can be the sole director and officer of a corporation or the sole member and manager of a LLC;

(b) shareholders can act in writing rather than holding meetings;

(c) records need not be kept in the state of Delaware; and

(d) no obligations are imposed on registered agents with respect to customer identification or record-keeping.

As a result of the requirement to maintain a physical address in the state, anyone from out of state wishing to establish a Delaware corporation must use the services of a registered agent to provide the appropriate address. Section 132 of the General Corporation Law provides that the registered agent may, among others, be an individual resident in the state, a corporation, a limited partnership, a limited liability company or a statutory trust. At present some 30,000 natural persons, professional service providers or companies offer this service in Delaware, although the vast majority are dedicated agents representing just one company. Approximately 240 formation agents represent more than 50 companies each. Delaware offers a special one-hour service for registration, when a registered agent facilitates formation.

The role of the agent may range from fulfilling the minimal legal requirements of maintaining a physical presence in the State of Delaware for service of process, including subpoenas, to a much broader range of client services. The degree of knowledge that the agent might have of its client will, therefore, vary significantly. There is no legal obligation to verify the identify of the customer, and in cases where the ultimate customer may be a private individual, it would typically be the case that the agent would deal with an intermediary, such as an attorney or other professional adviser. As a matter of business practice, the agent would seek to maintain three contact points, one for onward service of process, one for tax affairs, and one for the billing of fees (who could be one and the same person).

There are currently no controls imposed on the majority of registered agents. The limited exception is for those agents who wish to have access to online incorporation facility. In order to be considered for such access (which facilitates, but is not a necessary pre-requisite, for using the one-hour and other expedited filing services), an agent simply has to meet certain performance criteria. Specifically, he/she must have been actively involved in the business of providing registered agents services for at least one year, he/she must hold a deposit account with the Division of Corporations, and he/she must enter into a standard contractual arrangement with the Division. Registered agents with online access do facilitate the overwhelming majority of all Delaware business formations.

The Delaware state authorities are conscious of the potential reputational damage that can be caused by unscrupulous or incompetent registered agents, and are considering introducing amendments to Section 132 to impose some degree of regulation over their activities. This might involve defining the role of the agent relative to the service of process, requiring agents to retain client contact information including the name, business address and phone number of a natural person who is a director, officer, employee or designated agent of the company, and requiring a Delaware business license. Legislation may also provide for some sanctions for agents who consistently fail to meet their obligations or have been convicted of a felony or engaged in practices intended or likely to deceive or defraud the public, including the possibility of the authorities making an application to the Court of Chancery to have an agent closed down. There is no proposal to extend a broader regulatory regime to this sector, or to require registered agents to adopt due diligence standards with respect to their clients.

In many respects, registered agents in Delaware are in competition for business with TCSPs operating in traditional offshore financial centers (OFCs). The style of advertising by many tends to portray an image that the standards of secrecy offered are greater than those in most OFCs. For example, one internet site, when talking of the attraction of Delaware for non-resident aliens, states:

> "To our many international clients, anonymity is important. Many of our clients select single-member Delaware LLCs as one component of their asset protection strategy. The Delaware LLC provides the anonymity that most international jurisdictions do not offer. As a Delaware Registered Agent, (name of company) is NOT required to keep any information on the beneficial owner, and the State of Delaware does NOT require that the beneficial owner is disclosed."

In terms of seeking to acquire information on the ownership and control of state-registered entities, the

law enforcement and regulatory authorities in Delaware have a range of investigative powers including subpoena powers when fraud or other illegal activity is suspected. Delaware's authority, as a state, does not extend beyond the state borders except through the exercise of statutorily provided long-arm jurisdiction, and, given the very limited amount of information that might typically be held within the state with respect to the owners and activities of the majority of Delaware-incorporated entities, these investigative powers on their own would appear to be encumbered by the process of exercising such jurisdiction in order to trace beneficial ownership. It is possible, as previously described, for federal law enforcement agents to access beneficial ownership information regarding a Delaware corporate vehicle or other business formation through parallel jurisdiction when a federal offense is suspected.

A Case Study – Nevada

In recent years, Nevada has sought to mount a challenge to Delaware as the favored location for incorporation by out-of-state residents. It currently has approximately 280,000 active business entities registered with the Division of Corporations, with 80,000 to 85,000 new registrations each year. About 30,000 entities fail to renew their registration each year, suggesting that many are established for one-off transactions. The establishment of LLCs has been available in Nevada since the early-1990s, and they currently account for about 50% of new registrations.

About 20% of the registrations are completed by residents of Nevada, in part reflecting the fact that Las Vegas has one of the country's highest population growth rates. However, a significant proportion (about 40%) of the registrations emanate from persons in California, with the other 40% largely spread around the other states within the U.S. California provides a major source of business because of its geographical proximity, its high rate of taxation, and the sheer size of its economy. There is reported to have been a dramatic decline in the number of registrations on behalf of non-U.S. persons since the introduction of the USA PATRIOT Act.

The primary advantages commonly cited for registration in Nevada are:

(a) the absence of any state corporation tax;

(b) the absence of an information sharing agreement with the IRS;

(c) one person can hold all corporate positions;

(d) minimal filing requirements, both on initial registration and annually thereafter; and

(e) a high degree of privacy offered by these filing requirements.

More generally, Nevada is also seen to offer better indemnification to officers and directors than any other state. This, together with the tax advantages associated particularly with the LLC structure, make Nevada favored as a jurisdiction for holding assets. Delaware law, by contrast, has a tradition of being more conducive to the interests of investors, and is, therefore, more widely used as a base for raising capital. A significant proportion of Nevada registrations are on behalf of private individuals, rather than established corporations.

The process for the registration of a corporate or other entity is not onerous. Where it does not physically conduct business in the state, each entity must appoint a resident agent in Nevada, and submit to the Division of Corporations a form containing the name and address of the agent, the number of shares and their par value, the name of the incorporators, and a letter from the resident agent accepting his/her appointment. Within two months of registration, the entity must also file the names of the president, secretary and treasurer. Thereafter, an annual filing containing the names of the officers is required. Nevada does not offer a "fast track" incorporation process, and all filings (which subsequently become available to the public) are currently made by physical documentation. There is no requirement at any stage to file the name of the beneficial owners or controllers, and the names of the incorporators and

officers submitted to the Division of Corporations may be those of the agents or other nominees. In the case of an LLC, if the entity appoints a manager, there is no requirement to include the names of the managing members (i.e. the owners) on the annual filing. There is no obligation imposed on the agents to know, or to maintain records of, the beneficial owner.

Nevada is one of only two states in the U.S. where bearer shares are not prohibited (the other being Wyoming), although there has been speculation that a bill will shortly be introduced to the state legislature to outlaw them. However, the authorities and agents have reported that the use of bearer shares by investors is extremely limited, probably due to the fact that they offer no particular advantage over registered shares, which have minimal filing requirements, and as bearer instruments, pose a risk of loss.

The Division of Corporations has no authority to refuse a filing provided that it is completed correctly, that the name selected for the entity does not replicate that of an existing entity, and that it does not use a term that is given statutory protection under state regulatory laws (e.g. bank, trust, insurance, etc). The Division does not verify the accuracy of the information contained in the filing. The Division has no investigatory powers in relation to any of the registered entities, and any concerns that it may have, including potential fraudulent filing of documents, must be passed to the Attorney General or the district attorney for investigation.

In 2003 provisions were introduced requiring all corporations to apply for a business license from the Department of Taxation. The application form for the license asks for details of the beneficial owners. However, in 2005 an amendment was adopted that limited the obligation to entities "providing service or conducting business for profit" in Nevada. This amendment was introduced specifically to take outside the scope of the process all private investment, asset holding or similar vehicles that do not conduct a physical business in Nevada. To date, only about 50% of the affected corporations have made the requisite filings. In addition, the accuracy of the information contained in the filing is not verified. The information in the possession of the Department of Taxation is protected by privacy laws, and it may only be accessed by law enforcement under a grand jury subpoena, supported by a Governor's Order.

As in the case of Delaware, the statutory role of the resident agents is to provide an address for service of notice, but they will usually also provide services relating to the submission of the initial registration, and to any subsequent routine filings. The function may be provided by any person (individual or corporate) that has a physical presence in the state, but in most cases it is performed by professional agents. For example, the Resident Agents Association has as its membership 40 firms that, between them, represent approximately 50,000 registered companies. There is no obligation on the agents to identify the beneficial owner of the entities for which they act, and an attempt in recent years to require disclosure of beneficial ownership by the registered agents without a proper court order (i.e. a subpoena) did not pass through the legislature. By law the agents must either hold the entities' stock register at the registered address, or maintain a record of where the register is held. In many cases, the register is held outside the state, and there is no restriction on the use of nominee shareholders. Bearer shares are also permitted. Of particular note is that many of the service provider websites advertise their ability to open bank accounts within the state on behalf of the client corporation.

The resident agents are not subject to any form of regulatory oversight, and proposals in the past to introduce a regulatory framework in Nevada have been deflected under pressure from the agents.

Summary of state issues

1023. The activities of the TCSPs are clearly instrumental in the rapid growth of company formation in these states. While the use of the states (Delaware, in particular) for capital formation by quoted companies will be transparent through the SEC and exchange disclosure requirements, reliable information on the identity of individuals for whom the very large number of private investment vehicles are being formed is held, at best, with the TCSPs. In many cases, such information, or its location, may be unknown even to the TCSPs. While many agents will undoubtedly wish to identify

their clients for their own business reasons (e.g. reputation risk, assurances on fee payments), it is clear that others are actively marketing the states as locations where anonymity can be assured.

1024. In its threat assessment published in January 2006, the U.S. authorities have highlighted the risks posed by the incorporation arrangements in states such as Delaware, Nevada and Wyoming. Some of the conclusions in this assessment are very stark, e.g.

> "The FBI has found that certain nominee incorporation services (NIS) form corporate entities, open full-service bank accounts for those entities, and act as the registered agent to accept service of legal process on behalf of those entities in a jurisdiction in which the entities have no physical presence. An NIS can accomplish this without ever having to identify beneficial ownership on company formation, registration, or bank account documents. The FBI believes that U.S. shell companies and bank accounts arranged by certain NIS firms are being used to launder as much as USD 36 billion a year from the former Soviet Union. It is not clear whether these NIS firms are complicit in the money laundering abuse.
>
> Several international NIS firms have formed partnerships or marketing alliances with U.S. banks to offer financial services such as Internet banking and wire transfer capabilities to shell companies and non-U.S. citizens. The FBI reports that the U.S. banks participating in these marketing alliances open accounts through intermediaries without requiring the actual account holder's physical presence, accepting by mail copies of passport photos, utility bills, and other identifying information.
>
> FinCEN reports that 397 SARs were filed between April 1996 and January 2004 involving shell companies, Eastern European countries, and the use of correspondent bank accounts. The aggregate violation amount reported in those 397 SARs totaled almost USD 4 billion.
>
> The State of New York Banking Department recently noted that Suspicious Activity Reports filed by New York banks indicate an increase in the volume of shell company wire transfer activity through high-risk correspondent bank accounts, both in terms of dollar amounts and the number of transactions. These reports indicate that money is passing through correspondent accounts established for Eastern European banks."

1025. FinCEN has indicated that in the longer term it will be mounting a three-pronged program to raise awareness further. First, this will involve an advisory to banks, highlighting the threat assessment and specifying the type of questions that it would expect banks to be asking when dealing with certain types of corporate customer. Second (possibly before the end of 2006), it plans to issue the long awaited notice of proposed rulemaking with respect to CIP requirements for company formation agents. Third, it will engage in an immediate outreach program to the key states to encourage them to legislate for greater transparency of ownership of corporate entities. However, with respect to the third objective, FinCEN recognizes that the federal government has no authority to force the states to amend their domestic legislation, and must, therefore, rely on their goodwill.

1026. In discussions with the state authorities, it was clear that there was a realization of the threats posed by the current "light-touch" incorporation procedures, including the failure to obtain meaningful information on individuals who effectively control the entities. However, the states primarily see this activity as a revenue-raising enterprise to substitute in part for their partial tax-free environment, and the company formation agents represent a powerful lobby to protect the status quo. Therefore, any proposals to enhance the disclosure requirements have not progressed, with defenders of the status quo arguing that, since the money laundering threat only crystallizes when the company gains access to the financial system, an effective safeguard should already exist in the form of the institutions' CDD obligations.

Bearer Shares

1027. The issue of bearer shares is prohibited in all States and Territories in the U.S. apart from Nevada and Wyoming. Website searches reveal a level of promotion of trading in these instruments in these States. As discussed, the Corporations Division in Nevada advised, however, that they were not aware of any trading in bearer shares in that state. This was separately confirmed by legal practitioners in that jurisdiction. There are no State laws regulating the issue of bearer shares in either state and in particular there are no systems to ensure that information regarding beneficial or control ownership is available.

5.1.2 Recommendations and Comments

1028. The U.S. relies on a combination of systems and measures to satisfy the requirements for access by authorities to accurate and current information on the beneficial ownership and control of legal persons upon suspicion in order to investigate money laundering. At both the federal and state level there is a range of investigatory powers available to law enforcement and certain regulators to compel the disclosure of ownership information. It is acknowledged that these are generally sound and widely used. However, the system is only as good as the information that is available to be acquired. In the case of companies that do not offer securities to the public or whose securities are not listed on a U.S. stock exchange, the information available within the jurisdiction is often minimal with respect to beneficial ownership. In the case of the states visited, the company formation procedures and reporting requirements are such that the information on beneficial ownership may not be adequate and accurate, and competent authorities would not be able to access this information in a timely fashion.

1029. It is recommended that the U.S. authorities undertake a comprehensive review to determine ways in which adequate and accurate information on beneficial ownership may be available on a timely basis to law enforcement authorities for companies which do not offer securities to the public or whose securities are not listed on a recognized U.S. stock exchange. It is important that this information be available across all states as uniformly as possible. It is further recommended that the federal government seek to work with the states to devise procedures which should be adopted by all individual states to avoid the risk of arbitrage between jurisdictions. As the January 2006 threat assessment indicates, the U.S. authorities are well aware of the problems created by company formation arrangements, and have formulated an initial program to try to address the issue. This should be pursued in a shorter timescale than seems to be envisaged at present. In particular, the proposal to bring company formation agents within the BSA framework, and to require them to implement AML Programs and CIP procedures should be taken forward in the very near future.

5.1.3 Compliance with Recommendations 33

	Rating	Summary of factors underlying rating
R.33	NC	• While the investigative powers are generally sound and widely used, there are no measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities.. • There are no measures taken by those jurisdictions which permit the issue of bearer shares to ensure that bearer shares are not misused for money laundering.

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

1030. In the U.S. a trust is a legal entity that is created under state law. The IRS retains oversight of income generated by trusts through federal tax laws.

1031. Virtually all U.S. state jurisdictions recognizing trusts have purposely chosen not to regulate trusts like other corporate vehicles. The U.S. authorities confirm that this is because in the U.S. a trust is essentially a contractual agreement between two private persons. This means that, unlike corporations, there are no registration requirements, other than tax filing requirements imposed on trusts by the IRS. Trusts are subject to the same general investigative powers exercised by those regulators and law enforcement agencies as discussed in Section 5.1, beneficiaries have some corporate reporting requirements under the Securities Exchange Act, and trusts also have obligations to apply for an EIN.

IRS Filing Requirements

1032. For U.S. federal tax purposes, there are three types of trusts:

(a) **Simple Trust:** A trust that requires that all income be distributed currently, with no authority to make charitable contributions or permanently set aside any amount for charitable purposes. A trust can be a simple trust only for a year during which it distributes income and makes no other distributions to beneficiaries. After a year, or when the trust does not otherwise meet these requirements, it is a "complex trust."

(b) **Complex Trust:** A trust that does not qualify as a "simple trust" for a taxable year.

(c) **Grantor Trust:** A trust that is set up by a living individual or an organization of which the grantor or some other person is treated as the owner of the trust, so that the income of the trust is taxable income of the owner.

1033. The trustee of a trust is a fiduciary. A beneficiary is a person to or for whom distributions from the trust may be made; the term “beneficiary” may also include an ultimate recipient of the assets remaining in the trust at its termination. The *corpus* or *res* is the principal sum or capital of a trust, as distinguished from interest or income. The settlor or grantor is the person(s) or organization(s) who created and/or funded the trust

1034. Under federal tax law, to the extent the trust is not a grantor trust, the tax on income generated by the trust property is payable by the trust, and/or by one or more of the beneficiaries. This tax serves as a check on the validity of financial transfers via a private trust. Trusts may not be used to transform a taxpayer's personal, living, or educational expenses into deductible items, or to avoid tax liability by ignoring either the true ownership of income or assets or the substance of the transactions. Therefore, the tax results promised by the promoters of abusive trust arrangements that hide illicit transactions are not allowed under U.S. law, and the participants and promoters of these arrangements may be subject to civil or criminal penalties.

1035. The income of a trust is required to be reported via IRS Form 1041.[94] These returns are required to include the name and taxpayer identification number of each beneficiary deemed to have received a distribution from the trust for that year, as well as the amount to be reported as income by that beneficiary. The taxation of trusts’ income through the filing of Form 1041 allows the IRS to track the earnings and wealth transfers to and from beneficiaries. Under U.S. law the relevant forms filed with the IRS by the trust detail any distributions of income to the beneficiaries, including the identifying information about the beneficiary, such as name, address, and identifying number. For grantor trusts, this income and the deductions and credits are not reported on IRS Form 1041 return, but are shown on a separate statement which is attached to IRS Form 1041 return; that information is then reported on the grantor’s own income tax return. Individual beneficiaries must report on their individual income tax returns for that year their share of the trust’s distributable net income, if any, as shown on the trust’s return. The filing of individual income tax returns by beneficiaries also allows

[94] Charitable trusts are also required to file tax return information with the IRS. Donors of gifts to the trust must file gift tax returns.

the IRS to monitor some transactions into, and out of, a taxable trust. The IRS can audit the filer and serve administrative subpoenas on the beneficiaries and the preparer.

Investigative Powers

1036. As discussed in Section 5.1, the SEC's subpoena powers under section 21(b) of the Securities Exchange Commission Act enable it to compel the production of documents or testimony from any person or entity anywhere within the U.S. where the SEC has reason to believe there has been a violation of federal securities laws. This includes the ability to compel the production of a trust document and the ability to compel testimony from parties to the trusts that are located in the U.S.

1037. As with legal persons the DOJ and other law enforcement entities, through the use of administrative or grand jury subpoenas, can also compel the production of documents or testimony from parties to a trust subject to the Constitutional bar to self-incrimination.

Employee Identification Number

1038. Although trusts (apart from grantor trusts) are required to apply for an EIN by filing Form SS-4 with the IRS the trust is only required to provide the name of the principal officer or the trustor (i.e. settlor or grantor) and the trustee. There is no requirement to identify any beneficiary on this form.

SEC Corporate Reporting Requirements

1039. Trusts are subject to the reporting requirements of section 16 of the Securities Exchange Act if the trust is a beneficial owner of more than 10% of any class of equity securities.[95] A trust beneficiary who is a section 16 insider[96] must report a trust transaction in issuer securities in which he or she has a pecuniary interest if the beneficiary has investment control with respect to the trust transaction or shares that investment control with the trustee.[97] A settlor who is a section 16 insider who reserves the right to revoke the trust without the consent of another is required to report trust transactions in issuer securities, unless the settler does not exercise or share investment control over the issuer securities held by the trust.[98] This reporting requirement, however, is subject to the same qualifications discussed in Section 5.1 which notes that these forms are publicly available and forms that are submitted electronically are made available immediately.

5.2.2 Recommendations and Comments

1040. The U.S. relies on a combination of systems and measures to satisfy the requirements for access by authorities to accurate and current information on the beneficial ownership and control of trusts. This includes the investigatory powers available in respect of legal persons. It is acknowledged that the investigatory powers are generally sound and widely used. However, the system is only as good as the information that is available to be acquired. In the case of trusts, the information available within the jurisdiction can often be minimal with respect to beneficial ownership.

1041. Under U.S. law, the IRS has access to beneficial owner information when distributions are made to the beneficiary or income is earned by the trust. However, the IRS-CI can only share this information with law enforcement agencies in the course of an on-going investigation that has criminal tax implications. Where there are no criminal tax implications, law enforcement agencies can only access the information by obtaining an *ex parte* order from a U.S. judge. The U.S. should implement

[95] 17 CFR 240.16a-8(a)(1).

[96] See section 5.1 of this report.

[97] 17 CFR 240.16a-8(a)(3).

[98] 17 CFR 240.16a-8(a)(4).

measures to ensure that adequate, accurate and timely information is available to law enforcement authorities concerning the beneficial ownership and control of trusts.

5.2.3 Compliance with Recommendations 34

	Rating	Summary of factors underlying rating
R.34	NC	• While the investigative powers are generally sound and widely used, there is minimal information concerning the beneficial owners of trusts that can be obtained or accessed by the competent authorities in a timely fashion.

5.3 Non-profit organizations (SR.VIII)

5.3.1 Description and Analysis

1042. The FATF issued an Interpretative Note to Special Recommendation VIII (INSR VIII) about a month after the last on-site visit of the U.S. Nevertheless, the U.S. has agreed to be evaluated on its compliance with Special Recommendation VIII, taking into account the new INSR VIII. It should be noted, however, that the methodology criteria for INSR VIII have not yet been agreed by the FATF.

1043. Statistics provided on the NPO sector were based on data kept by the IRS. According to the IRS the sector consists of nearly one million public charities and private foundations. There are also approximately 350,000 churches or smaller public charities which are exempt from applying to the IRS. The IRS estimates that the charitable sector controls approximately USD 3 trillion in assets. Overall, these tax-exempt organizations form an important part of the U.S. economy, employing about one of every four workers in the U.S., and represent a significant portion of the financial resources under control of the NPO sector and a substantial share of the sector's international activities.

Review of the NPO sector

1044. Under U.S. law, any person or group may establish a charitable organization, and the creators of the organization are free to choose any charitable endeavor they wish to pursue. The U.S. has conducted a number of internal reviews of its domestic charitable sector.[99]

1045. In the review of its non-profit sector, the U.S. identified the following terrorist financing related risks:

(a) Charities most vulnerable to terrorist financing abuse, or those established, at least in part, to facilitate terrorist financing, naturally focus their relief efforts on areas of conflict, which tend to also be prime locations for terrorist networks. Charities provide excellent cover for the movement of money, personnel, and even military supplies to and from high-risk areas.

(b) Unlike the funds or assets of for-profit commercial organizations, charitable funds and assets are usually meant to move in one direction only; accordingly, large charitable transfers do not raise suspicion merely because there is no corresponding return or transfer of value.

(c) Charities attract large numbers of unwitting donors along with the witting, thus increasing the amount of money available to terrorists, and the attractiveness of charities to raise and move funds in support of terrorist-related activities.

(d) Many of these charities engage in the legitimate delivery of aid to needy beneficiaries through legitimate activities, such as the operation of schools, religious institutions, and hospitals, which

[99] The U.S. presented the results of one review to the FATF Working Group on Terrorist Financing in a paper entitled, "Terrorist Financing and the U.S. Charitable Sector: A U.S. Discussion Paper for the FATF Working Group on Terrorist Financing."

provide necessary cover and create fertile recruitment grounds, allowing terrorists to generate support for their causes and to propagate extremist ideologies.

(e) The provision of genuine relief affords these charities vast public support and an attendant disinclination by many governments to take enforcement action against them, particularly when aid is being delivered in areas where they are the only provider of assistance.

1046. In light of these factors and the immense size of its domestic charitable sector, the U.S. has concluded that it is important to develop a strategy that maximizes limited resources through a coordinated risk-based approach to examining and investigating suspected cases of terrorist abuse within the charitable sector, and targeting enforcement action accordingly.

Identifying, preventing and combating terrorist misuse of NPOs

1047. In developing its strategy to combat terrorist financing in the charitable sector, the U.S. has focused on the investigatory and enforcement powers afforded to numerous authorities. The U.S. has adopted a four-pronged approach to identify, prevent and combat the terrorist misuse of non-profit organizations (NPOs). This approach involves: (1) outreach to the NPO sector; (2) coordinated oversight, supervision or monitoring; (3) information gathering, investigation, designation, and prosecution; and (4) mechanisms for international cooperation.

Outreach to the NPO sector concerning terrorist financing issues

1048. The U.S. has undertaken an outreach program to raise awareness in the NPO sector about the vulnerabilities of NPOs to terrorist abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse. In November 2002, the Treasury Department released "Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities." This document includes measures set out in the Best Practices Paper for SRVIII. In addition to providing practical best practices that NPOs should apply to protect against terrorist abuse, these Guidelines serve to raise awareness of the risks of terrorist financing abuse in a sector that previously had not recognized the seriousness of the threat.[100]

1049. Following consultations with the sector, a working group primarily comprised of international grant-makers and service delivery groups as well as some nonprofit sector organizations was formed in April 2004 regarding replacement Guidelines. Treasury worked with the NPO sector to refine the Guidelines with a view to more effectively protecting the sector from terrorist abuse. On 5 December Treasury released a revised version of the November 2002 Guidelines seeking public comment by 1 February 2006. Treasury's ongoing discussion and debate with the NPO sector in settling these Guidelines demonstrates a high level of engagement with the NPO sector.

1050. The Guidelines are provided as a tool to help guide charities to better protect themselves from potential terrorist financing abuses, where the risk of such abuse is identified. They would appear to promote transparency, integrity and public confidence in the administration and management of all NPOs. In particular, the Guidelines encourage NPOs to conduct transactions via regulated financial channels (e.g. making disbursements by wire transfer or check) wherever feasible, keeping in mind that normal financial services may not always exist or other exigencies require making disbursement in currency (as in the case of humanitarian assistance being provided in developing countries). They also encourage NPOs to enact and practice sound governance and fiscal policies, which includes detailed record-keeping, as well as to collect information on and vet key employees, members of the governing body, and potential grantees. There is also guidance on the adoption of specific practices

[100] The Guidelines also led to a strong engagement with the American-Muslim NPO community, which often faces heightened risks due to the high-risk regions in which many American-Muslim NPOs operate (see Paragraph 1094 for a more detailed discussion of this dialogue). Treasury's parallel engagement with the American-Muslim NPO sub-sector and the larger NPO sector have resulted in NPOs adopting more proactive approaches to protect their assets and the integrity of their operations.

that help better facilitate compliance with OFAC sanctions programs, (including those that address terrorist financing), and provide information on directing inquiries and/or suspicions and referrals to the appropriate state and federal law enforcement authorities.

