[*Text as released to Congress; see revised version]

Rwanda

Rwanda is not a major financial center. Since recovering from the 1994 genocide and war, Rwanda's banking system has been largely controlled by the government and is now in the process of privatization. Two of eight banks were privatized in 2004. The Rwandan financial system lacks the efficiencies of more modern banking systems, such as electronic funds transfers or credit card transactions. As that system develops and the country becomes more stable, and as neighboring countries like Kenya and Tanzania increase their enforcement efforts, there is a risk of increased illegal financial activity in Rwanda.

There are no documented reports of money laundering in Rwanda, primarily due to the government's close monitoring through the Central Bank of monetary transfers totaling more than $50,000, whether domestic or international. The authority for such monitoring is granted in the Rwandan Banking Act of 2000. We do not know if Rwandan financial institutions engage in international narcotics-trafficking transactions or whether Rwanda has entered into bilateral agreements for the exchange of information on money laundering with other countries. Since Rwanda has been the recipient of large amounts of foreign assistance, the IMF and the World Bank continue to monitor the banking sector, particularly with regard to government spending. In addition, most of the country's charitable and nonprofit entities are recipients of international aid and are largely monitored by their donors, the IMF and/or the World Bank.

There is evidence that the Government of Rwanda (GOR) indirectly engaged in mineral transfers from the Congo during the Rwandan occupation of the eastern Congo that ended in the fall of 2002. The National Bank of Rwanda (BNR) and the Rwandan Private Sector Federation (the Rwandan equivalent of the chamber of commerce) both confirmed the large amounts of Rwandan profits obtained from the processing of coltan from 1999 through 2001. According to the BNR, the profits reportedly peaked at $3 million in customs fees and banking profits in a two-month period in 2000. These profits helped fuel the Rwandan GDP growth rate of 9 percent for 2002. Neither organization could confirm significant transactions in Congolese diamonds.

For the past three years, Rwanda has been completely overhauling its legal system, and the Rwandan Parliament is enacting new legislation affecting Rwandan financial law. There remains no provision for the prosecution of potential money laundering cases, however, and, no regulation of imports and exports, except for post-checks on transferred goods. According to legal experts with the Rwandan Finance Ministry and the Prosecutor General's office, no laws under consideration would curb secrecy in respect to client and ownership information in either domestic or offshore financial transactions. Additionally, there are no laws in place concerning banker negligence or the forfeiture and seizure of assets in cases involving narcotics-trafficking, serious crimes or terrorists. No arrests for money laundering or terrorist financing have occurred in Rwanda since January 1, 2003.

Rwanda has officially committed itself to locating and freezing terrorist assets identified by the international community. However, Rwanda has yet to develop fully its laws and its ability to enforce regulations against terrorist financing in accordance with the relevant UN resolutions. The GOR does, however, retain the power to identify, freeze, and seize terrorist-related financial assets. The Ministry of Finance circulates lists of identified individuals and organizations included on the UNSCR 1267 Sanctions Committee's consolidated list. Rwanda is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism.

The GOR cooperates with the U.S. when requested in connection with investigations and proceedings related to narcotics, terrorism, terrorist financing, and other serious crimes. For example, the Rwandan National Police's (RNP) Economic Crimes Division has cooperated with the USG in check embezzlement investigations that led to arrests in Uganda. However, the RNP lacks the experience, training, and resources to be effective in investigating and enforcing laws concerning modern money

laundering and terrorist financing. Furthermore, no formal body of laws or regulations concerning this cooperation currently exists in Rwanda.

The Government of Rwanda should enact comprehensive anti-money laundering legislation covering all serious crimes, including terrorist financing, and take steps to develop a viable anti-money laundering regime. Rwanda should also consider becoming an observer to the Eastern and Southern Africa Anti-Money Laundering Group.

Samoa

Samoa does not have major organized crime, fraud, or drug problems. The most common crimes that generate revenue within the jurisdiction are primarily the result of low-level fraud and theft. The domestic banking system is very small, and there is relatively little risk of significant money laundering derived from domestic sources. Samoa's offshore banking sector is relatively small. The Government of Samoa (GOS) enacted the Money Laundering Prevention Act (the Act) in 2000. This law criminalizes money laundering associated with numerous crimes, sets measures for the prevention of money laundering and related financial supervision. Newly adopted regulations and guidelines fully implementing this legislation came into force in 2002. Under the Act, a conviction for a money laundering offense is punishable by a fine not to exceed Western Samoa Tala (WST) one million (approximately $354,000), a term of imprisonment not to exceed seven years, or both.