Supervision or monitoring of the NPO sector

1051. In the U.S., the NPO sector is monitored by the federal government and state authorities. Transparency is facilitated by federal tax laws, which provide that most information reported by tax-exempt NPOs to the Tax Exempt and Government Entities Division (TEGC) of the IRS is available to the public. The other main transparency mechanisms include the certification program for USAID. Charities operating in the U.S. are also subject to self-regulation managed by umbrella and watchdog organizations. The U.S. states and the District of Columbia oversee the fund-raising practices of charities domiciled or operating in their jurisdictions. Many of the larger states have a separate agency to oversee charities, including the Offices of the Attorneys General and State Charities Officials. Thirty-nine U.S. states require any charity to register before soliciting funds within the state, no matter where the charity is domiciled.

FEDERAL LAWS

Scope of the sector that is subject to supervision or monitoring

1052. Any organization may apply to the IRS for recognition of tax-exempt status provided it shows that it meets the requirements of section 501(c)(3) of the IRC. If an NPO for some reason does not choose to apply for tax exempt status, it will still have obligations to pay tax and the IRS will have oversight of such organizations in its role as the administrator of the US tax system. U.S. federal income tax law affords two principal advantages to organizations that qualify as charities under section 501(c)(3). First, charities are not taxed on income from their charitable activities. Second, under section 170(c), donors to eligible charities generally will be able to reduce their own federal income taxes (and usually State income taxes as well) by a percentage of the amount of their donation (as much as 40%). This second advantage helps to encourage donations to charities by making the gifts less of a burden to the donor.

1053. Churches and equivalent institutions such as synagogues, temples, and mosques have a preferred status among other section 501(c)(3) organizations. They need not file applications for exempt status (Form 1023), as they are automatically recognized as being exempt.[101] Section 6033(2)(A) of the IRC creates a mandatory exception from the requirement to file annual information returns (Form 990) for churches, their integrated auxiliaries, and conventions or associations of churches and organizations which conduct exclusively religious activities. Further, civil tax examinations of churches are subject to strict approval and notice procedures before they can begin. Although exempt from filing both Form 1023 applications (and annual Form 990 information returns), these organizations must still meet the financial record keeping requirements of IRC section 501(c)(3). Many churches seek IRS recognition of exempt status because it provides certain benefits, such as assuring church leaders, parishioners, and contributors that the church is eligible for tax-exemption and related tax benefits. In addition, State and local laws that exempt charitable organizations from State and local income and property taxes generally require the organization to demonstrate tax-exempt recognition by the IRS.

1054. Foreign charities may also apply for tax exempt status in the U.S., however, foreign charities are not eligible to receive tax-deductible charitable contributions from U.S. taxpayers except as tax treaties may allow. A U.S. charity can carry on or financially support overseas charitable programs as part or all of its activities as long as it can demonstrate that the funds are used for charitable purposes.

[101] Public charities whose annual gross receipts are normally less than USD 5,000 are also not required to file for tax exempt status.

1055. Organizations claiming tax-exempt status under section 501(c)(3) must, within 27 months of their establishment, apply to the IRS for recognition of their exempt status. Section 501(c)(3) sets out those organizations eligible for tax-exempt status. Generally they must be organized and operated exclusively for religious, charitable, scientific, testing for public safety, literary or educational purposes or to foster national or international amateur sports competition or for the prevention of cruelty to children or animals. Section 170(c) sets out those organizations eligible to receive tax deductible donations. These are listed in IRS Publication 78 (Cumulative List of Organizations Described in Section 170(c) of the Internal Revenue Code of 1986), which is also available to the public on the IRS website.

1056. Under section 501(c)(3), charities applying for tax-exempt status must complete IRS Form 1023 and relevant associated documents, including various 1023 Schedules that apply to particular forms of charities (e.g., schools, hospitals, houses of worship, etc.). Form 1023 includes identifier and organizational information, such as:

(a) Employer Identification Number (whether or not it has employees);

(b) the name and address of the organization;

(c) the form of organization (e.g., corporation, trust, association) and copies of organizing documents (e.g. Articles of Association);

(d) full description of activities and operational information including standards, criteria or procedures;

(e) names, addresses, and titles of officers, directors, trustees, etc., and their compensation;

(f) detailed financial statements showing receipts and expenditures for current year and preceding 3 years; and

(g) any additional information as required by the IRS.[102]

1057. In addition to being organized as not-for-profit organizations the organizing documents which accompany Form 1023 must include provisions regarding distribution of its income upon dissolution and, in the case of a private foundation, prohibiting any self-dealing (section 508 IRC).

1058. The IRS may need to request additional information from an applicant during consideration of its application. Charities which have one of more subordinates under general supervision or control can seek a "group exemption" covering affiliated subordinates. A charity may have its section 501(c)(3) application denied or its existing tax-exempt status revoked by the IRS if it does not comply with the requirements described above. Since November 2003, a charity will have its exempt status (and deductibility of contributions) suspended under IRC section 501(p) when and while it is designated as a terrorist financing organization under applicable U.S. law (discussed further below), and will subsequently be removed from the list of tax exempt organizations in the IRS's Publication 78.

1059. Charities receiving tax-exempt status must still file various returns and reports after their accounting period. These include annual information returns (Form 990; Form 990-PF for a private foundation).[103]

1060. Annual information returns are required to include the organization's gross income for the year, its expenses and disbursements, a balance sheet showing its assets, liabilities, and net worth, the total of the contributions and gifts received by it during the year, and the names and addresses of all

[102] IRS Publication 557 cites examples of such additional information as representative copies of advertising place; copies of publications such as magazines; distributed written material used for expressing views on proposed legislation; and copies of leases, contracts or agreements into which the organization has entered.

[103] Other information required to be filed by a tax exempt organization includes tax returns for business unrelated to the charity, employment tax returns, reporting requirements for certain political organizations, information to donors and Form 8300 reports where an amount of USD 10,000 is received that is not a charitable contribution.

substantial contributors, the names and addresses of its foundation managers and "highly compensated employees", and the compensation and other payments made during the year to each of these people. IRS Publications 1771 and 4221 provide tax exempt organizations and charities with general compliance guidelines for recordkeeping, reporting and disclosure requirements. Exempt organizations are required to keep records that support an item of income or a deduction on a return until the statute of limitations for that return runs out—usually a period of three years. However, in practice, exempt organizations that engage in international transactions must maintain records for at least five years – notwithstanding the general three year statute of limitations on assessment and collection of tax imposed by Section 6501(a) – because financial and other records concerning grants, programs, etc., generally apply to more than one tax year. Thus, an organization cannot merely discard financial records for a year once the statute date for that year has expired.

1061. Additionally, exempt organizations are required (by Section 6104 of the Code) to maintain, and make available to the public, a copy of their approved application for recognition of exemption (Form 1023), including documents and supporting information submitted with the application. This information must be maintained and made available for far more than five years, as it applies as long as the organization continues to be recognized exempt. To the extent this information changes, the changes are required to be reported on the Form 990, as well as major changes in its purposes or activities.

Supervision and monitoring for compliance - IRS

1062. The IRS-TEGE currently employs approximately 340 examiners in its examination program for charities. The IRS will add an estimated 30 additional examiners over the next year to expand its program.

1063. An examination program by the IRS monitors compliance with the tax laws by reviewing and verifying the information on annual returns filed by exempt organizations, conducting audits to determine if organizations continue to operate as required by the tax laws, and imposing taxes and other IRS sanctions for non-compliance. As part of the review of each application, Treasury advises that IRS personnel have been instructed to cross-check names on the application (the applicant itself as well as its directors and officers) against a list that sets forth those organizations and individuals (as well as their aliases) that have been designated as being associated with terrorism, known as the SDN List. The appropriate investigative office at IRS is notified for further action where names on the application match those on this list. IRS-TEGE monitors changes to the SDN List, and OFAC concurrently informs the IRS of any new designated charities and takes action as described above regarding the suspension of its tax exempt status. Section 501(p) of the IRC requires the IRS to suspend a charity's tax-exempt status when and while the charity is designated as a terrorist financing organization under applicable U.S. law.

Supervision and monitoring for compliance - IEEPA and AEDPA designations

1064. NPOs that are suspected of being involved with terrorist financing activity may be designated as such. This can occur either by Presidential Order pursuant to Executive Orders 13224 and 12947, or by the Secretary of the Treasury, who has the authority to designate charitable organizations and other entities or individuals that meet the criteria contained in the Executive Orders, or by the Secretary of State (pursuant to Section 302 of the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) and Section 219 of the Immigration and Nationality Act), who can designate charitable organizations as FTOs. Once designated any U.S. person is prohibited from dealing with the NPO, and that NPO's assets are subsequently blocked or "frozen." All future transactions are also accordingly blocked. Conversely US-based charities are prohibited from accepting contributions from or otherwise dealing with any designated entities or persons.

1065. As of May 2006, the United States has designated 41 charities under EO 13224 and EO 12947 because of their support for terrorist activity. This includes five U.S.-based charities and 36 additional international charities (two of which have branch offices located in the U.S.). On February 19, 2006, the United States blocked the assets of a sixth U.S.-based charity pending further investigation, which

has the effect of freezing all assets located within U.S. jurisdiction and prohibiting U.S. nationals from transacting with the charity. In addition, several FTOs, also designated under EO 13224, have operated under names that appear as potential fundraising fronts for terrorist activities.

Supervision and monitoring for compliance–Umbrella, watchdog and academic organizations

1066. The U.S. charitable community's self-regulatory system includes umbrella organizations that focus on management support and other operational issues that affect all or parts of the charitable community, "watchdog" organizations that focus on helping donors make informed choices, and academic organizations that study how well the charitable community is meeting societal needs and how its effectiveness can be improved.

1067. These "umbrella" organizations focus on issues that affect the entire charitable community or particular segments. The most well known of these is Independent Sector, a nonprofit, nonpartisan coalition of more than 700 national organizations, foundations, and corporate philanthropy programs that collectively represent many thousands more organizations throughout the United States. Its many research activities include studies of the impact of public policy on charitable giving, and defining and addressing ways to improve accountability in the charitable sector. The Independent Sector has played a key role in the sector's participation and dialogue with the U.S. Treasury regarding guidance to the sector, and its concerns about the revised "Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities" are set out on its website.

1068. Other umbrella organizations focus on particular segments of the charitable sector. The Council on Foundations focuses on issues affecting private foundations. The Evangelical Council for Financial Accountability (ECFA) serves a major segment of the religious community as an accreditation organization that either grants or withholds membership based on an examination of the financial, grant-making and management practices and accomplishments of charitable organizations that apply. It provides public disclosure of its more than 900 members' financial practices and accomplishments, including on its website. While the U.S. Treasury has engaged with ECFA regarding terrorist financing abuse and methodologies to combat such abuse in the charitable sector, there appears to be no mention of Treasury's "Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities" on the EFCA website. ECFA is also the U.S. member of the International Committee for Fundraising Organizations (ICFO), an umbrella organization that links the accreditation organizations of 9 countries (US, UK, Canada, Norway, Sweden, France, Germany, Switzerland, and Austria).

1069. Watchdog organizations focus on providing the contributing public with the information needed to make informed decisions. Well-known organizations include the Philanthropic Research Institute, whose Guidestar organization maintains a database containing IRS filings and other financial information of over 200 000 charities, which it makes accessible through its website. Another donor-information /watchdog organization, the Better Business Bureau (BBB) Wise Giving Alliance, focuses on organizations that conduct broad-based fund-raising appeals. It collects and distributes information about the programs, governance, fundraising practices, and finances of hundreds of nationally soliciting charitable organizations that are the subject of donor inquiries. BBB asks the selected organizations for information about their programs, governance, fund raising practices, and finances, and measures the results against general guidelines and standards it has developed for measuring organizational efficiency and effectiveness. BBB publishes these results, including whether the selected organization refused to supply information, on its website.

1070. The wide variety of academic research organizations which deal with charitable organizations in the U.S. include: The National Council on Charitable Statistics (NCCS), a project of The Urban Institute, the National Center on Philanthropy and Law of the New York University Law School, and the Center on Philanthropy at Indiana University

Certification program

1071. The U.S. has implemented mechanisms to ensure that NPOs participating in the USAID program follow a "know your beneficiaries and associate NPOs" rule. To provide USAID with assurances that it is not entering into assistance agreements with organizations that provide or have provided assistance to terrorists or for terrorist activity, USAID issued Acquisition and Assistance Policy Directive (AAPD) 02-19 in December 2002, also known as the Anti-Terrorism Certification (ATC). Under this Directive, before making any award or grant to any grantee worldwide, USAID requires any grantee worldwide to certify that, to the best of its current knowledge, the grantee did not provide, within the previous ten years, and it will take all reasonable steps to ensure that it does not and will not knowingly provide, material support or resources to any individual or entity that has engaged or engages in terrorist activity, as described in the Certification. Revised versions of the AAPD (04-07 and 04-14) were issued in March and September 2004, respectively. The latest version (AAPD 04-14) of the Anti-Terrorism Certification is located on the USAID website.

1072. In addition to the USAID certification program, the Office of Personnel Management (OPM) revised the rules pertaining to the Combined Federal Campaign (CFC), which is a program allowing federal employees to contribute money directly from their paychecks to participating NPOs. The new regulation (5 CFR Part 950), issued on November 7, 2005, states that any NPO wishing to participate in the CFC program must complete a certification that it is in compliance with all statutes, Executive Orders, and regulations relating to economic sanctions programs administered by OFAC. The certification also requires participants to be aware of the Specially Designated Nationals and Blocked Persons (SDN) List and other sanctions programs administered by OFAC. Finally, the guidance accompanying the new certification rule, CFC Memorandum 2005-13, encourages charities to follow Treasury's Anti-Terrorist Financing Guidelines, Voluntary Best Practices for U.S.-based Charities, adopt the risk-based approach contained in those Guidelines, and review the OFAC Web site regarding obligations and compliance information with existing sanctions programs.

Information gathering, investigation, designation, and prosecution

1073. The IRS has established a number of mechanisms to ensure that IRS-TEGE and the Criminal Investigation Division of the IRS (IRS-CI) communicate and work together on potential cases of terrorist financing. These mechanisms include: cross-training initiatives, including a two-week training class, and programs whereby IRS-TEGE examiners and IRS-CI investigators learn about each other's operations, resources and needs; staffing IRS-TEGE examiners on task forces dedicated to investigating terrorist financing leads in the charitable sector; and sharing red flags, typologies and information from IRS-CI to IRS-TEGE to assist in conducting examinations on charities particularly vulnerable to terrorist abuse.

1074. Based on these interactions, IRS-TEGE has recently revised the Form 1023 application for tax-exempt status to include more relevant information for criminal investigators in terrorist financing and criminal cases. These new sections request information on whether the organization operates in a foreign country and whether the organization makes grants loans or other distributions to other organizations including foreign organizations. IRS-TEGE has also created a new Compliance Unit to target high risk charities for examination, based in part on information gained from IRS-CI. IRS-TEGE has also established a Screening Center to process leads from all sources, including state and local officials, on potentially abusive charities. Finally, IRS-TEGE identifies media reports concerning abuses within the charitable sector.

1075. The IRS has also identified areas where IRS-CI can have a greater impact addressing terrorism related financial issues without duplicating the efforts of any other law enforcement agency. IRS-CI has created a Lead Development Center (LDC) to pilot a counter-terrorism project focusing on charitable abuse by using advanced analytical technology, along with subject matter experts, to support ongoing investigations and proactively identify potential patterns and perpetrators. The LDC is comprised of a staff of IRS-CI special agents, investigative analysts, and representatives from

TEGE, who will research investigative leads and field office inquiries concerning terrorism investigations. The LDC integrates its work within the larger U.S. law enforcement community; largely through IRS-CI representatives on Joint Terrorism Task Forces (JTTFs) led by the FBI. The target information packages developed by the LDC will be sent to the JTTF or IRS field office that requested the analysis and to such other law enforcement entities as may be appropriate and consistent with the statutory limitations on disclosure.

1076. IRS-CI has also used new funding to construct a data warehouse to house information gathered from internal IRS sources, including the LDC described above, and from other public and government databases. The data warehouse has sophisticated data mining tools that will supplement and expand the LDC's analytical capabilities. Data storage at the warehouse will be based on the statutes and rules governing or restricting disclosure of certain classes of information (tax disclosure rules, grand jury secrecy rules, etc.), and dissemination of that information will be made only in accordance with those rules. The following sources of information have been used in this integrated analysis:

(a) Tax-based information, including all publicly available IRS Form 990 and IRS Form 1023 information and confidential Form 990 Schedule B donor information;

(b) Government information obtained from other government agency databases, to which IRS-CI may be given access under the terms of specific agreements;

(c) Criminal investigation information received or to which IRS-CI has access from grand jury investigations and others in the law enforcement community;

(d) Intelligence that may be obtained from the intelligence agencies, whether as part of an ongoing data sharing arrangement or as case-specific data; and

(e) Commercial information from LEXIS-NEXIS, Choicepoint, and other commercially available data services.

1077. Because of the sensitive and private nature of tax information received by the IRS, Federal tax laws generally preclude sharing certain tax-related information outside of the IRS. The U.S. has addressed this constraint to some extent through the joint task force and LDC mechanisms described above. Tax-related information falls into three categories: information received by the IRS about a taxpayer that is received from returns filed with the IRS (taxpayer information), information obtained from tax returns filed by the taxpayer and subsequent information provided by the representative for the taxpayer pursuant to an audit (taxpayer return information), and information gathered by the IRS during audits and investigations received independently of the taxpayer's returns (return information). In addition, the U.S. Tax Disclosure Law (26 U.S.C. 6103) was amended[104] permitting the disclosure of the taxpayer's identity and return information "other than taxpayer return information" to federal officers or employees for administration of federal laws not relating to tax administration that may be related to a terrorist incident, threat, or activity to the extent necessary to investigate or respond to such terrorist incident, threat, or activity.

1078. The exclusion of "taxpayer return information" from these exceptions may appear confusing. But what this exclusion means is simply that information provided by the taxpayer or the taxpayer's representative to the IRS may not be disclosed. However, any additional information that the IRS has obtained during an audit or investigation may be disclosed under appropriate circumstances. Therefore, the information that may be disclosed consists of any information that the IRS has gathered that was not directly derived from filed tax returns, and includes information gathered from third parties, such as banks, customers of taxpayers, real estate companies, and car dealerships,

1079. Prosecutorial actions against charities suspected of terrorist financing crimes form another central component of the comprehensive U.S. strategy to fight terrorist financing in the NPO sector. DOJ's

[104] 26 USC 6103(i)(3)(C).

Counter-Terrorism Section (CTS) is comprised of a group of experienced prosecutors that guide U.S. attorneys across the country. Past and ongoing criminal cases demonstrate this group's effectiveness.

International cooperation

1080. As reflected in Section 6 and elsewhere in this report, the U.S. has in place comprehensive mechanisms to facilitate information sharing with its international counterparts depending on the type and intent of the request. These include mechanisms for FIU to FIU information sharing, provision of mutual legal assistance, law enforcement, diplomatic and regulatory channels, and other information sharing conduits. In addition to these established channels, Treasury's Office of Terrorist Financing and Financial Crimes (TFFC) serves as the primary point of contact for responding to international requests for information regarding particular NPOs suspected of terrorist financing or other forms of terrorist support. TFFC acts as the appropriate point of contact for such requests by marshalling U.S. intelligence and enforcement capabilities with the twin aims of combating terrorist financing in the charitable sector and promulgating policies and other initiatives to better safeguard charities from the threat of terrorist abuse. Based on this active engagement with other agencies involved in investigation, enforcement, and/or oversight of the charitable sector, TFFC is able to send out requests for information promptly to the relevant agency or individual.

State Laws

1081. The states also exercise oversight of charities that complements or supplements federal authority. All 50 U.S states and the District of Columbia oversee the practices of charities domiciled or operating in their jurisdictions,. State Attorneys-General have statutory jurisdiction over the charitable assets of these organizations and the fundraising activities of charities. Oversight responsibilities and practices vary from state to state, and are directed at consumer protection issues. Thirty-nine of the 50 states require that any charity raising money in their state register with that state.[105] In addition, state charities officials have formed a national-level organization, the National Association for State Charity Officials (NASCO). Among other things, NASCO has promoted harmonization in registration requirements among the states, and has advanced a "Model Act Concerning the Solicitation of Funds for Charitable Purposes" for adoption by state legislators. NASCO has also promoted the Unified Registration Statement, which is a project aimed at consolidating the data requirements of all states in order to standardize and simplify compliance with State registration laws. Currently, 35 of the 39 States that have registration requirements are cooperating with this project.[106] In addition, NASCO and the federal government have consistently worked together to share information and coordinate on law enforcement actions taken against NPOs. This past cooperation resulted in the recent development of a working group to discuss new policies and share information and other developments relating to charitable organizations and terrorist financing abuse within the sector. The first jointly chaired working group meeting was held in March 2006 and included officials from Treasury, IRS-CI, IRS-TEGE, DOJ, and NASCO members.

1082. For the purposes of this evaluation, the assessment team considered the state-level measures that have been implemented in New York.

Case study—New York

The Charities Bureau of the New York State Attorney General is responsible for overseeing the

[105] These states are: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, District of Columbia, Florida, Georgia, Illinois, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Utah, Virginia, Washington, West Virginia, and Wisconsin

[106] The four states that are not yet participating in the Unified Registration Statement are Alaska, Colorado, Florida, and Oklahoma.

administration of charitable assets in the State of New York, representing the interests of beneficiaries of charitable dispositions and enforcing laws governing the conduct of fiduciaries of charitable entities. This includes authority to oversee the solicitation of charitable assets from New Yorkers including investigation and prosecution of fraudulent charitable solicitations, registration of charitable entities which solicit monies in the State of New York and registration and regulation of professional fund raisers.[107]

The Attorney-General's registration and oversight extends to charitable trusts created under the laws of other jurisdictions including foreign jurisdictions and to foreign charitable corporations that conduct activities in New York. Not all NPOs are required to be registered. Groups that are regulated by other State agencies (such as hospitals and educational institutions) or groups that are essentially for the benefit of their own members (such as fraternal and patriotic organizations and veterans groups) are exempted from registration and reporting requirements. Religious groups are also exempted.

If an NPO is required to be registered by the New York State Attorney-General's Charities Bureau there are detailed financial reporting requirements.

The New York Attorney-General's Department confirmed that one of the biggest problems for State Regulators of NPOs is that despite recent changes to the tax disclosure laws under Federal law permitting disclosure to Federal employees in terrorist cases, the IRS still cannot disclose any information to State Charities officials.[108]

Another problem raised by the New York Attorney-General's office is the size of the charitable sector in the State of New York. With a staff of 18 lawyers, the office of the Charities Bureau of the New York State Attorney General is one of the largest State Regulatory offices. Even in such a large office it is difficult to review and verify the operational program of all registered charities. Most State Charities offices with staff of only one or two lawyers would have even more difficulty. Nonetheless within the constraints of resourcing the New York Attorney-General's oversight role in the operational activities of registered NPOs is impressive and backed up by active enforcement actions.

5.3.2 Recommendations and Comments

1083. Overall, the measures which are being implemented to ensure that the NPO sector cannot be abused by terrorists or terrorist financiers are working effectively. U.S. authorities at both a state and federal level take action against illegitimate or fraudulent charities particularly where they are able to demonstrate that these charities have been established to facilitate terrorist financing.

1084. In May 2002, the International Committee on Fundraising Organizations (ICFO) published the results of a comparative survey of ICFO members and their countries which included the U.S. In relation to the IRS requirements to file Form 990, the IFCO noted that:

> "because of the high volume only those organizations which are exposed by media investigations or are otherwise the subject of numerous complaints, get investigated. The same limited resource is true of State monitoring agencies. The result is a lightly regulated industry brought about in part because of the lack of resources to monitor so many organizations, plus the very real constitutional protections that are afforded U.S. charities. The issues of free speech and separation of Church and State allow NPOs considerable latitude in functioning without close oversight"

---

[107] Sections 8-1.1 & 8-1.4 Estate, Powers and Trusts Law.

[108] In November 2005 the Senate Finance Committee and the House Ways and Means Committee passed a tax bill containing reform provisions relating to the regulation of charities which included a provision that will allow the IRS to share with State enforcement officials more information concerning ongoing IRS actions with respect to specific charities. However this provision is not yet law.

1085. The U.S. has taken many steps to improve oversight of NPOs as discussed above. The U.S. should continue to devote resources to preventing the abuse of this sector from terrorist organizations, including ensuring the effective flow of information between competent authorities. Federal cooperation and information-sharing with NASCO officials has yielded enhanced communication, a greater understanding of federal policies on the part of state officials, and increased outreach to the NPO sector through state officials.

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	C	• This Recommendation is fully observed.

6. NATIONAL AND INTERNATIONAL COOPERATION

6.1 National cooperation and coordination (R.31)

6.1.1 Description and Analysis

Recommendation 31 (Domestic cooperation and coordination)

Policy level cooperation and coordination mechanisms

1086. The interagency process is widely used within the U.S. government to enhance the development and implementation of AML/CFT policies and strategies. National policy to combat terrorist financing is coordinated by the National Security Council (NSC) Terrorist Financing Policy Coordinating Committee (TF PCC), a high-level interagency group that reports to the National Security Advisor, who in turn reports directly to the President. The TF PCC meets regularly to assess the effectiveness of current policies and to coordinate appropriate adjustments. No agency exists at a similarly high level in relation to AML.

1087. National policy to combat money laundering is primarily coordinated by the Treasury in the context of the Money Laundering Working Group. The Money Laundering Working Group focuses on a wide range of AML/CFT issues (particularly those related to the FATF and FSRBs) and cooperates on specific courses of action relative to particular issues or concerns. Chaired by the Treasury Department/TFFC, it includes representative from the DOJ, State Department, DHS, FinCEN, law enforcement agencies and financial regulators.

1088. The U.S. authorities also consult with the Bank Secrecy Act Advisory Group (BSAAG) which is comprised of representatives from the Treasury, FinCEN, the DOJ, the Office of National Drug Control Policy, various law enforcement agencies, financial regulatory agencies (including SROs and state regulatory agencies) as well as financial services industry representatives which are subject to BSA regulation (including trade groups and practitioners).[109] The BSAAG receives, for consideration and comment, information from the Secretary of the Treasury or his designee(s) concerning the administration and enforcement of the BSA and associated reporting requirements, and law enforcement's use of such data. It also informs the participating private sector representatives about how law enforcement agencies make use of the filed reports. On the basis of this dialogue, the BSAAG advises the Secretary of the Treasury on ways in which the reporting requirements could be modified to enhance the ability of law enforcement agencies to use the information and/or to reduce the burden on reporting entities.

[109] The BSAAG was established pursuant to the Annunzio-Wylie Anti-Money Laundering Act of 1992 [s.1564, Public Law 102-550 (28 October 1992)].

Operational level cooperation and coordination mechanisms amongst law enforcement agencies and the FIU

1089. Interagency coordination among U.S. law enforcement agencies is formalized through interagency agreements. In the area of CFT, a memorandum of agreement between the DHS and DOJ (entered into in May 2003) delineates specific coordination of terrorist financing investigations to the FBI's Terrorist Financing Operations Section (TFOS) and Joint Terrorism Task Forces (JTTFs), both of which are described below. In the area of AML, statutorily required MOUs between the Attorney General, the Secretary of the Treasury and the Postmaster General specify the jurisdiction of the various law enforcement agencies and require them to coordinate their ML investigations with each other. Additionally, cooperation and coordination is facilitated through the use of interagency groups and task forces.

Interagency working groups and task forces focused on CFT

1090. **Coalition Building Group (CBG):** The CBG, chaired by the Assistant Secretary of State for Economic and Business Affairs, includes the NSC, State, Treasury, Justice, FBI and intelligence agencies. It coordinates U.S. diplomatic engagements on terrorist financing, including sanctions under UN resolutions. Overall direction is provided by the NSC.

1091. **Terrorist Finance Working Group (TFWG):** The State Department chairs the TFWG, which brings together State, Justice, Treasury, Homeland Security, USAID and financial regulators to coordinate U.S. planning, funding and delivery of training and technical assistance to a selected group of some two dozen countries where financial systems are particularly vulnerable to abuse by terrorists. TFWG bilateral assistance programs utilize a comprehensive model aimed at developing or reinforcing legal, judicial, financial regulatory, financial intelligence, and law enforcement capabilities.

1092. **Terrorist Financing Operations Section (TFOS):** The TFOS is an inter-agency group that is spearheaded by the FBI. A main focus of TFOS is to conduct full financial analysis of terrorist suspects and their financial support structures in the U.S. and abroad. It was created during the early stages of the 9/11 investigation when the FBI and the DOJ identified a critical need for a more comprehensive, centralized approach to terrorist financial matters. To better coordinate this work, an ICE official has been designated to serve as the Deputy Section Chief of TFOS with a view to ensuring that ICE financial leads are thoroughly evaluated for any terrorist nexus which may exist. The TFOS works jointly with the intelligence community, prosecutors, domestic law enforcement agencies, foreign law enforcement agencies (through the FBI Legal Attaché program) and financial sector regulators to develop predictive models and conduct data analysis to facilitate the identification of previously unknown terrorist suspects.

1093. **Antiterrorism Advisory Councils (ATAC):** ATACs promote and ensure proper training and information sharing on terrorism cases and terrorism threats (including terrorist financing) among federal, state and local law enforcement and private sector representatives.[110]

1094. **Joint Vetting Unit (JVU):** The JVU is staffed by ICE and FBI personnel who have full access to relevant ICE and FBI databases to conduct reviews to determine whether a nexus to terrorism or terrorism financing exists in a given investigation. Where such a nexus is found to exist, the JTTF is responsible for conducting an investigation.

1095. **Joint Terrorism Task Forces (JTTF):** The FBI sends all terrorism leads and terrorism related information directly to the FBI-led JTTFs which have primary investigative responsibility for the investigation of terrorism and terrorist financing. Eighty-four JTTFs exist across the country.[111]

[110] This body was not referenced by the U.S. authorities prior to or during the on-site visit. Consequently, the assessment team did not have the opportunity to meet with this agency or discuss its AML/CFT role.

[111] Prior to September 11th there were 34 JTTFs in existence.

Various federal, state and local agencies participate, including representatives from the ICE, the IRS, the Treasury, State Department, Department of Defense, the Postal Inspection Service and the Environmental Protection Agency. In cases where ICE has significant investigative equity, ICE agents assigned to the JTTF serve as lead agents and affiants on violations within ICE's authority.[112] Every agency has an open-ended invitation to participate in the JTTF. Additionally, each USAO has been encouraged to create a multi-agency task force (as part of either the FBI-led JTTF or the Anti-Terrorism Advisory Council) to periodically review all SARs that may be terrorism/terrorist financing related and ensure that each is properly examined and further investigated, when appropriate. All participating agencies have full access to each others' information systems and files, and can use the full resources of the entire task force when required for the purpose of investigating terrorism cases.

1096. **National Joint Terrorism Task Force (NJTTF) and the Foreign Terrorist Asset Targeting Group (FTAT-G):** The NJTTF and FTAT-G are interagency task forces that coordinate federal, state and local investigative agencies on terrorist-related investigations which are targeting key money laundering professionals and financial mechanisms (e.g. bulk cash movement and wire transfers).

1097. **National Counterterrorism Center (NCTC):** At the intelligence level, the NCTC orchestrates an interagency CFT action plan and/or response by integrating diplomatic, financial, military, intelligence, homeland security and law enforcement activities within and among relevant agencies. This work involves receiving, retaining and disseminating information from any federal/state/local government or other sources (as needed), and coordinates the information flows which are generated by the U.S. intelligence agencies. Agencies authorized to conduct CFT activities may access NCTC intelligence data for any information to assist in their respective responsibilities.

Interagency working groups and task forces focused on AML

1098. **High Intensity Financial Crime Areas (HIFCAs):** HIFCA Task Forces seek to improve the quality of federal money laundering and other financial crime investigations by concentrating the expertise of the participating federal, state and local agencies in a unified task force that can utilize all of the FinCEN, DEA/SOD and DHS/ICE MLCC financial databases. Seven HIFCAs have been designated: California Northern District, California Southern District, Chicago, New York/New Jersey, Puerto Rico and the Southwest Border of the U.S. The ICE is a core member within each HIFCA. Other participating agencies include the DEA, FinCEN and IRS-CI. The most highly developed and successful HIFCA is the ICE-led El Dorado Task force which is located in New York/New Jersey HIFCA and funded through the New York High Intensity Drug Trafficking Area (HIDTA) program. (Similar in structure to the HIFCAs, the HIDTA program is intended to concentrate the AML efforts of federal, state and local law enforcement agencies in designated high-intensity drug trafficking zones.)

1099. **Organized Crime Drug Enforcement Task Forces (OCDETF):** Led by the DOJ, the following agencies also participate in the OCDETFs: the DEA, FBI, the Department of Alcohol Tobacco and Firearms, the USMS, the IRS, ICE and the U.S. Coast Guard–in cooperation with the DOJ's Criminal and Tax Divisions, the 94 U.S. Attorneys' Offices (USAOs), and state and local law enforcement. The OCDETFs conduct intelligence-driven investigations that target the most significant, high-priority drug trafficking organizations in their region. Every OCDETF investigation must include a financial investigative plan for attacking the financial structure of the criminal organization and identifying forfeitable assets.

1100. **Drug Enforcement Administration Special Operations Division (DEA/SOD):** The DEA/SOD is a DEA-led division with participation from ICE, CBP, the FBI, the IRS and DOJ's Criminal Division. Its mission is to dismantle major national and international drug trafficking

[112] These authorities include money laundering, bulk cash smuggling, illegal MSBs, sanction violations, illegal exports of arms and dual-use technology, alien smuggling, identity and immigration benefit fraud along with various administrative violations pertaining to the Immigration and Naturalization Act.

organizations by attacking their command and control communications. The DEA/SOD acts as a 'force multiplier' for drug law enforcement by providing a medium for communication, intelligence sharing and coordination between the major U.S. drug law enforcement agencies. Significant and successful operations supported by SOD include the targeting of international money brokers responsible for laundering drug proceeds.

1101. **Money Services Business Working Group (MSB-WG):** The MSB-WG is comprised of representatives from ICE, IRS, FinCEN, Treasury, the FBI the DEA and members of the intelligence community. Its mission is: (1) to gather intelligence to identify unlicensed MSBs that may be providing remittance services to persons associated with "countries of interest" (as listed by the U.S. Foreign Terrorist Tracking Task Force) and identify any criminal associations; (2) to conduct outreach to unlicensed MSBs which have no known links to any other criminal activity; and (3) to take enforcement actions targeting unlicensed MSBs which are involved in criminal activity or have failed to comply with licensing and registration requirements.

Interagency information-sharing mechanisms and networks

1102. In addition to the interagency working groups and task forces described above, the cooperation and coordination of U.S. law enforcement agencies and the FIU is facilitated by a number of information-sharing mechanisms and networks.

1103. **Platform Program:** FinCEN maintains the Platform Program, an information system that facilitates the sharing of terrorism-related data between domestic and international law enforcement agencies, and financial intelligence units. In addition to the 12 domestic law enforcement agencies that are represented at FinCEN, an additional 22 law enforcement agencies participate in the Platform Program. Through this program, agencies can come to FinCEN and access its BSA and commercial databases. Law enforcement information can also be queried, but cannot be disseminated until authorization is received from the owning agency. If multiple agencies, domestic or foreign, express interest in the same entities involved in illegal activities, FinCEN coordinates the various agencies and links them together or networks them to facilitate information sharing.

1104. **Gateway Program:** FinCEN also disseminates SARs to domestic law enforcement agencies who participate in the Gateway Program, a system which permits state and local law enforcement, and an ever expanding number of federal law enforcement agencies, to directly query the BSA repository without making a formal request for research to FinCEN. SAR dissemination statistics for the Gateway Program for 2000 through 2004 are reflected below.

Gateway Program Suspicious Activity Report Disseminations from 2000-2004		
Year	# Cases	# SARs
2000	713	2,736
2001	1,139	3,861
2002	1,615	5,793
2003	2,181	8,765
2004	3,387	14,772

1105. In addition, some U.S. federal law enforcement agencies can directly access the BSA database at the Detroit Computing Center (DCC). IRS-CI has a liaison situated at the DCC, who can conduct special analytical projects at the request of field agents.

1106. **Section 314(a) requests:** In its role as a network, FinCEN receives requests made by domestic federal law enforcement authorities pursuant to section 314(a) of the USA PATRIOT Act and FinCEN's implementing regulations at 31 CFR 103.100 (Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions) and transmits them to designated contacts within

financial institutions across the country.[113] Upon receiving a request, the financial institution is required to query its records for matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last six months. Generally, financial institutions have two weeks from the transmission date of the request to respond. Section 314(a) provides lead information only and is not a substitute for a subpoena or other legal process. To obtain documents from a financial institution that has reported a match, a law enforcement agency must meet the legal standards that apply to the particular investigative tool that it chooses to use to obtain the documents.[114] Requests must be very explicit concerning what kind of information is being sought, since the financial institutions will not automatically deliver all available information about their clients (i.e. stock accounts, loans/mortgages, etc.). Moreover, law enforcement may not receive relevant information that falls outside the period defined in the request itself. Despite these limitations, section 314(a) requests have yielded productive leads for both terrorist financing and money laundering investigations, including the identification of new accounts and transactions (see Annex 6, Table 1 for some examples of the processing of section314(a) requests).

1107. **OCDETF Fusion Center (OFC):** The OFC is a comprehensive data center containing all drug and related financial intelligence information from six OCDETF-member investigative agencies, the National Drug Intelligence Center and FinCEN. The technical infrastructure that supports the Center (and which is in the process of being developed) is designed to conduct cross-agency integration and analysis of drug and related financial data with a view to creating comprehensive intelligence pictures of targeted organizations (including those identified as Consolidated Priority Organization Targets (CPOTs) which are the U.S.'s 'most wanted' international drug and money laundering targets, and regional priority targets. This will allow the OFC to pass actionable leads through the DEA/SOD to OCDETF participants in the field. It is anticipated that the OFC will reach an initial operating capability in mid-June 2006.

Operational level coordination/cooperation mechanisms amongst law enforcement and regulatory agencies

1108. In addition to reporting incidents of possible money laundering to appropriate authorities, the Federal Banking Agencies actively cooperate with the IRS, ICE, the DOJ and other law enforcement agencies in money laundering investigations. Furthermore, in special cases, bank examiners have been designated as agents of a grand jury to assist in the investigation and development of particular cases. Interagency working groups are also used to facilitate coordination and cooperation amongst law enforcement and regulatory agencies. An example of this is the Drug Enforcement Administration Financial Office which conducts and maintains liaison with other federal law enforcement and regulatory agencies concerning money laundering techniques and financial investigative techniques, provides a full-time staff coordinator to FinCEN and represents the DEA before numerous multi-agency groups involved in AML/CFT.

Operational level coordination/cooperation mechanisms amongst regulatory agencies

1109. There is a significant amount of coordination and cooperation amongst regulatory agencies in the banking sectors, most of which is formalized through a series of MOUs. For a more detailed discussion of how regulatory agencies for the banking sector coordinate their work, see section 3.10 of this report.

1110. In the securities sector, FinCEN is in the process of finalizing MOUs with the SEC and the CFTC. Additionally, the SEC and the SROs have numerous ongoing cooperative efforts to combat

[113] More than 40,000 points of contact at over 20,000 financial institutions have been designated by those financial institutions to receive such requests pursuant to Section 314(a) of the USA PATRIOT Act and FinCEN's implementing regulations. Financial institutions also are permitted, pursuant to Section 314(b) of the USA PATRIOT Act and FinCEN's implementing regulations at 31 CFR 103.110, to share information among themselves under the circumstances described in the rule.

[114] Representatives from the Puerto Rico HIFCA advised assessment team that all relevant information can be obtained with an appropriate subpoena.

money laundering and terrorist financing. The SEC and SROs meet quarterly to discuss examination techniques, goals and trends. FinCEN and OFAC have participated in these meetings as well. Additionally, the SEC conducts AML/CFT examinations jointly with the NYSE and the NASD.

1111. In the insurance sector, coordination among the various state/territorial supervisors/regulators is facilitated through the NAIC. This is a voluntary organization of chief insurance regulatory officials from 50 U.S. states, the District of Columbia and four U.S. territories (American Samoa, Guam, Puerto Rico and the U.S. Virgin Islands). The NAIC was created in 1871 by state insurance regulators to address the need to coordinate regulation of multi-state insurers. The NAIC's role is to, among others: (1) provide its members with national forums for discussing common issues and interests as well as for working cooperatively on regulatory matters and the development of uniform policy; (2) help regulators to fulfill the obligation of state regulators' primary responsibility in protecting the interests of insurance consumers; (3) advise state regulators on policy implications of federal legislation and other federal and international actions affecting their authority over the business of insurance; and (4) support and improve state regulation of insurance. The NAIC also collects national statistics on the insurance sector. In support of the NAIC's role and responsibilities, state insurance laws provide for their insurers to cooperate and furnish the NAIC with the necessary information for it to carry out its functions effectively.[115] The NAIC's Ad Hoc (EX) Task Force on USA PATRIOT Act Compliance considers policy issues, develops and coordinates appropriate examination standards, and coordinate with state and federal regulators regarding the USA PATRIOT Act AML amendments to the BSA.

1112. In the MSB sector, interagency coordination is formalized by MOUs. The IRS has signed MOUs with FinCEN and with individual states to share examination information and leverage examination resources at the state and federal levels. Pursuant to its MOU with FinCEN, the IRS provides to FinCEN, on a quarterly basis, extensive information concerning their inspection and examination procedures, the number of examinations conducted, and the results of the examinations of MSBs. In return, FinCEN provides the IRS with quarterly aggregate reports, notice and status of possible enforcement actions, analytical products, assistance in identifying institutions with BSA compliance deficiencies, and prior review of public documents, all of which will assist them in the overall supervision and monitoring of MSBs. Coordination amongst state MSB regulators is facilitated by the MTRA. The MTRA is a national non-profit organization that works towards the effective and efficient regulation of money transmitters and check sellers. Its membership is comprised of the relevant regulators in 37 states and the District of Columbia.[116] In order to help states enact or modernize their money transmission legislation, MTRA drafted model legislative guidelines and made them available to the states. MTRA has also referred to the states for consideration and adoption a uniform annual renewal form and cooperative interstate examination agreement which promotes coordination and information sharing amongst state regulators.

Effectiveness of domestic cooperation and coordination

1113. The U.S. has implemented mechanisms at both the policy and operational level to enhance domestic cooperation and coordination in the area of AML/CFT. However, overall, a gap still seems to remain between the policy level and the factual operational law enforcement work.

[115] For example, section 931 of the California Insurance Code, requires each domestic, foreign, and alien insurer doing business in California annually to file with the NAIC a copy of its annual and quarterly statements exhibiting its condition and affairs together with any additional filings as prescribed by the Commissioner for the preceding year. Further, section 934 empowers the Commissioner to suspend, revoke, or refuse to renew the certificate of authority of any insurer failing to file its annual or quarterly statement with the NAIC when due or within any extension of time which the Commissioner, for good cause, may grant.

[116] Alabama, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Mississippi, Missouri, Michigan, New Jersey, New York, North Carolina, North Dakota, Ohio, Massachusetts, Oregon, Pennsylvania, Oklahoma, Tennessee, Texas, Virginia, Washington, West Virginia, Wisconsin and Wyoming.

1114. The law enforcement arena appears to be fragmented. The U.S. authorities have tried to overcome this problem by, among other initiatives, undertaking a series of important reorganizations with a view to better coordinating its ability to combat terrorism and terrorist financing. The creation of the DHS represents the most comprehensive reorganization of the federal government in a half-century. DHS consolidates 22 agencies and 180,000 employees, unifying multiple federal functions in a single agency dedicated to protecting America from terrorism. Similarly, the U.S. has accomplished the most thorough reorganization of the U.S. intelligence community in more than a half-century with the creation of a National Intelligence Director to oversee the U.S. intelligence community and the establishment of the National Counterterrorism Center (NCTC). The overall effectiveness of this strategy cannot be clearly measured, as the reorganization is still in the relatively early days. Certainly, since the attacks of 9/11, the U.S. has very much focused its resources and strategies to combat terrorism and terrorist financing. The evaluation team noted the important reorganizations that have occurred, but also noted that there is a discrepancy between the policies in place and the actual law enforcement work being undertaken. Officially the law enforcement agencies indicated to the assessment team that cooperation between them works well; however, unofficially when met with individually there was some mention that cooperation between the agencies is not always as effective as was indicated in the official meetings. However, challenges remain for the continued integration of well-established and successful law enforcement agencies (such as ICE) within the large, still young and evolving framework of the DHS.

1115. The assessment team also acknowledges the efforts that are currently being undertaken by the U.S. to improve the efficiency of its co-ordination mechanism by establishing joint task forces. The examples which the assessment team witnessed in the U.S. show that the concept works effectively. For instance, the HIFCA Task Forces generate an effective level of cooperation amongst law enforcement agencies; however, despite being a sound strategy, no budgetary resources have been allocated to support them. Consequently, the HIFCAs are at various stages of development. The Task Force concept, like the HIFCAs and HIDTAs, seems to work extremely well; they are providing a useful tool to improve the coordination among the various relevant agencies and a platform for inter-agency cooperation in investigations. The example of the ICE-led El Dorado HIFCA in New York should be considered as a model for the rest of the country. However, during the onsite visit, it became apparent that coordinating problems still exist, particularly outside of the joint task force model where there is competition between law enforcement agencies. The fact that the Treasury recently has presented a government-wide analysis on money laundering (the U.S. Money Laundering Threat Assessment, 2006) could create an opportunity to evaluate the present fragmented system. Such an analysis should not lead towards the creation of new entities, but rather should initiate a discussion on the basic law enforcement framework in a country as big as the U.S.

1116. Another complicating factor is the fact that, at the operational level, there is a great deal of overlap between the jurisdictions of the relevant law enforcement agencies. For instance, the DEA, the ICE, the FBI and the IRS all handle money laundering investigations. Multiple mechanisms exist at the operational level to co-ordinate the work of these various law enforcement agencies, including multi-agency task forces (such as the HIFCAs, HIDTAs and JTTFs) and bilateral working agreements (such as the MOU between the DEA and the FBI). Some of the interagency task forces work particularly well in this regard. For instance, the OCDETF concept seems to work very well where it concerns targeting the most significant drug trafficking organizations in their regions for investigation and prosecution. Also, the HIFCAs (where they are properly funded and developed, as is the case with the El Dorado/New York HIFCA) produce excellent results and opportunities for coordinated collaboration. Moreover, in some jurisdictions at least, the aftermath of the 9/11 terrorist attacks resulted in a more cooperative environment amongst law enforcement agencies. Although these mechanisms have significantly improved operational coordination amongst law enforcement agencies, given the amount of jurisdictional overlap amongst the relevant law enforcement agencies, there remains a need for more refined coordination.

1117. With regards to the securities sector, the SEC and the SROs all reported during the on-site visit that they experience very good interagency coordination. As well, no issues were raised concerning interagency cooperation in the insurance and MSB sectors.

1118. In the banking sector, private sector representatives noted that, historically, approaches taken by the various banking regulators towards supervision and examination have not always been consistent. Consequently, the development and issuance of the common manual for BSA examination has been strongly welcomed by the private sector. At the time of the on-site visit, this FFIEC manual had only been in existence for seven months, so it is too early to draw any final conclusions about its effectiveness in improving domestic cooperation and coordination; however, it is a promising step.

6.1.2 Recommendations and Comments

1119. Overall, the U.S. has implemented sufficient policy- and operational-level mechanisms to facilitate interagency cooperation and coordination at all levels. However, the U.S. should continue to work towards closing the gap that still seems to remain between the policy level and the factual operational law enforcement work. The HIFCA and HIDTA model seems to be generally effective, provided that it is appropriately resourced and developed. The assessment team is of the view that, with appropriate monitoring, it would be beneficial to expand this initiative and allocate additional resources to it.

1120. At the operational level, there is a great deal of overlap between the jurisdictions of the various law enforcement agencies. This creates the need for more refined coordination. The fact that the Treasury recently has presented a government-wide analysis on money laundering could create an opportunity to evaluate the present fragmented Law Enforcement system. Such a study should not lead to the creation of new entities, but rather initiate a discussion on the basic law enforcement framework in a system as complex as that in the U.S.

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	LC	• There remains a gap between the policy level and operational level law enforcement work. • More refined coordination is needed amongst law enforcement agencies with overlapping jurisdictions.

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

Recommendation 35 and Special Recommendation I:

1121. The U.S. ratified the Vienna Convention on 20 February 1990. The U.S. signed the Palermo Convention on 13 December 2000 and ratified it on 3 November 2005.

1122. The U.S. has adopted a range of measures to substantially implement the Vienna and Palermo Conventions. However, some aspects of these Conventions have not been completely implemented. In particular, not all conduct specified in Article 3 (Vienna) and Article 6 (Palermo) has been criminalized. Additionally, the U.S. system does not include a sufficiently comprehensive list of foreign predicates related to organized criminal groups as required by Article 6(2)(c) of the Palermo Convention.

1123. The U.S. ratified the UN Convention for the Suppression of the Financing of Terrorism on 26 June 2002. Title II of Public Law 107-197, the "Suppression of the Financing of Terrorism Convention Implementation Act of 2002," created a new Section 2339C in Title 18 of the U.S. Code

(Prohibitions against the financing of terrorism) which implements Article 2 of the Convention. This section as well as sections 2339A and 2339B is discussed in Section 2.2.

1124. As discussed in section 2.4 of this report, the U.S. has sufficiently implemented S/RES/1373(2001) and is substantially in compliance with S/RES/1267. In its report dated 17 April 2003 to the UN Security Council 1267 Committee[117], the U.S. government confirmed that its administration of sanctions imposed pursuant to EO 13224 (which deals with blocking property and prohibiting transactions with persons who commit or support terrorism) through OFAC as the way in which the 1267 Committee's List has been incorporated into the U.S. legal system. EO 13224 is also discussed above in section 2.4. The preamble to EO 13224 notes that the Order is made pursuant to the authority of various U.S. statutes[118] and in view of UN Security Council Resolutions 1214 (8 Dec 1998), 1267 (15 Oct 1999) and 1333 (19 Dec 2000).

Additional elements

1125. The U.S. signed the Inter-American Convention against Terrorism on 3 June 2002 and ratified it on 15 November 2005.

6.2.2 Recommendations and Comments

1126. The U.S. has ratified and substantially implemented the relevant sections of the Vienna, Palermo and Terrorist Financing Conventions. The U.S. should, in particular, review its money laundering offenses to ensure that all conduct specified by the Vienna and Palermo Conventions is covered. Additionally, the U.S. should include a sufficiently comprehensive list of foreign predicates as required by Article 6(2)(c) of the Palermo Convention. The U.S. should also transpose all S/RES/1267(1999) designations in the OFAC list.

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	LC	• Not all conduct specified in Article 3 (Vienna) and Article 6 (Palermo) has been criminalized, and there is not a sufficiently comprehensive list of foreign predicates related to organized criminal groups as required by Article 6(2)(c) (Palermo).
SR.I	LC	• Not all S/RES/1267(1999) designations are transposed in the OFAC list.

6.3 Mutual Legal Assistance (R.36-38 & SR.V)

6.3.1 Description and Analysis

Recommendation 36 and Special Recommendation V (Mutual Legal Assistance)

1127. All legal assistance requests are channeled through the Office of International Affairs of the Department of Justice (OIA) that serves as the U.S. Central Authority for all such matters. The OIA, as the conduit for mutual legal assistance (MLA) requests coordinates all international evidence gathering. OIA has attorneys and support staff with responsibilities and expertise in various parts of the world and different substantive areas. Typically, at least one OIA attorney will have primary responsibility for coordinating all incoming and outgoing mutual legal assistance and extradition requests for every country in the world, and in some cases an OIA attorney is also posted overseas in the U.S. embassies.

[117] This report was submitted by the U.S. in accordance with paragraph 6 of resolution 1455 (2003) and follows the template suggested by the 1267 Committee in its Guidance for these reports.

[118] IEEPA (50 USC 1701), the National Emergencies Act (50 USC 1601), section 5 of the UN Participation Act 1945 (22 USC 287c) and Title 3 Section 301 of the USC.

1128. Mutual Legal Assistance Treaties (MLATs) provide the normal appropriate basis for executing requests. As of 19 July 2005, the U.S. has 50 bilateral MLATs in force.[119] The following other arrangements also further the expediency of the MLA process.

(a) An agreement was entered into on 25 June 2003 between the U.S. and the EU concerning mutual legal assistance which, among other things, provides a mechanism for more quickly exchanging information regarding bank accounts held by suspects in criminal investigations. The OIA and the State Department are now in the process of concluding implementing bilateral agreements with each member of the European Union;

(b) International multilateral conventions providing for mutual legal assistance, including: the Inter-American Convention on Mutual Legal Assistance of the Organization of American States; the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism; and the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances; the United Nations Convention against Transnational Organized Crime; and

(c) Executive agreements for cooperation in criminal matters with the People's Republic of China (PRC) and Taiwan.

1129. The U.S. can also respond to requests in the form of letters rogatory on an ad hoc basis.

Range of mutual legal assistance provided

1130. Generally, the U.S. government is able to provide a very wide range of mutual legal assistance in AML/CFT investigations, prosecutions and related proceedings. The range of legal assistance provided in its bilateral mutual legal assistance treaties (MLAT) is substantial and includes:

(a) taking the testimony or statements of persons;

(b) providing documents, records, and other items;

(c) locating or identifying persons or items;

(d) serving documents;

(e) transferring persons in custody for testimony or other purposes;

(f) executing searches and seizures;

(g) assisting in proceedings related to immobilization and forfeiture of assets and restitution;

(h) collection of fines; and

(i) any other form of assistance not prohibited by the laws of the Requested State.