The Act requires financial institutions to report transactions considered suspicious to the Money Laundering Prevention Authority (MLPA), the Samoa Financial Intelligence Unit (FIU) currently working under the auspices of the Governor of the Central Bank. The MLPA receives and analyzes disclosures, and if it establishes reasonable grounds to suspect that a transaction involves the proceeds of crime, it refers the information to the Attorney General and the Commissioner of Police. In 2003, Samoa established under the authority of the Ministry of the Prime Minister, an independent and permanent Transnational Crime Unit (TCU). The TCU is staffed by personnel from the Samoa Police Service, Immigration Division of the Ministry of the Prime Minister and Division of Customs. The TCU is responsible for intelligence gathering and analysis and investigating transnational crimes, including money laundering, terrorist financing and the smuggling of narcotics and people.

The Act requires financial institutions to record new business transactions exceeding WST 30,000 (approximately $10,000), to retain records for a minimum of seven years, and to identify all parties to the transactions. This threshold reporting system could expose the financial institutions to potential abuse. Nevertheless, Section 43(a) of the Money Laundering Prevention Regulations 2002 requires financial institutions to identify their customers when "there are reasonable grounds for believing that the one-off transaction is linked to one or more other one-off transactions and the total amount to be paid by or to the applicant for business in respect to all of the linked transactions is WST 30,000, or the equivalent in another currency." Moreover, proposed amendments to the Act would delete the threshold reporting system, leaving it open for all financial institutions to report any amount or transaction that purports to involve money laundering.

Section 12 of the Act establishes that all financial institutions have an obligation under this law to "develop and establish internal policies, procedures and controls to combat money laundering, and develop audit functions in order to evaluate such policies, procedures and controls." The Regulations and Guidelines that have been developed remedy the lack of specificity in the Act about the obligation of financial institutions to establish the identity of the beneficial owner of an account managed by an intermediary. Specifically, Section 12.06 of the Money Laundering Prevention Guidelines for the Financial Sector provides that "…If funds to be deposited or invested are being supplied by or on behalf of a third party, the identity of the third party (i.e., the underlying beneficiary) should also be established and verified." The law requires individuals to report to the MLPA if they are carrying with

them WST 10,000 (approximately $3,300) or more, in cash or negotiable instruments, upon entering or leaving Samoa.

The Act removes secrecy protections and prohibitions on the disclosure of relevant information. Moreover, it provides protection from both civil and criminal liability for disclosures related to potential money laundering offenses to the competent authority.

The Central Bank of Samoa, the Office of the Registrar of International and Foreign Companies, and the MLPA regulate the financial system. There are four locally incorporated commercial banks, supervised by the Central Bank. The Office of the Registrar of International and Foreign Companies has responsibility for regulation and administration of the offshore sector. There are no casinos, but two local lotteries are in operation.

Samoa is an offshore financial center, with eight offshore banks licensed. For entities registered or licensed under the various Offshore Finance Centre Acts, there are no currency or exchange controls or regulations, and no foreign exchange levies payable on foreign currency transactions. No income tax or other duties, nor any other direct or indirect tax or stamp duty is payable by registered/licensed entities. In addition to the eight offshore banks, Samoa currently has 13,465 international business corporations (IBCs), three international insurance companies, six trustee companies, and 175 international trusts. Section 16 of the Offshore Banking Act stipulates prohibition for any person from applying to be a director, manager, or officer of an offshore bank who has been sentenced for an offense involving dishonesty. The prohibition is also reflected in the application forms and Personal Questionnaire that are completed by prospective applicants that detail the licensing requirements for offshore banks. The application forms list the required supporting documentation for proposed directors of a bank. These include references from a lawyer, accountant, and a bank, police clearances, curriculum vitae, certified copies of passports and personal statements of assets and liabilities (if also a beneficial owner). The Inspector of Offshore Banks must be satisfied with all supporting documentation that a proposed director is fit and proper in terms of his integrity, competence and solvency.

International cooperation can occur only if Samoa has entered into a mutual cooperation agreement with the requesting nation. Under the Act, the MLPA has no powers to exchange information with overseas counterparts. All cooperation under the MLPA is through the Attorney General's Office, which is the Competent Authority under the Act for receiving and implementing. However, according to a 2003 Samoa Report to the UN Counter-Terrorism Committee, Samoa is reviewing the legal framework for the effective operation of the MLPA in order to further strengthen domestic and international information exchange. In addition, the Office of the Attorney General, in conjunction with the Central Bank, the Ministry of Police and the Division of Customs of the Ministry for Revenue, is currently preparing amendments to the Money Laundering Prevention Act of 2000 for purposes of strengthening and complementing legislation that is being drafted or developed, including the Proceeds of Crime Bill, the Mutual Assistance in Criminal Matters Bill, and the Extradition Amendment Bill. Samoa is a party to the UN International Convention for the Suppression of the Financing of Terrorism. In 2002, Samoa enacted the Prevention and Suppression of Terrorism Act. The Act defines and criminalizes terrorist offenses, including offenses dealing specifically with the financing of terrorist activities. The combined effect of the Money Laundering Prevention Act of 2000 and the Prevention and Suppression of Terrorism Act of 2002 is to make it an offense for any person to provide assistance to a criminal to obtain, conceal, retain or invest funds or to finance or facilitate the financing of terrorism.