1131. Pursuant to multilateral treaties that the U.S. is party to, such as the 1988 Vienna Convention and the 1999 UN Terrorism Financing Convention, the U.S. can also provide wide measures of mutual legal assistance to foreign authorities for criminal investigations, prosecutions and related proceedings for offenses covered by these conventions.

[119] Namely with the following countries: Antigua and Barbuda, Argentina, Australia, Austria, the Bahamas, Barbados, Belgium, Belize, Brazil, Canada, Cyprus, Czech Republic, Dominica, Egypt, Estonia, France, Grenada, Greece, Hong Kong (SAR), Hungary, Israel, Italy, Jamaica, Latvia, Liechtenstein, Lithuania, Luxembourg, Mexico, Morocco, the Netherlands (including its Caribbean territories - Aruba and the Netherlands Antilles), Nigeria, Panama, the Philippines, Poland, Romania, Russia, South Africa, South Korea, Spain, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Switzerland, Thailand, Trinidad and Tobago, Turkey, Ukraine, the United Kingdom, the United Kingdom with respect to its Caribbean overseas territories (Anguilla, the British Virgin Islands, the Cayman Islands, Montserrat, and the Turks and Caicos Islands), and Uruguay. MLATs have been signed but have not yet taken effect with the following countries: Colombia, Germany, India, Ireland, Japan, Sweden and Venezuela.

1132. Apart from foreign requests for assistance on a treaty basis, the U.S. also responds to requests in the form of a letter rogatory on an ad hoc basis and through direct letters of request by Ministries of Justice. In such a case, the OIA (through which all such requests are routinely channeled) can seek the appointment of a commissioner pursuant to 28 USC 1782, when compulsory process is necessary to obtain the requested assistance. The authority of commissioners appointed pursuant to section 1782 is limited. They are only authorized to issue subpoenas to compel testimony as well as the production of documents and other items for use in foreign proceedings, excluding search warrants and other compulsory measures. OIA can seek authorization from a federal judge for search warrants and other compulsory measures. Any person can voluntarily give testimony or produce documents or surrender other items for use in any foreign proceeding.

1133. Execution of incoming requests for assistance is organized in close cooperation/coordination between OIA and other law enforcement authorities, typically the FBI, the U.S. Marshals Service (USMS), and/or Interpol Washington. The USMS is responsible for locating and arresting fugitives sought for extradition by foreign authorities. At the request of the OIA, FBI Special Agents are tasked to collect evidence sought by foreign authorities, the gathering of which does not require the use of compulsory process. To facilitate this coordination, a Deputy U.S. Marshal and an FBI Special Agent are detailed to OIA. OIA also works with International and National Security Coordinators designated in each of the 94 USAOs located throughout the U.S. Although no statistics were available on the duration of the processing of the MLA requests, there are no reports or indications of undue delays or non-executions.

1134. Pursuant to formal mutual legal assistance requests, the U.S. can also provide assistance in the freezing, seizure, and confiscation of assets. When a mutual legal assistance request seeks the freezing, seizure, or confiscation of assets, OIA works closely with the DOJ's Asset Forfeiture Money Laundering Section and a network of asset forfeiture experts in the USAOs located throughout the U.S. to provide the requested assistance.

1135. Federal law enforcement agencies may also enter into case-specific MOUs with other countries for money laundering and the financing of terrorism investigative assistance. These are purely operational tools and are not legally binding. No comprehensive statistics are kept concerning these case-specific agreements.

Prohibitions and conditions

1136. Mutual legal assistance is not subject to excessive conditions. For instance, the fact that no judicial proceedings have been initiated in the requesting country or a conviction has not yet been obtained is no ground for refusal. Title 28 USC 1782 even specifically authorizes assistance for "criminal investigations conducted before formal accusation." U.S. MLATs are based on the principle of reciprocity in the investigation and prosecution of crime. Furthermore most U.S. MLATs cover a broad range of crimes without requiring that a request for assistance relate to activity that would be criminal in the requested state, although some MLATS still require dual criminality in respect of coercive measures.

1137. Most of the bilateral MLATs entered into by the U.S. contain no dual criminality requirement as a condition for granting assistance. Furthermore, there is no dual criminality requirement for court orders issued pursuant to 28 USC 1782.[120] For the treaties with dual criminality provisions, those provisions are mostly limited to requests for assistance requiring compulsory or coercive measures.

1138. Dual criminality does not affect terrorism-related MLA procedures, as the scope of terrorism related offenses is quite broad under U.S. law and largely corresponds with the definitions provided in the Terrorist Financing Convention.

[120] According to section 1782, a court may order a person to give testimony or a statement, or produce a document or other thing "for use in a proceeding in a foreign or international tribunal, including criminal investigations conducted before formal accusation".

1139. The fact that a MLA request contains fiscal aspects is not considered a ground for refusal. In fact, although some MLATs include an exemption on purely fiscal matters, the U.S. does not have a general law or policy prohibiting mutual legal assistance for these types of offenses.[121] Further to this, as provided for in the UN Terrorist Financing Convention, a request for mutual legal assistance in a terrorism financing matter is never refused on the grounds that it concerns a fiscal offense.

1140. Information is readily provided from banks, financial institutions and the DNFBP located in the U.S., if needed by way of court order. Information properly protected by the attorney-client privilege is, however, exempted from disclosure. Nevertheless, attorney-client privilege can be overcome where it can be shown that the attorney in question was actively participating in the criminal activities of his client (crime fraud exception).

Powers of competent authorities when responding to MLA requests

1141. OIA and other U.S. authorities helping OIA to execute foreign requests have the authority to obtain documents and information for use in ML and FT investigations and in prosecutions and related proceedings. The extent of the authority will depend on the legal basis for the request, in particular whether there is an applicable bilateral MLAT or multilateral convention. Even in the absence of an applicable treaty or convention, OIA may seek the appointment of a commissioner pursuant to 28 USC 1782 in response to any rogatory request or letter request from a foreign authority. The commissioner has the authority to order someone to give testimony or produce a document or other evidence "for use in a proceeding in a foreign or international tribunal, including criminal investigations conducted before formal accusation.". As stated above, their authority does not extend to search or seizure warrants.

1142. FinCEN also has the authority to respond to requests for lead information and has procedures in place to facilitate this. It routinely responds to requests for information from foreign FIUs and serves as a conduit for domestic law enforcement requests directed to foreign FIUs for information in support of their investigative efforts.

Conflicts of jurisdiction

1143. When OIA receives a request for mutual legal assistance relating to a criminal investigation or prosecution overlapping with an ongoing U.S. criminal investigation or prosecution, OIA generally encourages the foreign and U.S. prosecuting authorities to communicate and work out, wherever possible, a mutually beneficial cooperative arrangement. If a mutually agreeable arrangement cannot be worked out by the U.S. and foreign prosecuting authorities, OIA will not generally deny a request for assistance but, depending on the precise terms of any applicable treaty, execution of the assistance request may be postponed until such time that its execution will no longer interfere with the ongoing U.S. criminal investigation. There is also the possibility for the U.S. to waive its authority and hand over the criminal case to the foreign jurisdiction (and vice versa), although this procedure is said to be an exception to the norm.

Additional elements

1144. Requests for formal mutual legal assistance in a criminal investigation or proceedings, in particular any requests necessitating the use of compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence in the U.S. cannot be made directly to the prosecutorial or law

[121] For instance the MLATs between the U.S. and Switzerland, the Bahamas and the Cayman Islands exclude fiscal matters, including offenses involving taxes, customs duties, governmental monopoly charges and/or exchange control regulations, from the scope of available assistance. Assistance is however generally available for criminal tax matters relating to the proceeds from criminal offenses.

enforcement authorities. They must be directed to OIA, which serves as the U.S. central authority for all formal mutual legal assistance requests.

Recommendation 37 and Special Recommendation V (dual criminality relating to MLA and extradition)

1145. Most of the bilateral MLATs entered into by the U.S. contain no dual criminality requirement as a condition for granting assistance. For the treaties with dual criminality provisions, those provisions are mostly limited to requests for assistance requiring compulsory or coercive measures. Furthermore, there is no dual criminality requirement for court orders issued pursuant to 28 USC 1782 in aid of requests for assistance from foreign authorities. The requirement also does not affect mutual legal assistance in TF matters as the Terrorist Financing Convention applies here.

1146. However, considering the ML offense under 18 USC 1956 and 1957 is not an "all crimes" offense but limited to a series of predicate offenses, it is not to be excluded that MLA may be negatively affected by the dual criminality requirement, especially when coercive measures are called for. This particularly may be the case when the foreign request is based on money laundering activity that is not specified in terms of the predicate criminal activity, either because the predicate is unknown or there is no legal requirement in the requesting country to identify the predicate offense. Moreover the U.S. authorities indicated that, as the delivery of a search warrant is subject to the probable cause examination by the court, the non-specification of the predicate could also be problematic in that respect.

1147. When dual criminality issues do arise under certain treaties, technical differences between the categorization of the crime in the U.S. and requesting state do not affect the provision of the requested assistance. The qualification of the offense is irrelevant, as long as the underlying acts are punishable in both states. In the case of extraditions, the U.S. Supreme Court has held that dual criminality requirement "does not require that the name by which the crime is described in the two countries shall be the same; nor that the scope of liability be coextensive, or, in other respects, the same in the two countries. It is enough if the particular act charged is criminal in both jurisdictions." The same principle applies to mutual legal assistance requests made pursuant to treaties that include a dual criminality requirement.

Recommendation 38 and Special Recommendation V (MLA – Freezing, seizing and confiscation)

Mechanisms to respond to requests for identification, freezing, seizing and confiscation

1148. There are a number of mechanisms in place through which assistance can be given to other governments in confiscation proceedings. Assistance in tracing and identifying assets normally does not necessitate formal proceedings and can mostly be done in an informal way via police-to-police communication (foreign law enforcement attachés.) Obtaining evidence and implementing coercive measures on criminal assets typically require formal requests, generally on a treaty or agreement basis. This is done either by the U.S. authorities enforcing the foreign court order or by initiating their own (criminal or civil) seizure/confiscation proceedings. Such actions may be applied to requests for the identification, freezing, seizure or confiscation of proceeds or the instrumentalities of crime.

1149. If the U.S. initiates a criminal or civil confiscation action, whether on its own initiative or at the request of a foreign country, it may seize or restrain the assets subject to confiscation pending further judicial proceedings. The U.S. can also restrain property located in the U.S. at the request of a foreign country where there is a treaty or agreement that provides for forfeiture cooperation in order to preserve the property in anticipation of receiving an enforceable foreign judgment of confiscation.

Procedures if the U.S. plans to open its own criminal or civil confiscation action

1150. If the U.S. authorities opt for a separate confiscation action, they can restrain assets as in any other civil *in rem* confiscation action upon a showing of probable cause that the property is subject to confiscation to the U.S. The foreign government must then provide evidence sufficient for the U.S. to

establish probable cause of a predicate offense for confiscation under U.S. law. Upon receipt of such evidence, the U.S. judicial authorities may seek a pre-trial seizure warrant, a restraining order immobilizing the property, or an arrest warrant *in rem* for the property, and would simultaneously or subsequently file a civil or criminal confiscation action. Criminal seizure is however only possible in conjunction with a criminal prosecution based on a violation of U.S. statutes.

1151. Property can be restrained without probable cause for 30 days (extendable) if the foreign country has arrested or charged someone in connection with criminal conduct that would serve as a basis for the U.S. seeking independent confiscation of the property. An independent domestic forfeiture action can be initiated against property involved in eleven categories of foreign offenses that are deemed specified unlawful activities under 18 USC 1956(c)(7)(B). In addition, forfeiture is also available for property involved in other foreign crimes (which domestic counterpart would be an SUA) where the proceeds or other objects of the offense travel through interstate or foreign commerce.

Procedures if the U.S. anticipates enforcing a final foreign judgment for criminal or civil confiscation

1152. The U.S. can enforce both property focused and value based judgments. In order for the U.S. to enforce a foreign confiscation judgment under 28 USC 2467, the requesting state seeking enforcement of its judgment must be a party to the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances or to a treaty or other international agreement with the U.S. that provides for confiscation assistance. In anticipation of a foreign criminal or *in rem* confiscation judgment property can also be restrained either by registering and enforcing a foreign restraining order or by seeking a U.S. restraining order based upon an affidavit from the foreign authorities as prescribed by 28 USC 2467(d)(3)(B)(i).

1153. In order to use one of these bases to restrain property in anticipation of enforcing a foreign judgment, a Temporary Restraining Order (TRO) can be issued under the procedures of 18 USC 983(j) when it is established that there is a reasonable basis to believe that the foreign government will issue an enforceable final confiscation judgment 18 USC 983(j). In the event a civil complaint has been filed against the property, alleging that the property to which the order is sought is subject to civil forfeiture, the restraining order will continue in effect for 90 days. In order to maintain the restraint, evidence must be presented that there is a substantial likelihood that the foreign government will issue an enforceable final confiscation order that would be enforceable under U.S. law. In some instances the 90 day limit can be extended by the court.

1154. The principle of dual criminality may also cause problems in registering and enforcing foreign criminal or *in rem* confiscation judgments in money laundering cases where the predicate offense falls outside the categories of foreign offenses for which initiation of an independent U.S. criminal action is authorized. In that case, only when the violation of foreign law would also constitute a violation for which confiscation would be available if the crime were committed in the U.S., the U.S. can enforce a foreign confiscation judgment. Such foreign confiscation judgments can be confiscation orders directed at particular property or value judgments ordering a defendant to pay a sum of money. An additional question relates to the controversy about the validity of the seizure orders or warrants issued by investigating magistrates in civil law jurisdictions, as these may not be generally accepted in the U.S. as "court orders". This issue remains, however, untested under section 2467.

Powers to confiscate property

Criminal (in personam) confiscation actions

1155. A criminal *in personam* confiscation action depends on a criminal conviction against the defendant. Where a foreign government seeks confiscation assistance in connection with a foreign offense, criminal prosecution often is not possible in the U.S. because the underlying offense occurred outside U.S. jurisdiction or because the defendant is not located in the U.S. This means that most often the U.S. would execute a request for confiscation assistance by initiating civil *in rem* proceedings.

Civil (in rem) confiscation actions

1156. Because U.S. civil *in rem* confiscation authority generally permits the confiscation of property only if involved in or derived from the offense, the property must be traced to the criminal offense. An exception applies in cases involving electronic funds in a bank account, which are considered fungible, making strict tracing to the offense unnecessary as long as the confiscation action is commenced within one year of the offense (18 USC 984).

1157. A conviction for the underlying criminal offense in the foreign country is not required. Generally, this procedure of initiating independent confiscation proceedings in the U.S. seems efficient as it provides greater flexibility and more rapid authority to impose a provisional restraint. Although there are some limitations to the ability for the U.S. to offer full assistance, criminal forfeiture is not possible when there is no offense under U.S. criminal law (foreign offense, no predicate offense under U.S. law), while equivalent value confiscation is impossible in civil forfeiture proceedings.

1158. The U.S. can seek the registration and enforcement of a foreign forfeiture judgment whether it is for specific property or is an order to pay a sum of money. Where the foreign judgment is an order to pay a sum of money, the exchange rate in effect at the time that the application to enforce the foreign judgment is filed will be used in calculating the amount of the judgment (28 USC 2467).

Freezing, seizure and confiscation of property of corresponding value

1159. Pre-trial seizure of untainted property to safeguard the execution of a money judgment in a criminal prosecution is generally not considered possible by U.S. jurisprudence on the grounds that the untainted property is not "involved in" or "traceable to" an offense. This raised the question if this limitation would not also affect the ability for the U.S. to enforce such foreign seizure orders. Nothing in 28 USC 2467, however, prevents the authorities from restraining such assets in the U.S. as long as these are subject to forfeiture and provided all the other requirements are met, regardless of whether the assets are actual proceeds or represent equivalent value. This assumption was recently confirmed by a ruling of the DC District Court that allowed the pre-trial restraint of untainted property at the request of a foreign jurisdiction.

Arrangements for coordinating seizure and confiscation actions

1160. Coordination with other countries on seizure and confiscation is facilitated by the OIA along the same lines as the MLA process. Moreover, the U.S. has also entered into executive agreements on forfeiture cooperation, including: (1) an agreement with the United Kingdom providing for forfeiture assistance and asset sharing in narcotics cases; (2) a forfeiture cooperation and asset sharing agreement with the Kingdom of the Netherlands; and, (3) a drug forfeiture agreement with Singapore. The U.S. has asset sharing agreements with Canada, the Cayman Islands (which was extended to Anguilla, British Virgin Islands, Montserrat, and the Turks and Caicos Islands), Colombia, Ecuador, Jamaica, Mexico and the United Kingdom.

Asset forfeiture funds

1161. The use of forfeiture funds is an integral part of the forfeiture system in the U.S. Confiscated assets are deposited in one of the following two forfeiture funds:

(a) the Justice Forfeiture Fund (JFF), established in 1984, into which all forfeited cash and proceeds from the sale of forfeited property are to be deposited (28 USC 524). Interest from the investment of JFF balances and interest from the Seized Asset Deposit Fund are also deposited into the JFF.[122]

[122] See Section 2.3.1, paragraphs 240 to 243 for statistical details.

(b) the Treasury Forfeiture Fund (TFF) (31 USC 9703) since 12 October 1993 receives the proceeds of all forfeitures that have occurred as a result of a law enforced or administered by a Treasury law enforcement organization or those law enforcement agencies that are now part of the Department of Homeland Security.[123] Interest from the investment of TFF balances and interest from seized funds held in the Suspense Account are also deposited into the TFF.

1162. The use of JFF and TFF funds is strictly defined and is generally intended to cover asset management and case-related expenses, payment of qualified third-party interests, sharing payments, program management and investigative expenses. Also, the TFF and JFF funds are used to support the investigative needs of the participating agencies, such as case-related travel, law enforcement equipment, translation/transcription of documents, investigative databases/data mining systems, and agent training.

Sharing of confiscated assets

1163. It is U.S. policy and practice to share the proceeds of successful forfeiture actions with countries that made possible, or substantially facilitated, the forfeiture of assets under U.S. law. The level or amount of sharing is in direct relationship with the importance and degree of the foreign assistance. From 1989 through June 2005, the international asset sharing program administered by the DOJ shared USD 227,886,820.94 with thirty-three foreign governments which cooperated and assisted in the investigations. From FY 1994 through December 2004, the international asset sharing program administered by the Department of Treasury shared USD 27,408,032.00 with twenty foreign governments which cooperated and assisted in investigations.

1164. Similarly, the U.S. has received a share of forfeited assets from other countries. Such shared proceeds are deposited into the JFF or the TFF, as appropriate, and made available for law enforcement purposes.

Effectiveness of measures relating to mutual legal assistance

1165. The capability and willingness of the U.S. for cross-border cooperation generally, and on AML/CFT specifically, is quite evident. Although based primarily on treaties and multilateral conventions allowing for extensive assistance, mutual legal assistance may also be granted in response to and on the sole ground of letters rogatory, although this can prove somewhat restricted in terms in respect of coercive measures. These restrictions are, however, not unreasonable and remain within the internationally accepted standard.

1166. The following chart sets out the number of incoming and outgoing mutual legal assistance requests (including requests relating to the freezing, seizing and confiscation of property) from the period 1 January 2000 to 22 July 2005.

MLA requests related to money laundering

NATURE OF THE REQUEST: Incoming MLA requests related to money laundering and criminal forfeiture	
Granted	496
Denied (reasons include lack of evidence, offense not covered by treaty, and unable to execute the request)	36
Pending	313
Other (includes canceled, deceased person, request not sufficient to proceed, no response from requestor, withdrawn, and partially granted)	139
Inexecutable under U.S. law	3
TOTAL NUMBER OF REQUESTS	987

[123] See Section 2.3.1, paragraphs 240 to 243 for statistical details.

NATURE OF THE REQUEST: Outgoing MLA requests related to money laundering and criminal forfeiture	
Granted	605
Denied (reasons include denied by U.S. Court, jurisdiction problems, and unable to execute)	12
Pending	521
Other (includes canceled, request not sufficient to proceed, no response from requestor, partially granted, referred to other office for response, and withdrawn)	321
Inexecutable under foreign law	5
TOTAL NUMBER OF REQUESTS	1,464

MLA requests related to terrorist financing

NATURE OF THE REQUEST: Incoming MLA requests related to financial transactions with a designated country/terrorism and providing material support or resources/terrorism	
Granted	17
Pending	18
Other (includes assistance no longer needed)	2
TOTAL NUMBER OF REQUESTS	37
NATURE OF THE REQUEST: Outgoing MLA requests related to financial transactions with a designated country/terrorism and providing material support or resources/terrorism	
Granted	44
Denied (grounds include lack of dual criminality)	2
Pending	67
Other (includes cancelled, partially granted and withdrawn)	20
TOTAL NUMBER OF REQUESTS	133

1167. The total number of exchanges shows a frequent use of the MLA process as is to be expected with cross-border phenomena as ML and FT. However, the number of denied incoming requests seems rather high in proportion.. According to OIA this is mainly a quality issue in that there is a lack of connection between the crime under investigation or prosecution and the evidence being sought.

1168. The system for providing international cooperation in relation to freezing, seizure and confiscation is notable for its flexibility which assists in achieving maximum efficiency. If for some reason an MLA request cannot directly be complied with in its own right, the U.S. authorities can seek implementation by initiating their own procedures based on a violation of U.S. statutes, with the only condition that the underlying activity can be translated in a criminal act punishable under U.S. law. This is particularly important within the context of foreign seizure and confiscation requests that can be met either through enforcement of the foreign order or by the U.S. authorities initiating their own criminal or civil forfeiture proceedings.

1169. The generally comprehensive and robust MLA system is however marred by some (minor) issues. First, it should make no difference to the U.S. whether the foreign seizure or other coercive order is issued by a court or by an investigation judge operating within a civil law jurisdiction whose warrants are equivalent to a court order. These latter are the subject of a controversy about the validity of the seizure orders or warrants issued by civil law jurisdiction investigating judges which are not generally accepted in the U.S. as "court orders".

1170. Also, the dual criminality principle again may prove problematic when registering and enforcing foreign criminal or *in rem* confiscation judgments in money laundering cases where the predicate offense falls outside eleven categories of foreign offenses for which initiation of an independent U.S. criminal action is authorized. In that case, only when the violation of foreign law would also constitute a violation for which confiscation would be available if the crime were

committed in the U.S., the U.S. can enforce a foreign confiscation judgment. Such foreign confiscation judgments can be confiscation orders directed at particular property or value judgments ordering a defendant to pay a sum of money.

6.3.2 Recommendations and Comments

1171. The U.S. MLA system is generally comprehensive and robust. To complete this system, the following issues need to be addressed. The introduction of equivalent value seizure in the U.S. legal system will provide for a formal legal basis for the implementation of such measures upon a foreign request. Also, the U.S. may not be able to provide mutual legal assistance in circumstances where the request relates to underlying conduct that has not been made a predicate offense for money laundering in the U.S. (see the discussion in section 2.1 of this report). Although there is no international standard imposing an "all crimes" money laundering offense, the U.S. is not fully compliant in respect of the designated predicate offenses, so the predicate list should at least be extended in that sense.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
R.36	LC	• Dual criminality may impede MLA where the request relates to the laundering of proceeds that are derived from a designated predicate offense which is not covered.
R.37	C	• This Recommendation is fully observed.
R.38	LC	• Dual criminality may impede MLA where the request relates to the laundering of proceeds that are derived from a designated predicate offense which is not covered.
SR.V	LC	• With regards to these elements, this Recommendation is fully observed.

6.4 Extradition (R.39, 37 & SR.V)

6.4.1 Description and Analysis

Recommendation 39 and Special Recommendation V (Extradition)

Extradition procedures

1172. Extraditions from the U.S. are generally governed by Chapter 209 of Title 18 USC 3181-3186. Pursuant to 18 USC 3184, offenses are extraditable when "provided for by" the extradition treaty or convention in force between the U.S. and the requesting country. As of July 2005, the U.S. had bilateral extradition treaties in force with over 115 countries. U.S. extradition treaties negotiated during approximately the last 40 years generally rely on the dual criminality principle rather than a list of crimes covered by the treaty, thus permitting extradition when, in general, the act in question is a serious crime in both countries. However, there are some exceptions to the treaty requirement:

(a) Section 3181(b) allows for the surrender of persons, other than U.S. citizens or residents of the U.S., who have committed crimes of violence against nationals of the U.S. in foreign countries when certain criteria are fulfilled.

(b) Chapter 209 of Title 18 is applicable to extraditions from the U.S. to the International Tribunal for Yugoslavia and the International Tribunal for Rwanda based upon agreements entered into between the U.S. and these tribunals.

1173. The OIA and the Department of State coordinate and review all extradition requests received from foreign countries. In urgent circumstances fugitives can be provisionally arrested in advance of the receipt of a formal extradition request. The request is subject to court scrutiny on whether:

(a) there are criminal charges pending or an outstanding sentence against the individual before the court;

(b) the charges are included under the treaty as extraditable offenses; and

(c) there is probable cause to believe that a crime was committed.

1174. The final decision to surrender the fugitive rests with the Secretary of State.

Extraditable offenses

1175. The United States extradites defendants only if the there is a bilateral extraditon treaty between the U.S. and the requesting state. Money laundering, as defined by U.S. law, is an extraditable offense for requests made under the dual criminality treaties. When extradition is governed by a treaty that lists the extraditable offenses, however, extradition will depend on what offenses are listed in that treaty. Finally, regarding States with which the U.S. has a bilateral extradition treaty, extradition is also possible pursuant to multilateral conventions, such as Article 3 of the Vienna Convention (for narcotics-related money laundering offenses) and Article 6 of the Palermo Convention (for organised crime offenses, where the U.S. and requesting States are both parties. Those multilateral treaties "deem" offenses established by those conventions to be included in the extraditable offenses listed in the relevant bilateral treaty.

1176. The U.S. vigorously combats any form of or participation in terrorism and actively pursues a policy of bringing suspect individuals to justice, domestic or foreign. Terrorism and terrorist financing offenses are considered extraditable offenses for requests made under the dual criminality treaties. However, whether these offenses are extraditable under extradition treaties that list the extraditable offenses will depend on what offenses are listed in the treaty, or on the requesting country and the U.S. 1) having a bilateral extradition treaty and 2) both being party to relevant multilateral conventions, such as the UN Terrorist Financing Convention, which makes all offenses covered by its Article 2 extraditable. Although U.S. extradition law and treaties foresee the possibility to refuse extradition on the grounds of the offense having a political character, U.S. jurisprudence has provided that terrorist acts or the financing thereof do not fall within the political offense exception.

1177. The dual criminality principle is to be understood as permitting extradition when, in general, the act in question is a serious crime in both the requesting country and the U.S. Technical differences between the categorization of the crime in the U.S. and requesting state do not prevent granting extradition. The question is not how the crimes are categorized, but whether the underlying acts are punishable in both states. This interpretation has constantly been upheld by the courts. However, even then it is quite conceivable that the limitation in respect of the predicate offenses may jeopardize an extradition request based on money laundering if it relates to predicate activity outside the U.S. list.

Extradition of U.S. nationals

1178. The U.S. has no law barring the extradition of its nationals. Moreover, the Secretary of State may authorize the extradition of U.S. nationals even in cases where the applicable bilateral extradition treaty does not require the extradition of nationals. 18 USC 3196. Although rather exceptional in practice, there is no legal impediment in principle for the U.S., instead of extraditing, to take over the foreign case and initiate its own criminal proceedings if the case in some way or another falls under U.S. jurisdiction.

Timeliness of handling extradition requests

1179. The centralizing and coordinating function of the OIA of the DOJ is aimed at ensuring an expedient processing of extradition requests and proceedings. Although no statistics were available on the duration of the extradition proceedings, it was stated that the handling of an unchallenged extradition is a matter of a few weeks up to two months, as consent to extradition eliminates the necessity of the court conducting a hearing to determine whether the fugitive is extraditable. In case the extradition request is seriously challenged in court, the delay can be substantially longer.

Additional elements

1180. Most recent extradition treaties permit the direct transmission of provisional arrest requests between OIA (as the designated representative of the U.S. DOJ) and the Justice Ministry of the foreign state. Persons cannot be extradited from the U.S. based simply upon the presentation of a foreign arrest warrant, however, a certified copy of a foreign conviction for an extraditable offense will generally be sufficient proof during the extradition proceedings. Fugitives sought for extradition by foreign states can either "waive" or "consent" to extradition at any point during the extradition process in the U.S. A fugitive who elects to waive extradition can be removed as soon as foreign authorities can arrange to travel to the U.S. to take custody of the fugitive. A fugitive can also elect to consent to extradition. It takes a bit longer to process a consent to extradition because the State Department has up to two months to issue the surrender warrant before foreign authorities can take custody of the fugitive. Finally, the U.S. can make use of immigration laws to remove and expel fugitives sought for extradition by foreign countries and return them to their country of origin.

Effectiveness of measures relating to extradition

1181. The U.S. extradition regime, based on a network of treaties supplemented by conventions, is underpinned by a solid legal framework allowing for an efficient and active use of the extradition process. The shift from rigid list based treaties to agreements primarily based on dual criminality has given the system much more flexibility and opportunities. The possibility to extradite their own nationals is an additional asset that can assist in dealing with issues of double jeopardy, jurisdiction and coordination. The following statistics cover the period between 1 January 2000 and 22 July 2005. No statistics per annum were provided.

Extradition requests related to money laundering

NATURE OF THE REQUEST: Incoming Extradition requests related to money laundering	
Granted (includes deportation, and waiver of extradition)	6
Denied (grounds for denial include double jeopardy, lack of evidence, extradited to another country, and unable to execute)	5
Pending	24
Other (includes arrested in requesting country, request not sufficient to proceed, and withdrawn)	19
TOTAL NUMBER OF REQUESTS	54
NATURE OF THE REQUEST: Outgoing Extradition requests related to money laundering	
Granted (includes deportation, expulsion, returned voluntarily, and waiver)	169
Denied (includes lack of dual criminality, lack of evidence, statute of limitations, charges dismissed and unable to execute)	22
Pending	274
Other (includes arrested in requesting country, located/arrested in another country, request not sufficient to proceed, and withdrawn)	89
TOTAL NUMBER OF REQUESTS	554

Extradition requests related to terrorism financing

NATURE OF THE REQUEST: Incoming extradition requests related to financial transactions with a designated country/terrorism and providing material support or resources/terrorism	
TOTAL NUMBER OF REQUESTS	0
NATURE OF THE REQUEST: Outgoing Extradition requests related to financial transactions with a designated country/terrorism and providing material support or resources/terrorism	
Granted (includes deportation)	2
Denied (includes double jeopardy)	2
Pending	7

Other (includes deceased person, located/arrested in another country and withdrawn)	4
TOTAL NUMBER OF REQUESTS	15

1182. These figures show an active use of the extradition process by the U.S. authorities, both in ML and TF. Conversely the number of extradition requests to the U.S. is relatively low (ML) or even nil (TF). Again one notices a proportionally rather high incidence of refusals and non-execution of incoming extradition requests.

1183. As with mutual legal assistance, the limitation to the ML offense in terms of predicate criminality may constitute a negative element in the light of the dual criminality condition. Indeed, if (in case of a non U.S. listed underlying offense) the facts cannot be translated to a criminal conduct punishable under U.S. law, the dual criminality principle will not be met and extradition may be obstructed or prohibited.

1184. Dual criminality does not affect terrorism-related extradition procedures, as the scope of terrorism related offenses is quite broad under U.S. law and largely corresponds with the definitions provided in the Terrorist Financing Convention.

1185. The older, list based extradition treaties that were concluded before the introduction of money laundering and terrorism financing offenses in the respective legislations and that have not been supplemented since, may also prove to cross the extradition process if the underlying criminal conduct constituting the money laundering or terrorism financing activity cannot be translated in an offense included in the treaty list and no multilateral convention can be invoked because of the absence of mutuality. Even if this situation has not occurred yet and may be considered rather exceptional, this eventuality needs to be addressed. Besides completing the "list" treaties by adding ML and TF offenses, consideration may be given allowing extradition according to the principles of the UN TF Convention on an ad hoc and unilateral basis. In addition, it has been noted that a new fast-track extradition treaty with the U.K., introduced specifically to expedite the transfer of terrorist suspects, has not been ratified by Congress some three years after its signature. Apparently, this delay has been caused by concerns among certain members of Congress that the treaty may be used to extradite Irish Republican Army suspects.

6.4.2 Recommendations and Comments

1186. The list of designated predicate offenses for money laundering should be extended to cover all 40 designated categories of offenses.

6.4.3 Compliance with Recommendations 37 & 39 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
R.39	LC	• Dual criminality may impede extradition where the request relates to the laundering of proceeds that are derived from a designated predicate offense which is not covered. • List-based treaties do not cover ML.
R.37	C	• This Recommendation is fully observed.
SR.V	LC	• List-based treaties do not cover FT.

6.5 Other Forms of International Co-operation (R.40 & SR.V)

6.5.1 Description and Analysis

Recommendation 40 and Special Recommendation V (Other forms of cooperation)

1187. In order to enhance the capacity of foreign governments to more effectively engage in international cooperation on anti-money laundering and counter terrorist financing, the U.S. government has established the interagency TFWG (see section 6.1 above). This body provides coordinated, comprehensive training to select priority countries designed to assist their efforts to implement FATF recommendations. For example, the TFWG is the only body to offer foreign counterparts training on implementing Special Recommendation IX.

FIU Cooperation

Ability to cooperate with foreign counterparts

1188. FinCEN is able to respond to requests for assistance from foreign FIUs and serves as the primary portal through which foreign FIUs request information from U.S. law enforcement, regulatory and/or supervisory bodies. FinCEN also assists U.S. agencies that are seeking information from foreign FIUs relating to law enforcement investigations, regulatory/supervisory actions or to counter terrorist activities.

1189. Depending on the information requested, FinCEN can go to third agencies for records and information. Certain types of information, such as bank records, can only be obtained through letters rogatory or an MLAT request; however, FinCEN does have the authority to release BSA information as it is the owner of that data. All other information requires prior permission by the third agency and is routinely requested and received when no impediments (such as grand jury information or classified information) exist. The information is forwarded via the FIU with appropriate caveats on the handling and use of the information clearly specified. Additionally, FinCEN makes requests of its foreign counterparts, either on its own behalf or on behalf of U.S. law enforcement agencies. When doing so, FinCEN specifies the source of the request, the violation suspected, whether it is civil or criminal, whether there is an active case and whether the information is needed for court proceedings.

1190. FinCEN also exchanges terrorist financing investigative and analytical information with other foreign financial intelligence units around the world. For instance, it worked closely with the Spanish FIU following the Madrid bombing and has offered assistance to the British FIU following the subway and bus bombings in London. FinCEN routinely serves as an intermediary between U.S. law enforcement and its FIU counterparts by requesting information on terrorism-related investigations. All requests from foreign FIUs relating to terrorism or terrorist funding receive immediate attention and comprehensive research and analysis. FinCEN is also upgrading its response to incoming requests for information from financial intelligence units by providing appropriate information and analysis tailored to what is requested.

1191. FinCEN's approximate time to respond to a request from a foreign FIU is: two months for routine requests; one to two days for urgent requests (those with impending court dates or law enforcement actions for example); and from two days to a week for terrorist financing related requests. FinCEN responds to all requests from foreign FIUs and places a priority on requests involving possible terrorist financing allegations. FinCEN is taking steps to reduce its response time for a routine foreign FIU request to one month in accordance with Egmont Group Best Practices.

Mechanisms to facilitate cooperation

1192. FinCEN does not require a Memorandum of Understanding in order to share information with its foreign counterparts. FinCEN, however, does negotiate and enter into MOUs with its foreign counterparts

that are required by their domestic law to exchange information pursuant to such Memoranda. As of 30 June 2005, FinCEN has entered into 20 MOUs with its Egmont counterparts.[124]

FOREIGN REQUESTS MADE TO FINCEN			
Year	Requests	Number of Subjects	Number of Requesters
2000	199	2,196	32
2001	325	2,562	53
2002	511	6,058	56
2003	530	4,996	72
2004	613	6,362	73

1193. Requests are facilitated via the Egmont Secure Web, but are also accepted via correspondence and facsimile. Where possible, responses are also routed via the Egmont Secure Web. However, where this cannot be done, the responses are sent to the requesters by commercial express courier or by facsimile.

1194. FinCEN occasionally receives unsolicited information from foreign banking authorities through the host government FIU about particular customers or financial transactions. Depending on the nature of the information provided and if authorized by the referring foreign FIU, FinCEN will share it with the appropriate regulators, law enforcement agencies, FinCEN's regulatory staff (for information) or network with other FIUs, domestic law enforcement and/or regulators.

Conducting inquiries or investigations on behalf of foreign counterparts

1195. FinCEN is authorized to conduct inquiries on behalf of its foreign counterparts. When a foreign FIU requests investigative assistance from FinCEN, it must complete a case request form and provide all relevant subject identifying data and case background information. Upon receiving the case request form, FinCEN immediately acknowledges receipt and provides the requesting agency with a case number and point of contact. FinCEN then screens the request to ensure that the requesting FIU has provided an adequate amount of identifying and background information. If there is insufficient data, FinCEN will correspond with the requesting FIU, via the Egmont Secure Web, to obtain additional identifying data. In the past FinCEN has ceased acting upon a request when the requester did not provide, despite repeated follow up, sufficient details to identify the nature of the request or to allow effective research on the subjects of the request. As there are several other reasons a case may be closed under this category FinCEN is unable to determine the number of cases that may have been closed due to a lack of response by the requester.

1196. After the initial screening process is complete, an analyst is assigned to the case. The assigned FinCEN analyst is responsible for making all relevant queries on the subjects named in the request, expanding their research as necessary (and as agreed upon) to include any 'new' entities that are identified through the research. Queries are made on all commercial databases, financial databases and law enforcement databases to which FinCEN has access. If other agencies have requested data on the same entities (and all parties agree), FinCEN can facilitate networking amongst the agencies involved (i.e. by sharing the contact names and telephone numbers of the other requesting agencies).

1197. In general, based on the needs of the requesting agency, FinCEN can provide a foreign FIU with three types of data: commercial data (public record information);[125] financial data (BSA

[124] Australia, Belgium, Canada, Chile, Cyprus, France, Guatemala, Italy, Japan, Mexico, Paraguay, Poland, Russia, Netherlands Antilles, Panama (letter agreement), Singapore, Slovenia, South Korea, Spain, and the United Kingdom.

[125] Includes general identifying information (name, address, social security number, driver license information, credit history information, tax payer identification number), as well as judgment, lien, incorporation data and property records for individuals and businesses.

information);[126] and law enforcement data (foreign travel, criminal history, and driver history records). FinCEN prepares a report that summarizes its findings and forwards it to the requester.

1198. During the on-site visit, the Director of FinCEN expressed a commitment to improving the quality of the research reports that FinCEN analysts produce in response to requests from foreign FIUs. In particular, FinCEN's stated objective is to generate a report that is more functional, contains a deeper level of analysis and is more tailored to the specific investigative needs of the requesting FIU. To facilitate this goal, FinCEN has undergone a reorganization that includes the adoption of a new mission statement and a restructuring of FinCEN's Analytics Division. It is important that FinCEN continue working toward this goal in the future.

1199. When a foreign FIU requests information from a U.S. law enforcement agency whose records FinCEN cannot access directly, the case is sent to the appropriate law enforcement agency representative at FinCEN for completion of the relevant queries. The law enforcement agency will then notify FinCEN if it has positive information on file and may authorize FinCEN to disseminate that information. If FinCEN receives dissemination authority, it will in turn notify the foreign FIU of the existing information. However, it is important to note that, at times, a U.S. law enforcement agency will choose against releasing the results of a positive query directly to FinCEN. Instead, U.S. law enforcement agencies often opt to release details of a match directly to the foreign FIU by directing the FIU to contact the relevant overseas Law Enforcement or Legal Attaché. It is also important to note that U.S. law enforcement agencies require good personal identifier data to perform conclusive checks of their databases.

1200. The practice of referring a foreign FIU to an outside law enforcement agency is FinCEN's standard procedure when dealing with the dissemination of law enforcement information to its foreign counterparts. This policy has been adopted because FinCEN is not the owner of (nor does it have direct access to) law enforcement information. Consequently, FinCEN does not have the authority to approve the dissemination of an outside law enforcement agency's information. The decision to release any law enforcement information is left to the discretion of the agency from which the information originated.

1201. In a great majority of cases, FinCEN's referral policy has been unproblematic and has resulted in the successful exchange of information between U.S. law enforcement and foreign FIUs. However, there have recently been some concerns regarding the utilization of this policy when dealing with the small number of FIUs that are restrained by law from having any contact with law enforcement. In such cases, it is often difficult for the requesting foreign FIU to obtain the needed law enforcement information. FinCEN understands the restrictions that are placed upon those foreign FIUs that are unable to contact law enforcement; however, it is bound to follow the information sharing procedures of U.S. law enforcement agencies and must honor the decision of those agencies when they choose to release information directly to a foreign FIU rather than to FinCEN.

Conditions on the exchange of information and grounds for refusal

1202. Neither the Egmont Principles regarding information sharing nor the provisions of the MOUs FinCEN has entered into are burdensome. FinCEN requests enough identifiers and information to process a request and will not provide information that will be used as evidence in court (this is done by OIA through a MLAT or letters rogatory as described above). FinCEN responds to all requests received from foreign FIUs where the information is available. It also seeks dissemination authority from law enforcement as necessary and provides points of contact information as warranted.

[126] FinCEN has access only to account information in reports that have been filed by financial institutions as required under the BSA and does not have direct access to official bank documentation. The securing of such information requires the use of the MLAT process.

1203. FinCEN does not refuse requests for cooperation or support, except for those relating to due diligence checks. Law enforcement research is conducted only for requests involving criminal investigations.

Controls and safeguards on the exchange of information

1204. FinCEN abides by the Egmont Group Principles of Information Exchange. In addition, FinCEN undertakes strict safeguards to protect the confidentiality of information it collects pursuant to law or regulation as well as to any information received from foreign counterparts. FinCEN does not provide BSA records to members of the general public. Reports and records of reports filed under the BSA are exempt from access under the Freedom of Information Act (31 USC 5319). In addition, FinCEN has exempted the system of records in which BSA reports are maintained from the access and amendment provisions of the Privacy Act [31 CFR 1.36(c), 1.36(g), and 31 CFR Part 1, Subpart C, Appendix N].

1205. All FinCEN employees undergo a rigorous security background check before being accepted into employment. Background checks are repeated/updated every five years on all FinCEN employees. Once on the job employees are required to sign confidentiality agreements as well as undergo several security training seminars covering such subjects as: Procedures for Protecting Information, Personal Conduct and Reporting Requirements, U.S. Government Ethics Standards, Computer and Other Technical Vulnerabilities, and Personal Safety Measures.

1206. FinCEN employs passwords and access controls, and all non-Treasury agencies are required to enter into signed agreements outlining usage and dissemination rules before electronic access is authorized. Procedural and physical safeguards include the logging of all queries and periodic review of such query logs, compartmentalization of information to restrict access to authorized personnel, physical protection of sensitive hard copy documents and magnetic tapes, encryption of electronic communications, intruder alarms and other security devices, and 24-hour building guards.

Diagonal cooperation

1207. FinCEN prefers to share information with partner FIUs, but engages in information sharing with non-counterparts on a case-by-case basis depending on the facts and circumstances. Because of the sensitivity of BSA information, FinCEN needs to ensure that there is accountability for how that information is to be used. With a non-FIU partner additional internal controls must be applied because the non-counterpart may not understand the sensitivity or importance of SARs and related information supplied by the FIU.

1208. Typically an exchange with non-counterparts would take place indirectly usually where a U.S. authority (for example, law enforcement or legal attaché based in the country) is jointly involved in a case with the non-counterpart and serves as an intermediary to facilitate the request. Under this process, the U.S. authority can provide FinCEN with assurances that there is a bona fide need for the information and FinCEN can hold the U.S. authority accountable for any problems with the non-counterpart's use of the information. The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority.

Effectiveness of the FIU's cooperation with foreign counterparts

1209. All requests for assistance received from foreign FIUs are accepted, with the exception of due diligence requests. FinCEN records all foreign FIU requests and domestic law enforcement requests sent to foreign financial intelligence units in its management information system, the FinCEN Database. The table below reflects requests that FinCEN received from foreign FIUs during the years 2000 to 2004.

FOREIGN REQUESTS MADE TO FINCEN

Year	Requests	Number of Subjects	Number of Requesters
2000	199	2,196	32
2001	325	2,562	53
2002	511	6,058	56
2003	530	4,996	72
2004	613	6,362	73

1210. The following chart shows the requests that FinCEN made to foreign FIUs on behalf of U.S. law enforcement agencies during the years 2000 to 2004.

U.S. LAW ENFORCEMENT REQUESTS REFERRED TO FOREIGN FIU'S					
Year	Requests	Resulting Referrals*	# of Subjects	# of Requesters	Requests Declined
2000	19	25	75	10	
2001	39	141	559	15	
2002	116	341	2,457	20	
2003	110	218	1,569	24	
2004	127	287	1,556	27	

* A single request made by a U.S. law enforcement agency may be referred to multiple FIU's. For statistical purposes this requested is counted as one referral only.

1211. FinCEN also records all spontaneous referrals made by foreign FIUs in its management information system. No such referrals were received in 2000; 48 were received in 2001 (primarily immediately after the events of 9/11); 36 were received during 2002; 21 during 2003 and 49 in 2004. According to that same in-house database, FinCEN made one pro-active referral to a foreign FIU in 2003 and again in 2004.

1212. FinCEN continues to expand the assistance that it provides to its international partners. Examples of such assistance include: (1) rapid and direct involvement in assisting Spanish authorities after the Madrid bombing; (2) expanding the analyst exchange training program; and (3) providing expert assistance to FIUs to maintain the Egmont Secure Web.

Law Enforcement Cooperation

1213. The primary pathway for the exchange of information with foreign law enforcement is through the use of MLATs, handled by DOJ/OIA as the competent authority, or through requests initiated by the country's FIU to FinCEN. However, law enforcement agencies (including ICE, the DEA, the CBP, the FBI and the IRS-CI) are also able to assist their foreign counterparts in the investigation and prosecution of money laundering offenses through informal means. Requests for simple investigative assistance and information sharing can be made by foreign police authorities to their DEA, FBI, IRS-CI or ICE counterparts in-country, who in turn will pass the request for informal assistance to the appropriate agents in the U.S. By having attachés assigned to foreign posts, IRS-CI, DEA, FBI and ICE have developed companion channels that permit the agencies to more effectively and expeditiously exchange the information once the formal request is received from the competent authority. Additionally, the role of the overseas attachés is to help their foreign law enforcement counterparts in a more rapid, constructive, and effective manner. Through constant interaction in face-to-face meetings, barriers are reduced and the type of assistance needed can be identified and provided expeditiously.

1214. Law enforcement and other agencies of the U.S. have entered into a number of general agreements that would, in most instances, cover cases involving money laundering. For instance, the legacy U.S. Customs Service, now ICE and CBP, has entered into 44 Customs Mutual Assistance Agreements (CMAAs) that allow ICE and CBP to assist another party in a wide variety of cases. Other law enforcement agencies with similarly broad agreements include the FBI and, with respect to narcotics and associated offenses, the DEA.

1215. All such exchanges of information between the various U.S. attachés and their foreign law enforcement counterparts can be made both spontaneously and upon request in relation to money laundering and the underlying predicate offenses. If needed, the respective attachés would forward the information to other U.S. federal law enforcement personnel that have jurisdiction over the predicate offense, such as DEA if it pertained to narcotics trafficking or IRS-CI for a tax-related offense and IRS-CI and ICE for a money laundering related offense. As mentioned above, if it is a request requiring the compulsion of records the foreign agency would be referred to the appropriate competent authority.

1216. All federal law enforcement agencies are authorized to conduct inquiries on behalf of their foreign counterparts. Such inquiries can be made pursuant to a qualified competent authority request such as a MLAT or more informally, when the inquiry does not require the use of compulsory process or the information can be attained through public databases. Law enforcement agencies (such as the DEA, IRS-CI, and ICE) may also work with their foreign counterparts by developing sources of information, conducting undercover operations, executing search warrants and interviewing witnesses.

1217. In general, information received by federal law enforcement agencies from their foreign counterparts is subject to controls and safeguards to ensure that such information is used only in an authorized manner. The placement of attachés overseas was done to facilitate the exchange of information with foreign counterparts. The attaché's responsibility is to assist in ensuring requests for information are not subject to disproportionate or unduly restrictive conditions.

1218. In particular, requests for assistance are not generally refused because judicial proceedings have not commenced in the requesting country or because a conviction has not yet been obtained. Title 28 USC 1782 specifically authorizes assistance for "criminal investigations conducted before formal accusation." In response to a properly supported request for mutual legal assistance, the U.S. will provide assistance in relation to fiscal offenses, for example, criminal offenses involving the failure to pay taxes and customs duties.

1219. Federal law enforcement officers are subject to a general prohibition against disclosing confidential information. In this regard, unless specifically authorized by law, it is a crime for an employee of the U.S. federal government to disclose certain confidential commercial and financial information that has been obtained in the course of his or her employment or performing official duties.

Regulatory Cooperation in the banking sector

1220. The Federal Banking Agencies all have similar statutory authority to share information (including specific customer information) with foreign bank supervisors, spontaneously or upon request, in appropriate circumstances, and to assist with investigations by foreign banking supervisors. They also have authority to exchange information with foreign bodies other than banking supervisors, but such exchanges are limited to information already in the possession of the U.S. agency. All of the agencies have established procedures under which requests for information are processed.

1221. As shown in the following table, the Federal Banking Agencies are party (either separately or jointly) to a number of bilateral supervisory information sharing arrangements with foreign bank supervisors. Such formal arrangements, however, are not a prerequisite to sharing.

Country	Type of Document	Agency	Date
Argentina	Statement of Cooperation	OCC + Federal Reserve	9/3/1999
Brazil	Statement of Cooperation	OCC + Federal Reserve	6/3/2003
Bulgaria	Exchange of Letters	OCC	9/17/2001
Canada	Memorandum of Understanding	OCC + Federal Reserve	4/24/1998
Chile	Statement of Cooperation	OCC + Federal Reserve	4/16/1998
China	Memorandum of Understanding	OCC + Federal Reserve + FDIC	6/17/2004
El Salvador	Exchange of Letters	OCC	12/8/2003

France	Memorandum of Understanding	OCC + Federal Reserve + FDIC	5/19/2004
Germany	Memorandum of Understanding	OCC + Federal Reserve	8/10/2000
Guatemala	Exchange of Letters	OCC	11/5/2003
Guernsey	Memorandum of Understanding	FDIC	2/3/1999
Hong Kong	Statement of Cooperation	OCC + Federal Reserve	2/19/2001
Jersey	Exchange of Letters	OCC	9/10/2003
Latvia	Exchange of Letters	OCC	7/9/2003
Mexico	Statement of Cooperation	OCC + Federal Reserve	7/3/2002
Netherlands	Statement of Cooperation	OCC + Federal Reserve	1/28/2003
Nicaragua	Exchange of Letters	FDIC	9/24/2004
Panama	Statement of Cooperation	OCC + Federal Reserve + FDIC	1/30/2004
Poland	Memorandum of Understanding	OCC + Federal Reserve + FDIC	10/23/2004
Slovakia	Exchange of Letters	OCC	8/27/2002
Switzerland	Statement of Cooperation	OCC + Federal Reserve + FDIC	5/24/2005
United Kingdom	Memorandum of Understanding	OCC + Federal Reserve + FDIC	5/28/1998

1222. Section 8(v) of the Federal Deposit Insurance Act [12 USC 1818(v)] permits the Federal Banking Agencies to provide assistance to foreign banking authorities, if the foreign authority is conducting an investigation to determine whether there is a violation of law or regulation dealing with banking matters or currency transactions that are administered or enforced by the foreign authority. In determining whether to provide assistance pursuant to this provision, the Federal Banking Agencies must consider whether the foreign banking authority has agreed to provide reciprocal assistance concerning banking matters within its jurisdiction, and whether compliance with the request will prejudice the U.S. public interest.

1223. Section 15 of the International Banking Act (12 USC 3109) authorizes sharing information with foreign bank regulatory or supervisory authorities, if such disclosure does not prejudice the interests of the U.S., and the foreign authority agrees to maintain the confidentiality of the information to the extent possible under applicable law. The conditions imposed on exchanges of information by the Federal Banking Agencies are limited to those necessary to preserve the confidentiality of information to the extent necessary. In addition, the Federal Banking Agencies will seek assurances that information will only be used by the foreign authority for lawful supervisory purposes.

1224. The Federal Banking Agencies do not refuse requests for cooperation on supervisory matters on the sole ground that the request is also considered to involve fiscal matters.

1225. Information received by the Federal Banking Agencies from foreign authorities is subject to controls and safeguards to ensure that such information is used only in an authorized manner. Employees of the Federal Banking Agencies are subject to a general prohibition against disclosing confidential information. In this regard, unless specifically authorized by law, it is a crime for an employee of the U.S. federal government to disclose certain confidential commercial and financial information that has been obtained in the course of his or her employment or performing official duties (18 USC 1905). The Federal Banking Agencies, in appropriate situations, will share: (a) with other federal and state banking authorities and regulatory agencies such as securities and insurance regulators, and (b) with U.S. law enforcement authorities, if information comes to their attention that indicates a possible violation of criminal law. In addition, it should be noted that the Federal Banking Agencies will respond to subpoenas issued by Congress or by a grand jury or pursuant to a court order. In such cases, the recipients of confidential information generally are required to protect the confidentiality of such information.

1226. The Federal Reserve and the OCC both maintain databases that include a record of requests for assistance made by foreign supervisors. The information exchanged by both agencies with foreign supervisors is related primarily to supervisory matters. The Federal Reserve reports that for the period

January 2004-October 2005 approximately 60 instances of correspondence with foreign supervisors were recorded, of which 2 contained a reference to AML/CFT. Those two requests for assistance were granted. The OCC figures indicate that, in the course of 2005, there 32 requests for confidential information, of which only one related to AML issues. All the requests were addressed, mostly within one month.

Regulatory Cooperation in the securities sector

1227. The SEC has the statutory ability to exercise its broad powers on behalf of, and share information with, "foreign securities authorities," a term very broadly defined in the Securities Exchange Act. The SEC is able to obtain non-public information and testimony from individuals and entities on behalf of foreign securities authorities, both formally through information-sharing arrangements with foreign counterparts such as memoranda of understanding, and informally through ad hoc arrangements. The SEC has entered into cooperative enforcement arrangements with the following foreign counterparts: Australia, Brazil, Canadian provincial regulators, France, Germany, Hong Kong, India, Israel, Italy, Japan, Jersey, Mexico, Netherlands, Norway, Portugal, Singapore, South Africa, Spain, Sweden, and the United Kingdom. The SEC is also a signatory to the IOSCO MMOU (which is the first global information-sharing arrangement among securities regulators).

1228. The SEC has authority to provide a wide range of assistance to foreign authorities in the investigation and prosecution of offenses that relate to potential securities violations, including matters related to the financing of terrorism. Pursuant to its statutory authority, the SEC can provide foreign regulators, investigators and prosecutors with a range of information, including financial records, witness statements and testimony. Specifically, the SEC may compel this information on behalf of foreign securities regulators [15 USC 78(u)(a)(2)] and for other entities, the SEC may provide them relevant information held in the SEC's files [15 USC 78x(c)]. This assistance does not depend on a formal arrangement.

1229. At the request of a foreign securities authority, the SEC can use its compulsory investigative powers to assist a foreign securities authority investigating violations, or potential violations, of any laws or rules administered or enforced by the foreign securities authority [s.21(a)(2), Securities Exchange Act]. These powers include requiring the production of documents held by regulated entities, as well as the ability to use the SEC's subpoena powers to compel the production of documents or testimony from any person or entity anywhere within the U.S. Notably, section 21(a)(2) specifically states that the SEC may provide assistance to foreign securities regulators regardless of whether the facts stated in the request would constitute a violation of U.S. laws. In exercising this authority, section 21(a)(2) of the Exchange Act directs the SEC to consider: (1) whether the requesting authority has agreed to provide reciprocal assistance to the SEC, and (2) whether compliance with the request would prejudice the public interest of the U.S. As part of providing assistance to a foreign securities authority, the SEC may conduct an investigation and use its compulsory powers under section 21(b) of the Exchange Act as it would in its own investigations. SEC subpoenas are issued by SEC staff to whom authority is delegated by the Commission, and do not require any judicial process or assistance by another regulator.

1230. The SEC has no provisions that restrict or limit a foreign authority's use of information and documents for the purposes of investigating potential violations of the securities laws and related criminal charges, including money laundering, conducting a civil or administrative enforcement proceeding, assisting in a self-regulatory organization's surveillance or enforcement activities or assisting in a criminal prosecution. While the SEC requires assurances of confidentiality under section 24(c) of the Exchange Act and Rule 24c-1, these confidentiality assurances do not restrict the foreign authority's ability to use the information for the purposes of its investigation and/or any related proceedings, or its ability to transfer the information to criminal law enforcement authorities and self-regulatory organizations.

1231. The SEC does not refuse requests for assistance related to potential violations of securities laws on the sole ground that the request is also considered to involve fiscal matters. No secrecy or blocking laws are imposed in the U.S. on information sharing with foreign securities authorities. Under section 24(d) of

the Exchange Act, the SEC is able to protect from unnecessary public disclosure information regarding requests made by foreign securities authorities as well as information received from foreign securities authorities. With the exception of a formal request from the U.S. Congress or a court order in an action commenced by the SEC or the U.S. government, section 24(d) states that the SEC shall not be compelled to disclose records obtained from a foreign securities authority if the foreign securities authority has stated that public disclosure of the records would violate its laws. This section explicitly exempts from disclosure under the Freedom of Information Act any records obtained from a foreign securities authority. Under section 24(a) of the Exchange Act, the term "records" is defined to include "applications, statements, reports, contracts, correspondence, notices and other documents," and would cover correspondence from the foreign securities authority and notes from consultations between or among the authorities involved requesting assistance. Section 24(d) also permits the SEC to refuse third party discovery requests to access confidential information received from a foreign securities regulator. This provision in effect gives such information greater protection than that afforded information gathered by purely domestic processes, which may be available to such discovery requests. At the same time, section 24(d) yields to a Constitutional principle that a defendant named in an action instituted by the SEC or the DOJ must have reasonable access to the information upon which the government relies or to information otherwise relevant to the government's allegations.

1232. The SEC can share information in its public and non-public files with other foreign authorities, including bank supervisory authorities and criminal authorities, provided that the SEC receives assurances of confidentiality where appropriate. The SEC may share the information in its files with any foreign or domestic person/entity (as the SEC by rule deems appropriate), spontaneously or upon request, "in its discretion and upon a showing that such information is needed…provided the SEC receives assurances of confidentiality from the person or entity requesting the records or information" [Section 24(c), Exchange Act]. Rule 24c-1 implementing Section 24(c) of the Exchange Act defines "appropriate" persons or entities to include federal, state, local or foreign governments or any political subdivision, authority, agency or instrumentality of such government, and foreign financial regulatory authorities.

1233. As a general matter, all information and documents obtained by the SEC in the course of any investigation (including an investigation initiated to assist a foreign securities authority) are deemed nonpublic and confidential, unless made a matter of public record (e.g., as part of a court proceeding). Officers and employees of the SEC are prohibited from making such confidential information or documents of the SEC available to anyone other than a member, officer or employee of the SEC without Commission authorization. The relevant provisions mandating the nonpublic nature of this information may be found at Subpart M of the SEC's Rules on Organization, Conduct and Ethics; and Information and Requests, Rule 2 of the SEC's Rules Relating to Investigations, Securities Act Rule 122, Exchange Act Rule 0-4, and Trust Indenture Act Rule 0-6.

1234. In 2005, the SEC's Office of International Affairs made 438 requests to foreign authorities for enforcement assistance and handled 315 requests from foreign authorities related to enforcement investigations and cases.

Regulatory Cooperation in the insurance sector

1235. As the insurance industry is regulated primarily at the state level, the extent of regulatory cooperation allowed with international regulators depends upon state law. In 2000, the NAIC undertook an initiative to update the confidentiality and information sharing provisions of several key model laws to allow for the sharing of information with international regulators. Specifically, the Model Examination Law, Standard Valuation Law, Risk-Based Capital For Insurers Model Act and Insurance Holding Company System Regulatory Act were revised to allow, through the state's insurance commissioner, the sharing of:

> "documents, materials or other information, including the confidential and privileged documents, materials or information subject to Paragraph (1), with other state, federal and international regulatory agencies, with the National Association of Insurance Commissioners

and its affiliates and subsidiaries, and with state, federal and international law enforcement authorities, provided that the recipient agrees to maintain the confidentiality and privileged status of the document, material, communication or other information."

1236. Also, beginning 1 January 2006, the NAIC accreditation standard for Information Sharing has been amended to provide that states should allow for such information sharing and each state insurance department should have a documented policy to cooperate and share information with respect to domestic companies with the regulatory officials of any state, federal agency, or foreign countries and the NAIC directly and also indirectly through committees established by the NAIC which may be reviewing and coordinating regulatory oversight and activities. Additionally, the International Insurance Relations Division of the NAIC signs MOUs with countries to demonstrate the intention to work together. MOUs have been signed with China, Brazil, Iraq, Vietnam, and drafts are underway with the EU, Russia, and Hong Kong.

Regulatory Cooperation in the MSB sector

1237. All information that IRS gathers pursuant to its regulatory capacity for BSA is the property of FinCEN, and only through FinCEN can a foreign regulatory counterpart request the information.

6.5.2 Recommendations and Comments

1238. The U.S. has implemented mechanisms that allow its FIU, law enforcement agencies and regulators to provide to their foreign counterparts with a wide range of international cooperation. Similar mechanisms exist to facilitate international cooperation diagonally (i.e. from FIU to law enforcement, or from law enforcement to regulator). In general, exchanges of information concerning money laundering or terrorist financing may be provided promptly, either spontaneously or upon request, and without unduly restrictive conditions. Additionally, many U.S. agencies (including the FIU) are authorized to make inquiries or conduct investigations on behalf of their foreign counterparts.

1239. For the most part, other FATF members reported experiencing a satisfactory level of informal cooperation with U.S. authorities at all levels. Only a very limited number of FATF members have encountered some difficulty in exchanging information with FinCEN. It is, therefore, recommended that FinCEN improve the quality of its analytical research reports so that they contain a more practical and deeper level of analysis tailored to the specific investigative needs of the requesting FIU.

6.5.3 Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.5 underlying overall rating
R.40	C	• This Recommendation is fully observed.
SR.V	LC	• With regards to these elements, this Recommendation is fully observed.

7 RESOURCES AND STATISTICS

7.1 Resources of Competent Authorities (R.30)

7.1.1 Description and Analysis

Resources and structure of the FIU

1240. FinCEN is organized into the Office of the Director and four major operating divisions. The four divisions cover regulatory activity, analysis, client liaison and services, and administration and communications. In addition, the Office of Chief Counsel provides legal services to all these units. Following a major restructuring in 2004-2005 with the overall aim to align FinCEN's functional units with its strategic priorities, four executive-level managers, the Associate Directors for the Regulatory

Policy and Programs, Analytic, Client Liaison and Services, and Administration and Communications Divisions were recruited and selected. Among other changes, the realignment set up a new Office of Compliance with responsibility for assuring that examinations for compliance with the BSA and related requirements are uniform and effective. FinCEN's staff includes about 107 analysts.[127]

1241. FinCEN's technology indicates when different agencies are searching the same data so those agencies can be put together–avoiding investigative overlap and permitting the agencies to leverage resources and information. FinCEN uses a secure information technology infrastructure to manage the collection, processing, storage and dissemination of BSA data. The Gateway and Platform programs enable regulatory agencies and law enforcement to access BSA data.

1242. FinCEN's re-structuring also focused on improving its technological resources, in particular the systems required to store, collect, and ease the dissemination of the data. For example, FinCEN launched a major initiative to make BSA data and analytical tools available to authorized users through an easy-to-use, secure, web-based program. In addition, FinCEN began taking the necessary steps to ensure its analysts greater access to classified information crucial to anti-terrorism efforts. This ongoing effort includes upgrading employee background investigation and security clearance requirements, tightening physical security, and upgrading computer security.

1243. FinCEN insists that its staff maintain high professional standards, adhere to confidentiality requirements, exhibit high integrity, and undergo adequate and relevant training. Every new FinCEN employee undergoes a rigorous security background check before being accepted into employment. Background checks are repeated / updated every five years on all FinCEN employees. Once on the job employees are required to sign confidentiality agreements as well as undergo several security training seminars covering such subjects as: Procedures for Protecting Information, Personal Conduct and Reporting Requirements, U.S. Government Ethics Standards, Computer and Other Technical Vulnerabilities, and Personal Safety Measures. FinCEN attracts, develops, and retains a high-performing, diverse workforce through implementation of a new recruitment program and using effective performance management and individual development plans. The team was informed that FinCEN has – at this moment – sufficient resources.

1244. Since the last evaluation, FinCEN has enhanced employee development by establishing a new training function charged with developing career path progressions for all employees and providing training to 93% of FinCEN's employees. Some 75% of the training expenditures were for technical skills, and 14% of training expenditures were for executive, managerial, and supervisory training. The remainder was for equal employment opportunity and retirement planning training. FinCEN sought to narrow gaps in technology skills by providing training in 39 areas related to information technology and software. FinCEN also offers its employees an extensive array of courses, including courses on: Illicit International Monetary Flows, International Banking Operations, Financial Crimes Seminar, Combating Terrorist Financing, Life Insurance Company Products, and Funds Transfer Training.

Resources and structure of the law enforcement and prosecutorial authorities

1245. Information concerning the structure, funding, staffing, technical and other resources of U.S. law enforcement and prosecutorial authorities is set out below. The authorities are listed alphabetically by acronym.

1246. Asset Forfeiture and Money Laundering Section, Criminal Division (AFMLS) (DOJ): As of 2 September 2005, the AFMLS has 34 attorneys and 12 support personnel. In addition, the Section has approximately 30 contract employees that are paid with funds from the Assets Forfeiture Fund. The staff is divided into four units, each headed by a Deputy Chief. See Annex 6 Table 5 for

[127] See Annex 6, Table 2 for more detailed description of FinCEN's divisions. See Annex 6, Table 3 for a description of FinCEN's staffing levels. See Annex 6, Table 4 for a description of FinCEN's budgetary resources.

additional information concerning the structure of AFMLS. AFMLS, in partnership with the Executive Office for the OCDETF, has conducted 24 Financial Investigation Training Seminars in every OCDETF region in the country during the past two and a half years. These seminars have trained more than 1,800 federal, state and local prosecutors and agents from 16 federal law enforcement agencies.

1247. Drug Enforcement Administration (DEA): In 2003, the DEA issued a directive restoring DEA's primary focus to the financial aspects of drug investigations. Consequently, every DEA investigation includes a financial investigation. Also, the DEA established: (1) an Office of Financial Operations; (2) specialized money laundering groups in every DEA Field Division; and (3) a "Bulk Currency Initiative" to coordinate all U.S. highway money seizures for the purpose of developing the evidence necessary to identify, disrupt and dismantle large-scale narcotics trafficking organizations. It also increased Special Agent resources devoted to money laundering in key foreign offices. The Special Agents in Charge of each of the DEA's 21 field divisions have established at least one Financial Investigative Team (FIT). Many of the FIT Teams are staffed with DEA special agents and also with special agents from the IRS-CI, ICE, FBI, the Postal Inspection Service, and state and local law enforcement officers. These FIT Teams are responsible for handling the more complex drug-money laundering investigations.

1248. The DEA's Financial Operations (FO) office provides training in money laundering and financial investigative techniques to: DEA personnel; foreign, state, and local law enforcement counterparts; private financial sector management personnel (Operation Contact); and information and training (upon request) to private companies and banking institutions regarding money-laundering trends. The FO also provides support and guidance in establishing and building specialized money laundering groups.

1249. Department of Justice (DOJ): The DOJ is organized into several divisions located in Washington D.C. and 94 U.S. Attorneys Offices located in 94 different judicial districts across the country. The Attorney General, the Deputy Attorney General, and each of the Assistant Attorneys General in charge of DOJ's divisions, as well as each U.S. Attorney in each district are appointed by the President with the advice and consent of the Senate. U.S. Attorney Offices ordinarily establish a specialized forfeiture unit or designate primary responsibility for forfeiture matters to particular attorneys. Each office also has named a senior prosecutor as its Antiterrorism Advisory Council Coordinator (ATAC), to serve as the district's terrorism prosecution point of contact, and to promote and ensure proper training and information sharing on terrorism cases and terrorism threats (including terrorist financing), throughout the district.

1250. While the DOJ has specialized sections to handle AML and CFT prosecutions (the AFMLS, the Counterterrorism Section, and the OCDETF), the DOJ is staffed by career prosecutors, some of whom handle a general docket. Others are experts in investigating and prosecuting complex and specialized matters, including those involving fraud, narcotics trafficking, organized crime, money laundering, public corruption, terrorism, or the financing of terrorism offenses.

1251. Federal Bureau of Investigation (FBI): In an effort to improve its data management, the FBI is implementing a next generation electronic file management system. The new system will support the FBI's mission by helping manage investigative, administrative, and intelligence needs while also improving ways to encourage information sharing with other agencies. Among the enhancements the FBI envisions is the ability to exploit SARs and other BSA data from FinCEN by using computer software to visualize financial patterns, link distinct criminal activities, and display the activity in link analysis charts.

1252. Department of Homeland Security Immigration and Customs Enforcement (ICE): Pursuant to enactment of the BSA in 1970, the former U.S. Customs Service, Office of Investigations (transferred to ICE in 2003) began conducting financial investigations With border search authority, ICE was also well suited for investigative activity pursuant to the "Currency and Foreign Transactions Reporting Act" under 31 USC and 18 USC 1956. The FTID of ICE attempts to identify, investigate, disrupt, and

dismantle criminal and terrorist organizations and the complex systems used to launder funds. The FTID is composed of four distinct units: (1) the Cornerstone Unit; (2) Trade Transparency Unit (which includes Money Laundering Coordination Center); (3) Financial Operations Unit; and (4) the Commercial Fraud Unit and National Center for Intellectual Property Rights. See Annex 6, Table 6 for a more detailed description of the four units of ICE.

1253. Internal Revenue Service Criminal Investigation (IRS-CI): IRS-CI has approximately 4 500 employees, of which 2,800 are special agents devoted to enforcing money laundering, terrorist financing and criminal tax statutes. The special agents are distributed into field offices throughout the country, but concentrated in the major money laundering centers in the U.S. such as New York, South Florida, Los Angeles, and the Southwest Border. The IRS-CI has 35 field offices, each with an SAR review team that reviews SARs for possible money laundering and other illicit finance activity. IRS-CI provides money laundering statistical data on its website. The Department of Treasury has provided USD 3.1 million per year to IRS-CI to equip and staff task forces located in HIFCAs. These funds are also used to support other money laundering task forces, SAR review teams, and to develop an electronic BSA report filing system for FinCEN.

1254. Organized Crime Drug Enforcement Task Forces (OCDEFT) Program (DOJ): The OCDETF operates nationwide with agent resources and Assistant U.S. Attorneys in the 94 judicial districts organized into nine geographic regions: the Florida/Caribbean Region; the Great Lakes Region; the Mid-Atlantic Region; the New England Region; the New York/New Jersey Region; the Pacific Region; the Southeast Region; the Southwest Region; and the West Central Region. Within each region, one U.S. Attorney oversees the region's OCDETF Coordination Group with includes investigative agencies throughout the region.

1255. Office of Foreign Assets Control (OFAC): OFAC is divided into three divisions: an Investigations and Enforcement division, a Program Policy and Implementation division, and a Resource Management division. In fiscal year 2005, OFAC had a staff of 138 full-time employees (nine of which are responsible for outreach) and an operating budget of USD 22.1 million. Not all of these staff would administer the OFAC programs that relates to EO 13224, as OFAC is responsible for administering 29 economic sanctions programs against foreign governments, entities and individuals. OFAC maintains offices in Miami, Mexico City, Bogotá and Bahrain and maintains a close working relationship with other federal departments and agencies to ensure that sanctions programs are implemented properly and enforced effectively. OFAC works directly with the Department of State; the Department of Commerce; the DOJ, the FBI, the CBP and ICE; bank regulatory agencies; and other law enforcement agencies to fulfill its mission. In addition, OFAC conducts significant public outreach programs to work with the broad range of industries potentially affected by OFAC-administered sanctions programs. Section 2.4 of this report describes the great deal of work involved in administering the OFA programs and, as discussed in that section, the size of the task presents a significant challenge for 138 full-time employees.

1256. Office of International Affairs, Criminal Division (OIA): First created in 1979, the DOJ's OIA now has nearly 50 attorneys with expertise in various geographical and substantive areas. Most attorneys are assigned to handle cases from one of the following main geographic areas: (1) the United Kingdom, Canada, Australia, New Zealand and the English-speaking Caribbean; (2) Western Europe; (3) Central and Eastern Europe; (4) Central America and the Spanish-speaking Caribbean; (5) South America; and, (6) Asia, the Middle East, and Africa. OIA's Fugitive Unit coordinates location and extradition efforts for "career fugitives" who remain at large despite extensive law enforcement efforts, and its Multilateral Team helps advance U.S. law enforcement interests in multinational organizations. OIA also has attorneys posted overseas in Brussels, Mexico City, Rome, London, Paris, San Salvador, and Manila. OIA coordinates its assistance with International and National Security Coordinators designated in each of the 94 United States Attorneys' Offices located throughout the U.S. These coordinators serve as points of contact for both incoming and outgoing requests for fugitives and evidence.

1257. U.S. Postal Service: In 2004, the U.S. Postal Inspection Service established an Intelligence Group at its Headquarters office in Washington, DC. This Group acquires access to a multitude of commercial and federal agency databases, including financial-related data from various sources within the Postal Service, such as the Postal Service's BSA Suspicious Activity database. The U.S. Postal Inspection Service has over 70 postal inspectors are assigned as liaison officers to the Terrorist Screening Center, the NJTTF, and the National Counter-Terrorism Center, which includes the Interagency Intelligence Committee on Terrorism. These inspectors work with Joint Terrorism Task Forces across the country to investigate domestic and international terrorism. In fiscal year 2004, the Inspection Service arrested 1 724 suspects for drug trafficking and money laundering through postal products and services.

1258. The Administrative Office of the U.S. Courts, a part of the Judicial Branch, is responsible for the training of judges. The team was informed that judges, at the different courts, receive preliminary training, but are generally not trained sufficiently to be able to deal with complicated ML/FT offenses/cases as well as freezing/seizing and confiscation.

1259. There was a general perception among the law enforcement agencies that they were under-resourced. Nevertheless, they seem to be working effectively and their staff are well trained.

Resources and structure of supervisors

Banking sector

Board of Governors of the Federal Reserve System

1260. The Federal Reserve is an independent agency that does not rely on Congressional appropriations for funding. The seven members of the Board of Governors of the Federal Reserve System are nominated by the President and confirmed by the Senate to serve 14-year terms of office. The President designates, and the Senate confirms, two members of the Board to the Chairman and Vice Chairman, for four-year terms. In making appointments, the President is directed by law to select a "fair representation of the financial, agricultural, industrial, and commercial interests and geographical divisions of the country". These aspect of selection are intended to ensure representation of regional interests and the interests of various sectors of the public.

1261. The System comprises the Board of Governors of the Federal Reserve System ("the Board") and 12 Reserve Banks located in major cities across the U.S. The Federal Reserve budget expenditures for BSA/AML supervision is covered within the overall supervision and regulation budget and not tracked separately. The 2005 calendar year budget for the Division of Supervision and Regulation of Federal Reserve Banks was USD 519.3 million. Additionally, the Board's Division of Banking Supervision and Regulation had a 2004-2005 annual budget of USD 84.3 million.

1262. The Federal Reserve BSA examination staffing and resources include supervision and regulatory policy staff at the Board and throughout the twelve Federal Reserve Districts. The Board's staff in Washington, D.C. is responsible for developing and coordinating BSA/AML supervisory policy and nation-wide training for the Federal Reserve System and overseeing system-wide compliance with BSA/AML requirements. The Reserve Banks are responsible for examining banking organizations subject to Federal Reserve supervision in their Districts and report findings quarterly to Board staff. The individual Reserve Banks have a high degree of autonomy with respect to their day-to-day regulatory functions, but are accountable to, and subject to oversight by, the Board in Washington.

1263. As of the end of calendar year 2004, the Federal Reserve had a total of 1,671 credentialed examiners of which 950 were commissioned field staff. Commissioned field examiners are those who have successfully completed the Federal Reserve's examiner education and proficiency process. Of these examiners 108 possess advanced BSA/AML skills, including 15 who have advanced Large Complex Banking Organization skills. In addition, there are 337 examiners who possess intermediate skills and another 478 with a basic skill level.

1264. The Federal Reserve's training plan for staff members seeking to obtain an examiner commission requires the individual to master a core curriculum and to successfully pass a proficiency test in each core area. For the BSA/AML proficiency test, an individual must demonstrate an understanding of the concept of money laundering, the purpose of the BSA, and the minimum requirements of Board's regulations on BSA/AML compliance programs, and requirements for filing SARs. Informal training is provided by Board and Reserve Bank staffs through a variety of means. Specifically, Board staff holds semi-annual fora with senior BSA/AML supervisory staff to provide the Reserve Bank staff with policy updates, and discuss recent examination experiences. In addition, the Board's senior BSA/AML examiners participate in select examinations throughout the country to provide on-the-job training to Reserve Bank examiners. Each Reserve Bank also provides ongoing training to supervision staff to keep them informed of the changes to regulations, laws, and procedures. Typically, BSA/AML training is offered at each Reserve Bank's annual examiner conference.

Federal Deposit Insurance Corporation

1265. The FDIC is an independent agency of the federal government. It receives no Congressional appropriations, but is funded by premiums that banks and thrift institutions pay for deposit insurance coverage and from earnings on investments in U.S. Treasury securities. BSA is an integral part of all safety and soundness examinations and as such, all examiners and supervisory staff are expected to be knowledgeable of and either perform BSA/AML examination work, or review the results of the examinations. FDIC staff that covers BSA/AML as part of their work or review processes is as follows:

FDIC resources	Number
Examiners	1,296
Supervisory Examiners	131
Field Supervisors	51
Regional Office Professional Staff	174*
Washington Office Professional Staff	8
Total	1,660

*Excludes regional senior management, accountants, and reporting staff.

1266. The BSA/AML examination staffing and resources include risk management supervisory examiners from over 80 Field Offices, professional risk management staff and management from six Regional Offices and professional staff from the Washington Office, AML Section. The AML Section is responsible for developing and coordinating BSA/AML supervisory policy, training risk management staff, and coordinating and monitoring FDIC-supervised institutions with significant BSA/AML Program deficiencies. The AML Section's resources were increased in 2004 to enhance its coordination and oversight role. The Regional and Field Offices are responsible for examining and reviewing findings of FDIC-supervised banks. The Washington Office also reviews significant BSA/AML problems, and provides interpretations, advice and guidance to FDIC Regional staff and others.

1267. The FDIC's risk management examiner training program requires the individual to master a core curriculum and to pass a proficiency examination. The pre-commission training program embodies basic concepts that every examiner is expected to know in order to perform at the commissioned level including BSA/AML. Additionally, there are approximately 320 BSA/AML subject-matter experts in the FDIC, of which 300 are at the field office level, 12 at the regional office level and eight in the Washington office. One primary role of such experts is to provide guidance to staff on any BSA/AML issue. Regional and Field Offices provide ongoing training to examination staff to keep them abreast of changes to regulations, laws, and procedures through on-the-job training and face-to-face sessions.

National Credit Union Administration (NCUA)

1268. The following table shows the number of employees of NCUA and the number of persons dedicated to AML/CFT issues in the agency.

Date	Total NCUA Employees	Examiners responsible for reviewing compliance with BSA/AML	Other staff involved with BSA/AML actions
30 Sep 2004	915	513	7
30 Sep 2005	924	521	7

1269. While NCUA does not have specialists who are solely devoted to AML, NCUA's consumer compliance subject matter examiners are provided with additional training on AML issues and serve as a resource for other staff. NCUA had 25 consumer compliance subject matter examiners in 2005, one fewer than the previous year. These examiners are included in the count above.

1270. NCUA examiners review compliance with BSA at all exams, and periodic AML training is provided to all NCUA examiners.

Office of the Comptroller of the Currency

1271. The OCC is an independent bureau within the Treasury. It is headed by the Comptroller of the Currency, who is appointed for a five-year term by the President, with the advice and consent of the Senate. The Comptroller is vested with general administrative powers and duties for the administration of the national banking laws, and is charged with the duty of supervising national banks. By statute, Treasury may not intervene in any matter or proceeding before the OCC unless otherwise provided by law. The Comptroller can be removed from office by the President upon reasons communicated by him to the U.S. Senate, and the U.S. Congress exercises oversight responsibilities over the OCC and may hold hearings and subpoena documents from the OCC. The position is non-partisan.

1272. The OCC has its headquarters in Washington D.C., a data center in Maryland, and four district offices in Chicago, Dallas, Denver and New York. It also has 48 field offices and 23 satellite locations in cities throughout the U.S., resident examiner teams in the 25 largest banking companies that it supervises, and an examining office in London, England.

1273. The OCC's revenue is derived primarily from assessments and fees paid by national banks and income on investments in U.S. government securities. It does not receive congressional appropriations to fund any of its operations. By federal statute 12 USC 481, the OCC's funds are maintained in a U.S. government trust revolving fund. The funds remain available to cover the annual costs of the OCC's operations in accordance with policies established by the Comptroller. To achieve its strategic goals and accomplish its mission, the OCC separates its activities into three major project areas: supervise, regulate and charter. It formulates its budget and tracks costs and full-time equivalents (FTEs) by these programs.

1274. The "supervise program", which is by far the largest program, encompasses the supervision of national banks and their subsidiaries, federal branches and agencies of foreign banks, national trust companies, bank data software vendors, and data processing service providers. For fiscal year 2004 the OCC devoted 2,212 FTEs (or 82% of total FTEs) to this program, which cost USD 392.1 million. The "regulate program" establishes regulations, policies and operating guidance, and interpretations of general applicability to national banks. The "charter program" involves activities related to chartering national banks, as well as evaluating the permissibility of structures and activities of national banks and their subsidiaries. The OCC devoted 14% and 4% of total FTEs, respectively, to each of these programs.

1275. The OCC has nearly 1,824 examiners in the field, many of whom are involved in both safety and soundness and compliance with applicable laws including the BSA. It has over 300 examiners

onsite at the largest national banks, engaged in continuous supervision of all aspects of their operations. In 2005, the OCC had the equivalent of approximately 49 full time employees involved in BSA/AML supervision. It has seven full time BSA/AML compliance specialists in Washington D.C. dedicated to developing policy, training, and assisting on complex examinations; and one full-time fraud expert, who is responsible for tracking the activities of offshore shell banks and other vehicles for defrauding banks and the public.

1276. The OCC has an extensive training program that examiners must complete in order to take and pass the Uniform Commission Examination (UCE) to be commissioned as a National Bank Examiner. The OCC's AML School is a 28-hour classroom course designed to train participants to recognize the potential money laundering risks confronting financial institutions, assess the adequacy of an institution's policies, procedures and practices in complying with BSA and AML Programs and provide access to information to maintain updated knowledge on AML issues. The OCC has also implemented an annual BSA/AML Examiner Specialized Skills Program.

1277. In 2005, the OCC undertook to provide extensive BSA/AML training to all of its bank examiners, which includes Community Bank and Mid-Size Bank examiners reporting to the four OCC District Offices and resident on-site Large Bank examiners. This training focused on the new FFIEC Examination Manual and incorporated modules on high risk products, services and customers.

1278. In addition to formal course offerings, the OCC periodically provides training in the form of agency-wide teleconferences, and provides external training opportunities to its employees, including the industry Certified Anti-Money Laundering Specialist certification, as appropriate.

Office of Thrift Supervision (OTS)

1279. The OTS was established in 1989 as a bureau of the Treasury. The Director is appointed by the President, with Congressional confirmation, for a five-year term. The OTS is headquartered in Washington D.C. with four regional offices located in Jersey City, Atlanta, Dallas, and San Francisco. Its budget in 2005 was approximately USD 187 million, which is expected to rise to about USD 215 million in 2006. As of September 2005, OTS had 474 examiners in the field examining for safety and soundness, compliance with applicable laws including BSA, and trust and asset management activities. In addition, approximately 100 staff, both in Washington and the regions, devote time to BSA compliance issue.

1280. The OTS educates its examiners for the BSA/USA PATRIOT Act in its Compliance I and Compliance II schools which involve 1.5 days of BSA training modules.

1281. OTS has hosted a number of regional conferences solely dedicated to BSA/USA PATRIOT Act issues. In early 2003, OTS held mandatory all-day training sessions for examiners from all four regions. At these conferences, case studies of BSA issues that may be encountered at savings associations were discussed as well as new BSA/USA PATRIOT Act regulations or other guidance that had been issued. During 2004 and 2005, BSA and USA PATRIOT Act examination issues were discussed at examiner team meetings and other examiner education initiatives. OTS regional offices also provide training sessions for examiners. Topics at such sessions have included BSA Program Review requirements (12 CFR 563.177); money laundering red flags and money laundering schemes; and AML case studies.

General integrity standards for Federal Banking Agency Staff

1282. Federal laws and regulations, as well as the individual conflict-of-interest rules and codes of conduct of each of the Federal Banking Agencies, set standards of integrity for agency staff. Under a newly enacted federal law introduced following the Riggs Bank case, an examiner may not, for a period of one year after leaving an agency, accept employment at any financial institution for which the examiner had served as senior examiner during the last year of employment at that agency

[12 USC 1820(k)]. Other federal laws prohibit examiners from accepting loans or gratuities from financial institutions that they examine (18 USC 213). The agencies' rules prohibit an employee from holding a financial interest in any financial institution that is supervised by that agency and also impose certain limitations on borrowing relationships between examiners and institutions for which the particular agency is the primary supervisor. Staffs of each of the Federal Banking Agencies are required to complete ethics training annually.

1283. The confidentiality of information obtained by the Federal Banking Agencies through the supervisory and examination processes and the reports and records of reports obtained by FinCEN through required reporting under its regulations ("Supervisory Information") is protected by a number of federal statutes and regulations. In the first instance, Supervisory Information is exempt from release to the public under section (b)(8) of the Freedom of Information Act (FOIA) (5 USC 552), as it is information "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions." In addition, depending on the nature of the information, certain Supervisory Information may also be exempt from disclosure under section (b)(4) of the FOIA as trade secrets information. Such information is also subject to the Trade Secrets Act (18 USC 1905), which is a federal criminal law that forbids a federal officer or employee from disclosing "trade secrets" information unless the disclosure is "authorized by law."

1284. Supervisory Information is also considered property of the U.S. and, as such, federal criminal law prohibits the unauthorized use of Supervisory Information for personal use or gain (18 USC 641). Further, to the extent that the Supervisory Information contains customer identifying information, its disclosure is also subject to the Right to Financial Privacy Act, which generally prohibits a U.S. government agency (and its officers and employees) from disclosing financial records of a customer to another U.S. government agency except in limited circumstances, such as disclosure to other financial regulators or law enforcement agencies (12 USC 3401 et seq.). The law defines customer as any individual or partnership of five or fewer individuals.

1285. Finally, each of the Federal Banking Agencies has promulgated regulations that specify the circumstances under which Supervisory Information may be disclosed to other regulators, other government agencies, and third parties generally (e.g. 12 CFR Part 261, subpart C and 12 USC 326).

1286. As regards general training, examination staff from each of the Federal Banking Agencies regularly participates in FFIEC workshops on BSA/AML compliance. The curriculum includes sections on planning and conducting a BSA/AML examination, customer due diligence, private banking, foreign correspondent banking, funds transfers, SARs, CFT, OFAC, and non-bank financial institutions. The FFIEC also has a web accessible "Info-Base" that provides the Federal Banking Agencies' field examiners with a quick source of training and basic information. The Info-Base is an automated tool for examiners and industry that provides information on the FFIEC Manual. The long-term goal of the Info-Base is to serve as a resource to examiners in the field and to provide training for development in the field to enhance on-the-job training of BSA/AML examinations examiners and for other topics of specific concern to examiners in FFIEC's five member agencies. The Info-Base features the entire Manual, together with laws, regulations and video presentations, as well as frequently asked questions and links to other resources that may be helpful in understanding BSA/AML requirements and examination expectations.

State Supervisory Agencies

1287. As indicated previously, although there has been no delegation of BSA compliance responsibilities to the state banking agencies, the majority of such agencies undertake examinations under cooperative arrangements with the federal agencies. These examinations are either performed jointly or on an alternate basis with the federal agencies. According to the CSBS data, of the 46 state, District of Columbia and Puerto Rican agencies that undertake BSA examinations, 18 have designated BSA/AML specialists or subject matter experts. The numbers of such experts in each agency range

from one to 12. In almost all cases the designated experts have undertaken training provided through the federal agencies. This is usually facilitated under the auspices of the CSBS, which maintains a close relationship with the federal agencies, which participate in the BSA 4-day BSA training program that it has developed. The third such program takes place in early 2006. It has also to be noted that a number of states have their own AML statutes, which may or may not contain provisions similar to those of the BSA. Therefore, in these cases examiners will already have exposure to AML concepts.

Securities sector

Securities and Exchange Commission and the SROs

1288. The SEC is an independent federal agency whose primary mission is to protect investors and maintain the integrity of the securities markets. The SEC resources dedicated to combating money laundering are integrated into its major program areas, and a risk-based approach forms an integral part of the SEC's approach to meeting its money laundering responsibilities. While the SEC did not separately track in its Fiscal Year 2006 Congressional Budget Request the portion of its budget attributable to AML initiatives, the SEC's total budget for fiscal year 2005 was USD 888 Million. In fiscal year 2005, the SEC employed 3,871 full-time equivalent employees, 1,258 of whom were employed in the SEC's Division of Enforcement, which is responsible for investigating and bringing enforcement actions on behalf of the SEC. Another 870 were employed in the Office of Compliance Inspections and Examinations, which is responsible for conducting compliance examinations and inspections of entities regulated by the SEC. The SEC stated in its Fiscal Year 2006 Congressional Budget Request that one of its strategic goals will be continuing to assess compliance of its regulated entities with AML rules.

1289. Rules for examiners focus on possible conflicts of interest that could arise during examinations, including potential corrupting influences of money launderers or other criminals who may have infiltrated a financial institution. For example, applicable criminal law imposes absolute prohibitions on job seeking with institutions an examiner is currently examining. Day to day interactions are preserved on a professional basis with such basic controls as a prohibition on the acceptance of meals and other gifts by examined institutions. See generally the Standards of Ethical Conduct for Employees of the Executive Branch 5 CFR Part 2635 et seq.

1290. Each SEC regional office has at least one Ethics Liaison, and most have an Ethics Liaison from the examination staff. In addition, the SEC's Office of the General Counsel has an entire group of attorneys devoted to ethics issues, and there is an "Ethics Officer of the Day" available for consultation at all times. Counseling is available to anticipate potential problems and advise staff regarding applicable ethics obligations. The agency also conducts ethics training as an integral part of the annual training for examiners in both the broker-dealer and mutual fund exam programs. Advanced training sessions, videoconferences and teleconferences are held throughout the year. In order to assure an agency-wide focus on ethics issues, each SEC regional office also has at least one Ethics Liaison, and most have an Ethics Liaison from the examination staff.

1291. In the post-employment area, the SEC's line managers are expected to respond to any potential conflict of interest arising from staff accepting employment from a firm that they recently examined. In addition, for the first two years after leaving the SEC, all former SEC staff must notify the Commission before they make an appearance before the Commission, which includes dealing with SEC examiners. The agency also administers an aggressive program to assure that former employees do not "switch sides" on matters for which they were responsible while working for the federal government. Departing staff are counseled with respect to their obligations to protect nonpublic information, and to avoid projects with which they have conflicts. Law firms that hire examiners (many of whom are lawyers subject to professional responsibility rules) who may have worked on a matter being handled by a law firm must make explicit representations regarding the walling off of that former employee in order to continue their participation in a matter. The SEC is developing a

more formalized exit procedure on ethics issues that will include asking all departing staff for the identity of their new employer, so line managers can follow-up on any identifiable conflicts.

1292. The SEC provides its staff with several AML training sessions each year and the sessions vary depending on experience level. The SEC recently has formed an internal AML Working Group consisting of examiners in each regional and district office. This Working Group serves as a discussion forum for issues that arise in the field and also an important communication channel for new regulatory and practical developments, Further, to ensure that examiners keep current on new developments and technologies, industry representatives and consulting firms regularly give presentations to the SEC as part of its professional development series. SEC regional offices throughout the country also conduct their own local training sessions.

NASD

1293. NASD (formerly known as the National Association of Securities Dealers) is an SRO with statutory examination and enforcement authority over all of its members -- approximately 5300 firms, of which approximately 50% are very small (typically one-person) operations. There are approximately 900 staff in the department of member regulation and 200 in the enforcement area. The NYSE has 349 member firms, of which 217 deal with the public. Those firms dealing with the public must be members of the NASD. As discussed below, there are firms that are members of both NASD and the NYSE and for those firms, the SROs reach an agreement as to which SRO will undertake AML compliance examinations.

1294. In an effort to educate SRO examiners about AML and to keep them up to date on AML initiatives, SRO examiners attend in-house AML training sessions and seminars as well as industry conferences. In addition, the NASD prepared web-based training regarding AML and BSA requirements which is available to NASD staff as well as the industry. The NASD also offers a one-day seminar regarding AML rules through its Institute for Professional Development. The SEC and SROs also work together to offer joint AML training for examiners. AML is covered annually in the "Joint Regulatory Conference." In February 2005, the SEC, NYSE and NASD conducted a two-day, intensive AML training session for examiners. SRO and SEC staffs regularly attend outside training sessions, including the Securities Industry Association's annual AML conference.

New York Stock Exchange

1295. The NYSE is an SRO with statutory examination and enforcement authority over its membership, which comprises 349 broker-dealers, of which 217 deal with the public and 132 have only broker-dealer clients. The Member Firm Regulation Division protects investors through regular and for-cause on-site examinations of NYSE member firms. It is the largest of the NYSE's four divisions employing more that 300 professionals. The NYSE has 187 examiners, of whom 67 specialize in AML work. In addition, there are 188 staff within the enforcement area. When violations of NYSE rules and federal securities laws are uncovered, the cases are sent to the Enforcement division for further action.

Commodity Futures Trading Commission and National Futures Association

1296. The CFTC is an independent federal agency whose primary mission is to protect market users and the public from fraud, manipulation, and abusive practices related to the sale of commodity and financial futures and options. The CFTC's resources dedicated to combating money laundering are integrated into its major program areas, and a risk-based approach forms an integral part of the CFTC's approach to meeting its money laundering responsibilities. In fiscal year 2005, the CFTC employed 511 full-time equivalent employees, 136 of whom were employed in the CFTC's Division of Enforcement, which is responsible for investigating and bringing enforcement actions on behalf of the CFTC.

1297. The NFA has about 230 employees covering some 4000 members, not all of which are currently subject to BSA requirements.

1298. All CFTC employees are subject to a comprehensive security background check that includes, by way of example: (1) checking each employee's employment, educations, residence and credit histories; credit checks, and checks with both local and federal law enforcement authorities; and (2) cross-checking with both local and federal law enforcement agencies. CFTC employees are also subject to ethical and conflict-of-interest guidelines that apply both during and after their tenure with the CFTC. All CFTC staff are subject to Office of Government Ethics annual training requirements and senior staff are required to file annual financial disclosure forms. Staff are also subject to government-wide restrictions on post-CFTC employment designed to minimize potential conflicts of interest.

1299. The CFTC provides in-house training opportunities for its entire staff, which includes auditors that conduct oversight examinations. The training covers all aspects of the anti-money laundering regulatory requirements applicable to futures firms. In addition to on-the-job training, all NFA examiners are required to attend formal training in AML such as instructor-led training sessions and technical roundtables on various anti-money laundering issues, such as the requirements for futures commission merchants and introducing brokers in commodities customer identification programs. In addition to in-house training, NFA also hosts outside agencies, such as FinCEN, to make presentations on relevant and timely issues related to AML requirements.

Insurance, MSB and DNFBP sectors DNFBPs

IRS-SBSE

1300. The IRS-SBSE is responsible for supervising the insurance sector (except for variable annuities brokers which will be supervised by the SEC), non-federally insured credit unions, credit card companies, MSBs (including money remitters and foreign exchange offices), casinos (tribal and non-tribal), some card clubs and dealers in precious metals/stones.

1301. The IRS-SBSE has 315 BSA examiners in 31 groups housed in 183 offices located in the 50 states, the District of Columbia, and Puerto Rico. IRS-SBSE is in the process of hiring an additional 90 examiners. Applicants have been interviewed and hiring began in April 2006. Examiners are not specialized; however, their grade level and training will determine what types of examinations they will conduct. These auditors only do audits for BSA compliance. The IRS has other auditors that handle tax audits. About 20% of the IRS-SBSE resources are devoted to supervising compliance with the Form 8300 reporting requirements. As noted in the discussion in section 3.11 of this report, the limited resources in the IRS have to be devoted to a very broad range of compliance monitoring duties. This task appears to be unrealistic.

Non-profit sector

1302. Another issue concerns the size of the charitable sector in the U.S. and whether existing resources particularly at state level are sufficient. The evident diligence and professionalism of both the IRS and State officers in this area is not in question. Within existing resources, it is also clear that anti-terrorism is a priority for IRS-TEGE. For example, recent public statements[128] by the IRS regarding priorities for FY2006 included four specific anti-terrorism initiatives commenced in 2005 which carried on from similar anti-terrorism initiatives for FY2004. The 2005 initiatives are:

(a) commencing examinations on foreign grant-making organizations to ensure that grant funds are being used for intended charitable purposes;

(b) providing fraud training to all Exempt Organization employees;

[128] See letter from IRS-TEGE dated 25 October 2005 announcing Exempt Organization implementation guidelines for FY2006 published on the IRS website.

(c) training Criminal Investigation agents on exempt organization issues, and providing technical assistance to Criminal Investigations in terrorism-related investigations; and

(d) continuing to work closely with Treasury and other agencies, including the DOJ, on terrorism task forces and specific cases.

7.1.2 Recommendations and Comments

1303. Overall, authorities seem to be well-equipped, staffed, resourced and trained. However, there is one particular weakness—specifically, the IRS which is understaffed and thus may not be equipped to carry out its responsibilities as currently defined.

7.1.3 Compliance with Recommendation 30

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.30	LC	• The IRS is not adequately resourced to conduct examinations of the entities that it is responsible for supervising, in particular, the MSB and insurance sectors.

7.2 Statistics (R.32)

7.2.1 Description and Analysis

Regular review of the AML/CFT system

1304. The U.S. regularly reviews the effectiveness of their AML/CFT systems. Most recently, the U.S. issued the 2006 U.S. Money Laundering Threat Assessment which sets out key AML risks that the U.S. is currently facing.

1305. Additionally, the U.S. government dedicates resources to monitoring the number of BSA examinations, blocked transactions and BSA enforcement actions taken by the U.S. against violators. Based on the results of this monitoring, FinCEN has taken steps to develop civil cases, where appropriate, that address non-compliance across the spectrum of financial institutions subject to the BSA. This has included the assessment of penalties and other appropriate remedies as the facts warrant. The U.S. government also has an ongoing process in place of taking a critical look at the regulations, assessing how they are working in practice, and making any necessary adjustments to ensure that they achieve their goals. The federal government also works to engage state governments, and in some instances tribal and municipal governments, in AML/CFT, particularly as AML regulation is extended to categories of financial institutions that are predominately regulated at the state level.

Statistics on suspicious transactions and other forms of reporting

1306. Twice annually, FinCEN publishes on its website the "The SAR Activity Review-By The Numbers". This publication provides statistics outlining the number of filings for each of the SARs required to be filed by depository institutions, MSBs, casinos and card clubs, and securities and futures industries. The statistics accumulated in the publication include number of filings by U.S. states and territories, by violation reported, and by year and month of filing. Additional law enforcement case summaries are published, again twice annually in the spring and fall, on FinCEN's website.

1307. FinCEN's annual report contains statistics relating to the number of SARs analyzed and disseminated.

1308. The U.S. also maintains comprehensive statistics on the number of reports filed on cash transactions above USD 10,000 (the CTR and Form 8300 reporting requirements) and cross border transportations of currency.[129]

1309. However, the U.S. does not keep statistics concerning the volume of wire transfer activity into or out of the U.S. annually. If wire transfer activity is considered to be suspicious, however, it may be reported to FinCEN. In such cases, the SAR may indicate, as a violation category, that the suspicious activity relates to wire transfer fraud or the unusual use of wire transfer. Statistics concerning the violation category that is recorded on SARs are maintained and routinely published by FinCEN in its annual publication, "Suspicious Activity Reports – By The Numbers".

Statistics relating to ML/FT investigations, prosecutions and convictions

1310. The U.S. collects and maintains statistics concerning the number of prosecutions and convictions that relate to the federal money laundering offenses. Statistics concerning the number of federal investigations for money laundering seem to be maintained by the federal law enforcement agency involved in the investigations as well as the DOJ which conducts the prosecutions. The statistics provided by law enforcement agencies on money laundering prosecutions are categorized broadly into the type of offense (e.g. "white collar crime) rather than according to particular felony violations.

1311. The executive branch is compelled by law to maintain records and statistics concerning, and to periodically report to Congress on, foreign terrorism investigations, prosecutions and convictions. Among the reports periodically prepared by the Executive Branch are semi-annual reports on each of the emergencies declared by the President under that authority. In addition, the executive branch is required to report to Congress semi-annually in relation to financial intelligence on terrorist assets [s.342(a) of the Intelligence Authorization Act for Fiscal Year 2003 amended Title I of the National Security Act of 1947]. Such reports must include information on: (1) the number of asset seizures, designations, and other actions against individuals or entities found to have engaged in financial support of terrorism; (2) the number of applications for asset seizure and designations of individuals or entities suspected of having engaged in financial support of terrorist activities granted, modified, or denied; (3) the number of searches of individuals or entities suspected of having engaged in financial support for terrorist activity; and (4) whether the financial intelligence information seized in these cases has been shared on a full and timely basis with other entities of the U.S. government involved in related intelligence activities. These reports and statistics were not made available to the assessment team. Due to the lack of information, it is not possible to assess the effectiveness of statistics collection in this area.

Statistics relating to freezing, seizing and confiscation

1312. The U.S. also maintains statistics concerning the amount of assets frozen, seized and confiscated. The statistical figures present an overall view on the amounts of assets forfeited. However, no differentiation is made between instrumentalities and proceeds. Likewise, there is no breakdown concerning which freezing/seizing and confiscation actions specifically relate to money laundering or terrorist financing cases. Additionally, no statistics were provided concerning the number and amount of TF-related confiscations. Nevertheless, overall, the statistics give an accurate picture of the performance of the forfeiture system as a whole.

Statistics relating to mutual legal assistance and international requests for cooperation

1313. The statistics that were provided to the assessment team are sufficiently detailed as to give a reliable picture of the MLA activity in respect of AML and CFT. However, although they cover a

[129] Reports concerning cash transactions over USD 10,000 are filed on a Form 104 (CTR) (in the case of a financial institution) or a Form 8300 (in the case of a person engaged in a trade and business—other than a financial institution required to file a CTR). Reports concerning the cross border transportation of currency are filed on a CMIR.

period of nearly 5 years, they are not broken down per year. Consequently, it is difficult to deduce any evolution in the annual number of requests.

1314. The U.S. keeps statistics on the number of incoming and outgoing mutual legal assistance requests relating to both money laundering and terrorist financing. OIA's electronic case tracking system reflects the approximate numbers of incoming and outgoing requests for mutual legal assistance and extradition from 1 January 2000 to 22 July 2005 (see section 6.4) for both money laundering and terrorist financing. In the area of terrorism financing, these cases are categorized in the OIA case tracking system as either "financial transactions with designated countries/terrorism" or "providing material support or resources/terrorism." Requests relating to the freezing, seizing and confiscation of property are included in the overall figure, but not specified. The statistics indicate the grounds of the request and whether it was granted or refused. However, the statistics do not show the nature of the request or the time that was required to respond.

1315. FinCEN maintains statistics concerning the number of requests for assistance received from foreign FIUs. All such requests (except those relating to due diligence) are accepted. Other statistics maintained by FinCEN include: (1) the number of requests that it makes to foreign FIUs on behalf of U.S. law enforcement agencies (although no statistics are maintained concerning whether such requests are granted or refused); and (2) the number of spontaneous referrals made to FinCEN by foreign authorities.

1316. However, FinCEN does not maintain statistics relating to the number of spontaneous referrals made by it to foreign FIUs. It is, however, researching the feasibility of tracking this information using its existing database tools.

Statistics relating to supervisory and other action

1317. The federal regulators maintain a broad range of statistics, including a record of examinations for AML/CFT compliance, and numbers and types of enforcement actions taken and penalties imposed for non-compliance.

Additional elements

1318. Although FinCEN does not maintain comprehensive statistics on SARs resulting in investigation, prosecution, or convictions for ML, FT or underlying predicate offenses, examples of investigations that have been assisted by this information can be found in various issues of "The Suspicious Activity Review – Trends, Tips & Issues", which is published twice a year; statistics for the "Suspicious Activity Review – By the Numbers" are published quarterly. Standard features of the SAR Activity Review include summaries of law enforcement cases in which Suspicious Activity Reports played a role in a successful investigation. All published SAR Activity Reviews are available on FinCEN's public website in the publications section. In addition FinCEN's public website provides links to various law enforcement agencies which provide examples where SARs assisted in their investigations for the period of December 2003 to May 2005.

1319. The U.S. does maintain some statistics concerning the criminal sanctions that have been applied to persons convicted of money laundering offenses, including the period of incarceration actually served.

1320. As noted above, FinCEN publishes the "SAR Activity Review" which includes statistics relating to the Section 314(a) process, broken down by the number of new accounts and transactions identified by industry responses to 314(a) requests, as well as the number of subpoenas, search warrants, arrests, and indictments resulting from 314(a) information. As well, each of IRS-CI's foreign posts maintains comprehensive statistics on all requests for assistance made by foreign counterparts to those posts, including those for money laundering and terrorist financing. IRS-CI is in the process of designing a new database that will allow the consolidation of this information into a

centralized database stored in headquarters. All requests for assistance are tracked from receipt until completion. Upon completion, the disposition of the request is noted in the database.

7.2.2 Recommendations and Comments

1321. FinCENs statistics do not provide a complete picture of the extent to which SARs ultimately contribute to investigations and convictions. This reflects the lengthy nature of money laundering and financial crime investigations, which makes it difficult for FinCEN and law enforcement to coordinate feedback on the ultimate utility of individual SARs; law enforcement may not immediately recognize the value of SAR information to an investigation. Furthermore, under U.S. law (generally) SARs cannot be used for evidentiary purposes and can only be used as a pointer to evidentiary documentation that is ultimately used in trial proceedings, perhaps months or years after the initial filing of a SAR. FinCEN does, however, collect and maintain data on the number of SARs analyzed and disseminated in connection with the law enforcement investigations it supports, as well as the pro-active products it refers to its law enforcement customers. FinCEN also tracks SAR value through FinCEN's Gateway system, which provides direct access to BSA data for law enforcement users. The Gateway system records pro-active use of SARS, as well as users' evaluations of whether SARs viewed by users are of interest for their investigations (see the discussion under section 2.5 in the discussion of Recommendation 26). Finally, FinCEN exerts considerable effort to obtain and record case-specific feedback from its law enforcement customers about the usefulness of FinCEN's products to law enforcement investigations, and FinCEN publishes case-specific information on SAR value through the SAR Activity Review.

1322. The statistics held in respect of terrorism and terrorist financing should also focus on the confiscation aspect.

1323. Statistics relating to supervisory actions are not comprehensive. In particular, there are no statistics that measure the supervisory actions that has been taken specifically in relation to the AML/CFT obligations in the MSB sector.

7.2.3 Compliance with Recommendation 32

	Rating	Summary of factors underlying rating
R.32	LC	• Freezing, seizing and confiscation statistics are not specified into ML and TF related seizures and confiscations. • No statistics on TF related confiscations. • FinCEN collects and maintains substantial valuable statistical BSA data, which can be used to provide a partial picture of the effectiveness of the U.S. AML/CFT regime; however, FinCEN's data would need to be coupled with that of other federal agencies and departments in order to produce a comprehensive view of overall effectiveness of U.S. AML/CFT systems. • MLA and extradition statistics are not broken down annually, and do not show the time required to respond to a request.

7.3 Other relevant AML/CFT measures or issues

1324. There are no other additional measures or issues to discuss in this section.

7.4 General framework for AML/CFT system (see also section 1.1)

1325. There are no particular structural elements of the general legal and institutional framework that significantly impair or inhibit the effectiveness of the AML/CFT system.

TABLES

Table 1: Ratings of Compliance with FATF Recommendations
Table 2: Recommended Action Plan to improve the AML/CFT system

Table 1. Ratings of Compliance with FATF Recommendations

The rating of compliance vis-à-vis the FATF Recommendations should be made according to the four levels of compliance mentioned in the 2004 Methodology (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC)), or could, in exceptional cases, be marked as not applicable (na).

Forty Recommendations	Rating	Summary of factors underlying rating[130]
Legal systems		
1. ML offense	LC	• The list of domestic predicate offenses does not fully cover 2 out of the 20 designated categories of offenses specifically (insider trading and market manipulation, and piracy). • The list of foreign predicate offenses does not cover 8 out of the 20 designated categories of offenses. • The definition of "transaction" in s.1956(a)(1) means that mere possession as well as concealment of proceeds of crime , does not constitute the laundering of proceeds. • The definition of "property" in relation to the section 1956(a)(2) offense (international money laundering) only includes monetary instruments or funds.
2. ML offense – mental element and corporate liability	C	• The Recommendation is fully observed.
3. Confiscation and provisional measures	LC	• Where the proceeds are derived from one of the designated categories of offenses that are not domestic or foreign predicate offenses for ML, a freezing/seizing or confiscation action cannot be based on the money laundering offense. • Property of equivalent value which may be subject to confiscation cannot be seized/restrained.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	C	• This Recommendation is fully observed.
5. Customer due diligence	PC	• No obligation in law or regulation to identify beneficial owners except in very specific circumstances (i.e. correspondent banking and private banking for non-U.S. clients). • No explicit obligation to conduct ongoing due diligence, except in certain defined circumstances. • Customer identification for occasional transactions limited to cash deals only. • No requirement for life insurers issuing covered insurance products to verify and establish the true identity of the customer, (except for those insurance products that fall within the definition of a "security" under the federal securities laws). • No measures applicable to investment and commodity advisers. • Verification of identity until after the establishment of the business relationship is not limited to circumstances where it is essential not to interrupt the normal course of business. • No explicit obligation to terminate the business relationship if

130 These factors are only required to be set out when the rating is less than Compliant.

		verification process cannot be completed. • The effectiveness of applicable measures in the insurance sector (which went into force on 2 May 2006) cannot yet be assessed.
6. Politically exposed persons	LC	• Measures relating to PEPs do not explicitly apply to MSBs, the insurance sector, investment and commodity trading advisers.
7. Correspondent banking	LC	• No obligation to require senior management approval when opening individual correspondent accounts.
8. New technologies & non face-to-face business	LC	• No explicit provision requiring life insurers MSBs, or investment and commodity trading advisers to have policies and procedures for non-face-to-face business relationships or transactions.
9. Third parties and introducers	LC	• No explicit obligation on relying institution to obtain core information from introducer. • No measures have been applied to investment and commodity trading advisers, or the insurance sector.
10. Record keeping	LC	• Life insurers of covered products are only required to keep limited records of SARs, Form 8300s, their AML Program and related documents.
11. Unusual transactions	LC	• In the insurance, and MSB sectors, there is no specific requirement to establish and retain (for five years) written records of the background and purpose of complex, unusual large transactions or unusual patterns of transaction that have no apparent or visible economic or lawful purpose (outside of the SAR, CTR and Form 8300 requirements) • No measures have been applied to investment and commodity trading advisers.
12. DNFBP – R.5, 6, 8-11	NC	• Casinos are not required to perform enhanced due diligence for higher risk categories of customer, nor is there a requirement to undertake CDD when there is a suspicion of money laundering or terrorist financing (R.5). • Accountants, dealers in precious metals and stones, lawyers and real estate agents are not subject to customer identification and record keeping requirements that meet Recommendations 5 and 10. • None of the DNFBP sectors is subject to obligations that relate to Recommendations 6, 8 or 11 (except for casinos in relation to R.11).
13. Suspicious transaction reporting	LC	• The existence of a USD 5,000 threshold for reporting suspicious activity. • No measures have been applied to investment and commodity trading advisers. • The effectiveness of measures in the insurance and mutual funds sectors cannot yet be assessed.
14. Protection & no tipping-off	C	• The Recommendation is fully observed.
15. Internal controls, compliance & audit	LC	• AML Program requirements have not been applied to certain non-federally regulated banks, investment and commodity trading advisers. • It is not yet possible to assess the effectiveness of these measures in the insurance sector • There is no obligation under the BSA for financial institutions to implement employee screening procedures.

16. DNFBP – R.13-15 & 21	NC	• Casinos are the only DNFBP sector that is required to report suspicious transactions; however, there is a threshold on that obligation. • Accountants, lawyers, real estate agents and TCSPs are not subject to the "tipping off" provision or protected from liability when they choose to file a suspicious transaction report. • Accountants, lawyers, real estate agents and TCSPs are not required to implement adequate internal controls (i.e. AML Programs). • Dealers in precious metals, precious stones, or jewels are required to implement AML programs; however, the effectiveness of implementation cannot yet be assessed. • There are no specific obligations on accountants, lawyers, real estate agents or TCSPs to give special attention to the country advisories that FinCEN has issued and which urge enhanced scrutiny of financial transactions with countries that have deficient AML controls.
17. Sanctions	LC	• Some banking and securities participants are not subject to all AML/CFT requirements and related sanctions at the federal level. • The effectiveness of the measures in the insurance sector can not yet be assessed. • There are concerns about how effectively sanctions are applied in the MSB sector given the current level of the IRS's resources.
18. Shell banks	C	• The Recommendation is fully observed.
19. Other forms of reporting	C	• The Recommendation is fully observed.
20. Other NFBP & secure transaction techniques	C	• This Recommendation is fully observed.
21. Special attention for higher risk countries	LC	• In the insurance sector, there is no specific requirement to establish and retain written records of transactions with persons from/in countries that do not or insufficiently apply the FATF Recommendations. • No measures have been applied to investment and commodity trading advisers
22. Foreign branches & subsidiaries	LC	• BSA requirements do not apply to the foreign branches and offices of domestic life insurers issuing and underwriting covered life insurance products.
23. Regulation, supervision and monitoring	LC	• Some securities sector participants are not subject to supervision for AML/CFT requirements. • The effectiveness of the measures in the insurance sector can not yet be assessed. • Concerns about IRS examination resources.
24. DNFBP - regulation, supervision and monitoring	PC	• There is no regulatory oversight for AML/CFT compliance for accountants, lawyers, real estate agents or TCSPs. • The supervisory regime for Nevada casinos is currently not harmonized with the BSA requirements.
25. Guidelines & Feedback	C	• The Recommendation is fully observed.
Institutional and other measures		
26. The FIU	LC	• The effectiveness of FinCEN, is impeded by: - perceptions concerning the value of its products and the risk that over-emphasis on FinCEN's network function will weaken its place in the AML/CFT chain; - the handling of the huge amount of 14 million reports of which 70% are still filed in a paper format; - the fact that SAR filing is only done in 30-60 days after detection;

		and - insufficient adequate/timely feedback to reporting institutions. • Since terrorism-related information in requests from foreign FIUs is shared with law enforcement—for networking—without the prior authorization of the foreign FIU, the U.S. does not act in accordance with international principles of information exchange established by the Egmont Group.
27. Law enforcement authorities	C	• The Recommendation is fully observed.
28. Powers of competent authorities	C	• The Recommendation is fully observed.
29. Supervisors	C	• This Recommendation is fully observed.
30. Resources, integrity and training	LC	• The IRS is not adequately resourced to conduct examinations of the entities that it is responsible for supervising, in particular, the MSB and insurance sectors.
31. National co-operation	LC	• There remains a gap between the policy level and operational level law enforcement work. • More refined coordination is needed amongst law enforcement agencies with overlapping jurisdictions.
32. Statistics	LC	• Freezing, seizing and confiscation statistics are not specified into ML and TF related seizures and confiscations. • No statistics on TF related confiscations. • FinCEN collects and maintains substantial valuable statistical BSA data, which can be used to provide a partial picture of the effectiveness of the U.S. AML/CFT regime; however, FinCEN's data would need to be coupled with that of other federal agencies and departments in order to produce a comprehensive view of overall effectiveness of U.S. AML/CFT systems. • MLA and extradition statistics are not broken down annually, and do not show the time required to respond to a request.
33. Legal persons – beneficial owners	NC	• While the investigative powers are generally sound and widely used, there are no measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. • There are no measures taken by those jurisdictions which permit the issue of bearer shares to ensure that bearer shares are not misused for money laundering.
34. Legal arrangements – beneficial owners	NC	• While the investigative powers are generally sound and widely used, there is minimal information concerning the beneficial owners of trusts that can be obtained or accessed by the competent authorities in a timely fashion.
International Co-operation		
35. Conventions	LC	• Not all conduct specified in Article 3 (Vienna) and Article 6 (Palermo) has been criminalized, and there is no a sufficiently comprehensive list of foreign predicates related to organized criminal groups as required by Article 6(2)(c) (Palermo).
36. Mutual legal assistance (MLA)	LC	• Dual criminality may impede MLA where the request relates to the laundering of proceeds that are derived from a designated predicate offense which is not covered.

37. Dual criminality	C	• This Recommendation is fully observed.
38. MLA on confiscation and freezing	LC	• Dual criminality may impede MLA where the request relates to the laundering of proceeds that are derived from a designated predicate offense which is not covered.
39. Extradition	LC	• Dual criminality may impede extradition where the request relates to the laundering of proceeds that are derived from a designated predicate offense which is not covered. • List-based treaties do not cover ML.
40. Other forms of co-operation	C	• This Recommendation is fully observed.
Nine Special Recommendations	Rating	Summary of factors underlying rating
SR.I Implement UN instruments	LC	• Not all UN1267 designations are transposed in the OFAC list.
SR.II Criminalize terrorist financing	C	• This Recommendation is fully observed.
SR.III Freeze and confiscate terrorist assets	LC	• Compliance monitoring in non-federally regulated sectors (e.g. insurance, MSBs) is ineffective. • Not all S/RES/1267(1999) designations are transposed in the OFAC list.
SR.IV Suspicious transaction reporting	LC	• The existence of a USD 5,000 threshold for reporting suspicious activity. • No measures have been applied to investment and commodity trading advisers. • The effectiveness of measures in the insurance and mutual funds sectors cannot yet be assessed.
SR.V International co-operation	LC	• List-based treaties do not cover FT.
SR VI AML requirements for money/value transfer services	LC	• The limitations identified under Recommendation 5, 8, 13 and SR.IV with respect to the MSB sector also affect compliance with Special Recommendation VI. • Major concerns with respect to resources of the IRS for monitoring of this sector.
SR VII Wire transfer rules	LC	• Threshold of USD 3,000 instead of USD 1,000 as is required by the revised Interpretative Note. • It is not mandatory to include all required originator information on batch transfers.
SR.VIII Non-profit organizations	C	• This Recommendation is fully observed.
SR.IX Cross Border Declaration & Disclosure	C	• The Recommendation is fully observed.

Table 2: Recommended Action Plan to Improve the AML/CFT System

AML/CFT System	Recommended Action (listed in order of priority)
1. General	
2. Legal System and Related Institutional Measures	
2.1 Criminalization of Money Laundering (R.1 & 2)	• Expand the list of foreign predicate offenses to include all of the domestic predicate offenses (including piracy, market manipulation and insider trading). • Amend the list of SUA to include the offenses of piracy, market manipulation and insider trading. • Take legislative measures to ensure that the definition of "transaction" is broadened to cover all conduct as required by the Vienna and Palermo Conventions. • Take legislative measures to ensure that the scope of the section 1956(a)(2) offense is broadened include proceeds other than funds or monetary instruments.
2.2 Criminalization of Terrorist Financing (SR.I)	• There are no recommendations for this section.
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	• Extend domestic and foreign predicates to fully cover all 20 categories of predicate offenses listed in the Glossary to the FATF 40 Recommendations. • Take measures to ensure that property which may be subject to equivalent value confiscation may be seized/restrained to prevent its being dissipated.
2.4 Freezing of funds used for terrorist financing (SR.III)	• Take further efforts to be made to improve compliance monitoring of all targeted entities, particularly the state-regulated sectors and DNFBPs. • Given that the reliability of the 1267 list has been improved through successive rounds of corrections and additions of identifiers, the U.S. should consider revising its approach to listing the Taliban as an entity, rather than including individual names, particularly where those names have sufficient identifiers.
2.5 The Financial Intelligence Unit and its functions (R.26)	• FinCEN should invest in a faster and more efficient reporting system with a preference to: (1) mandatory e-filing for all reporting institutions, and (2) the use of a single form for all reporting institutions. • FinCEN should ensure that it receives adequate and continual feedback from law enforcement agencies using the BSA-direct system so that it does not lose its important position within the AML/CTF chain. • FinCEN should improve its guidance and feedback with a view to improving the quality of reports filed by reporting entities. • FinCEN should also ensure that its information and guidance for reporting entities is combined and/or coordinated with the law enforcement agencies and regulators that issue similar or related material. • FinCEN should focus on the challenge of promoting the added-value of its analytical products to law enforcement. • Law enforcement agencies should work at the operational level to change their perceptions concerning the value of FinCEN's products (i.e. by promoting within their agencies a broader use of FinCEN's ability to produce operational and/or strategic analysis). • The U.S. should handle terrorism-related information received in requests from foreign FIUs in accordance with international principles of information exchange.
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	• There are no recommendations for this section.

2.7 Cross Border Declaration & Disclosure	• Further invest in the detection and investigation as well as the resources, techniques and methods to counter outgoing cross-border transportations of cash or any negotiable bearer instrument. • Focus on conducting thorough border checks of people, vehicles, trains, cargo, etc., without allowing the level of thoroughness to be dictated by the volume of traffic waiting to cross the border.
3. Preventive Measures – Financial Institutions	
3.1 Risk of money laundering or terrorist financing	• Extend AML/CFT measures to investment and commodity trading advisers, and the limited number of depository institutions that are currently not covered,
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)	• Introduce a primary obligation to identify the beneficial owners of accounts (which may, of course, be implemented on a risk-based approach with respect to low-risk customers or transactions). • Implement a CIP requirement for the insurance sector. • Introduce an explicit obligation that financial institutions should conduct ongoing due diligence, rather than rely on an implicit expectation within the SAR requirements and on the existing guidance. • In the case of occasional transactions, extend the customer identification obligation to non-cash transactions. • Other than with respect to non-face-to-face business, securities transactions, and life insurance business, limit the circumstances in which institutions may open an account prior to completing the verification process, and introduce a presumption that institutions should close an account whenever the verification cannot be completed, for whatever reason. If necessary, accompany this with some form of indemnification against other conflicting statutes. • Introduce an explicit requirement that the opening of individual correspondent accounts should involve senior management approval. • Extend AML/CFT obligations (including the PEPs requirements) to investment advisers and commodity trading advisers, in line with those applicable to the rest of the securities industry. • Publish confirmation that, despite the promulgation of the final section 312 rule, the 2001 Guidance on PEPs remains in force and that it applies to all relevant financial institutions. • Introduce an explicit requirement for the life insurance and MSB sectors to address the specific risks associated with non-face to face business relationships or transactions. • Extend the obligation for AML Programs and CIP (as applicable) to all depository institutions to remove the historical anomaly.
3.3 Third parties and introduced business (R.9)	• Introduce a requirement that the relying bank or other financial institution should obtain immediately from the introducing institution details relating to the identity of the account holder, the beneficial owner, and the reason for which the account is being opened. • Extend such measures to investment and commodity trading advisers, and the insurance sector (including insurance agents and brokers).
3.4 Financial institution secrecy or confidentiality (R.4)	• There are no recommendations for this section.
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	• Ensure that NACHA completes its current process of developing and approving a rule that would allow cross-border ACH transfers to meet the new FATF requirements with respect to batch transfers before January 2007. • Ensure that the threshold is lowered to USD 1,000 before January 2007. • Extend full record-keeping requirements to the insurance sector, including insurance brokers and agents. • Consider simplifying the record keeping framework.
3.6 Monitoring of transactions and	• Extend the requirement to establish and retain (for five years) written findings

relationships (R.11 & 21)	that relate to unusual transactions to those participants in the securities sector that are currently not subject to a requirement to file SARs. • Require insurers to establish and retain written records of transactions with persons from/in countries that do not or insufficiently apply the FATF Recommendations to the extent that this is not already addressed by the AML program and SAR requirements • Extend the requirements to establish and retain written records of transactions with persons from/in countries that do not or insufficiently apply the FATF Recommendations to those participants in the securities sector that are currently not covered.
3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	• Remove the threshold from the reporting obligation. • Extend the SAR obligations to investment advisers and commodity trading advisers. • Consider imposing direct SAR reporting requirements on independent insurance agents and brokers. • Clarify that confidentiality of SARs applies to the more limited disclosure restrictions under the BSA (i.e. to any person involved in the transaction) to put current practice beyond doubt.
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	• Extend the AML Program requirement to the limited number of non-federally regulated depository institutions that are currently exempted. • Complete the process of extending AML Program requirements to unregistered investment companies, investment advisers and commodity trading advisers. • Ensure that insurance companies are required to apply AML/CFT measures to their foreign branches and subsidiaries. • Require all financial institutions (not just those in the securities sector) to screen prospective employees for high standards.
3.9 Shell banks (R.18)	• There are no recommendations for this section.
3.10 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	• In the securities and insurance sectors issue guidance similar to the FFEIC manual. • Extend AML Program requirements to the limited number of uninsured, state-chartered banks and other depository institutions that are currently exempt. • Consider providing more and better resources to examining AML compliance in the privately insured credit union sector. • Ensure that the new AML/CFT measures applicable to the insurance sector are implemented effectively. • Once AML/CFT measures are applied to the investment advisers and commodity trading advisers, ensure that they are effectively supervised, monitored and (if appropriate) sanctioned for compliance. • Ensure that the IRS has sufficient resources to undertake comprehensive examinations of the large number of institutions for which it is responsible.
3.11 Money value transfer services (SR.VI)	• Undertake a thorough review of the workload and resources of the IRS in the area of BSA compliance to ensure that the allocation of responsibilities is delivering the most effective and efficient results (i.e. are other agencies better placed to take on some of these responsibilities?). • Irrespective of any reallocation of responsibilities, it is clearly the case that the IRS needs to be allocated significantly more resources simply to address the MSB sector. • Extend the examination program for agents quite extensively. • Make further efforts are made to standardize the AML examination procedures both between the states, and between the individual states and the IRS.

4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	• Explicitly require casinos to perform enhanced due diligence for higher risk categories of customers and to undertake CDD when there is a suspicion of money laundering or terrorist financing. • Extend customer identification, record keeping and account monitoring obligations that are consistent with FATF Recommendations to these sectors as soon as possible. • Extend obligations that relate to Recommendations 6, 8 or 11 to all DNFBPs. (This does not apply to casinos in relation to R.11). • In the short term, a proposed final rule should be issued to expedite the introduction of AML obligations for "persons involved in real estate closings and settlements." • Prepare an advanced notice of proposed rulemaking in the near future in relation to the TCSP sector to extend both the AML Program and CIP requirements to this sector.
4.2 Suspicious transaction reporting (R.16)	• Remove the threshold on the SAR reporting obligation for casinos. • Extend the obligation to report suspicious transactions to the other DNFBP sectors. • Accountants, lawyers, real estate agents and TCSP should be made subject to the "tipping off" provision and should be protected from liability when they choose to file a suspicious transaction report. • Accountants, lawyers, real estate agents and TCSP should also be required to implement adequate internal controls (i.e. AML Programs). • Continued work is needed to ensure that dealers in precious metals and stones are aware of their obligation to establish AML Programs and are implementing them effectively. • The U.S. should obligate accountants, lawyers, real estate agents and TCSPs to give special attention to the country advisories that FinCEN has issued and which urge enhanced scrutiny of financial transactions with countries that have deficient AML controls.
4.3 Regulation, supervision and monitoring (R.24-25)	• Accountants, lawyers, real estate agents and TCSPs should be made subject to AML/CFT obligations and appropriate regulatory oversight. • In the case of TCSPs a registration process should be introduced for agents engaged in the business of providing company formation and related services (perhaps with a de minimis threshold to ensure that single company agents are not required to register). • The regulatory regime applied to the casino sector generally appears to be working effectively. However, the work to further harmonize Nevada's regulatory requirements with the BSA should continue as rapidly as possible.
4.4 Other non-financial businesses and professions (R.20)	• Consideration of extending BSA requirements to other sectors should proceed as quickly as possible.
5. Legal Persons and Arrangements & Non-Profit Organizations	
5.1 Legal Persons – Access to beneficial ownership and control information (R.33)	• Undertake a comprehensive review to determine ways in which adequate and accurate information on beneficial ownership may be available on a timely basis to law enforcement authorities for companies which do not offer securities to the public or whose securities are not listed on a recognized U.S. stock exchange. It is important that this information be available across all states as uniformly as possible. It is further recommended that the federal government seek to work with the states to devise procedures which should be adopted by all individual states to avoid the risk of arbitrage between jurisdictions. As the January 2006 threat assessment indicates, the U.S. authorities are well aware of the problems created by company formation arrangements, and have formulated an initial program to try to address the issue. This should be pursued in a shorter timescale than seems to be envisaged at present. In particular, the proposal to bring company formation agents within the BSA framework, and to require them

	to implement AML Programs and CIP procedures should be taken forward in the very near future.
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)	• Implement measures to ensure that adequate, accurate and timely information is available to law enforcement authorities concerning the beneficial ownership and control of trusts.
5.3 Non-profit organizations (SR.VIII)	• Continue to devote resources to preventing the abuse of this sector from terrorist organizations, including ensuring the effective flow of information between competent authorities.
6. National and International Co-operation	
6.1 National co-operation and coordination (R.31)	• Continue to work towards closing the gap that still seems to remain between the policy level and the factual operational law enforcement work. • Consider expanding the HIFCA and HIDTA model, provided that it is appropriately resourced and developed • Law enforcement agencies should take more refined coordination at the operational level, perhaps in the context of the Treasury's recent government-wide analysis on money laundering. Such a study should not lead to the creation of new entities, but rather initiate a discussion on the basic law enforcement framework in a system as complex as that in the U.S.
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	• Review the money laundering offenses to ensure all conduct required to be criminalized by the Vienna and Palermo Conventions is covered. • Include "participation in an organized criminal group" as a foreign predicate offense as required by Article 6(2)(c) of the Palermo Convention. • Transpose all S/RES/1267(1999) designations in the OFAC list.
6.3 Mutual Legal Assistance (R.36-38 & SR.V)	• A formal legal basis should be provided to allow for equivalent value seizure upon a foreign request. • Extend the list of domestic and foreign predicate offenses to all 20 designated categories.
6.4 Extradition (R.39, 37 & SR.V)	• Extend the list of domestic and foreign predicate offenses to all 20 designated categories. • Ensure that older, list based extradition treaties that were concluded before the introduction of money laundering and terrorism financing offenses in the respective legislations and that have not been supplemented since do not pose an obstacle to extradition. • Consider allowing extradition according to the principles of the UN TF Convention on an ad hoc and unilateral basis.
6.5 Other Forms of Co-operation (R.40 & SR.V)	• FinCEN should improve the quality of its analytical research reports so that they contain a more practical and deeper level of analysis tailored to the specific investigative needs of the requesting FIU.
7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	• Ensure that the IRS is adequately resourced to effectively supervise all of the entities that it is responsible for. • Ensure that all of the statistics required by R.32 are collected and maintained. • The statistics held in respect of terrorism and terrorist financing should also focus on the confiscation aspect. • Statistics relating to supervisory actions are not comprehensive. In particular, there are no statistics that measure the supervisory actions that has been taken specifically in relation to the AML/CFT obligations in the MSB sector.