Samoa is a member of the Asia/Pacific Group on Money Laundering and the Pacific Island Forum. Samoa hosted the annual plenary of the Pacific Island Forum in August 2004. Samoa has not signed the 1988 UN Drug Convention. Nor has it signed the UN Convention against Transnational Organized Crime.

Since the passage of the Money Laundering Prevention Act in June 2000, Samoa has continued to strengthen its anti-money laundering regime and has issued regulations and guidelines to financial institutions so that they have a clear understanding of their obligations under the Act. Particular emphasis is directed toward regulation of the offshore financial sector, principally the establishment of due diligence procedures for owners and directors of banks and the elimination of anonymous accounts for onshore and offshore banks. The GOS is strengthening relevant legislation to identify the beneficial owners of IBCs to help ensure that criminals do not use them for money laundering or other financial crimes. Samoa is in the process of adopting amended and additional legislation to allow for international cooperation and information sharing.

The inability of the Money Laundering Prevention Authority simply to exchange information on an administrative level is a material weakness of the current system and is an impediment to international cooperation. To rectify that situation, the Government of Samoa should enact legislation to provide the Money Laundering Prevention Authority with the legal authority to share information with foreign analogs. Samoa should also accede to the 1988 UN Drug Convention and become a party to the UN Convention against Transnational Organized Crime.

San Marino

San Marino is a small, landlocked, independent republic located on the eastern side of the Italian peninsula. It is the third smallest country in Europe after the Holy See and Monaco. San Marino was founded in 301 and claims to be the oldest republic in the world. Its policies and social trends closely track those of Italy. The financial sector is a large component of the republic's small economy. The Government of San Marino (GOSM) passed anti-money laundering legislation in 1998. In June 2003 the GOSM approved a law that provides functional integration between the Office of Banking Supervision and the Central Bank, thus strengthening the supervisory system and its efforts to counter money laundering and terrorist financing.

Also in 2003, the Office of Banking Supervision issued Circular No. 33 addressed to banks and financial companies that obligates the collection of customers' personal data and their business/professional activity. The GOSM has also approved a law on the "Provisions of Anti-Terrorism, Anti-Money Laundering and Anti-Insider Trading," which became effective on February 26, 2004. The legislation criminalizes terrorism; introduces rules supplementing the Anti-Money Laundering Law of 1998 by incorporating modifications recommended by the Financial Action Task Force (FATF) and the Council of Europe; provides for the freezing of financial assets or property; allows special investigative techniques; and contains rules on insider trading. In April 2003, San Marino had its second round of mutual evaluations by MONEYVAL.

The GOSM is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It signed, but has not yet become a party to, the UN Convention against Transnational Organized Crime. The San Marino Financial Intelligence Unit (the Department of Treasury inspection office) will adhere to the Egmont Group at its next meeting in April 2005.

The Government of San Marino should continue its efforts to thwart money laundering and terrorist financing and should ratify the UN Convention against Transnational Organized Crime.

Sao Tome and Principe

Sao Tome, which has a small economy and several commercial banks, is not a regional financial center.

Sao Tome is a party to the 1988 UN Drug Convention but not to the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Crime. It has not criminalized either money laundering or terrorist financing and has no laws allowing the government to freeze assets related to those activities. The need for it to enact and implement such legislation has been heightened by the successful conclusion of an agreement with Nigeria that will bring substantial oil revenues to the country. Sao Tome should consider devoting a portion of that revenue to develop a comprehensive anti-money laundering/counterterrorist regime that comports with international standards.

The Government of Sao Tome should criminalize money laundering and terrorist financing. Sao Tome should also enact legislation allowing the government to freeze assets related to money laundering and terrorist financing. Sao Tome should become a party to both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Saudi Arabia

Saudi Arabia is a growing financial center in the Gulf Region of the Middle East. There is little known money laundering in Saudi Arabia related to traditional predicate offenses. All ten commercial banks in Saudi Arabia operate as standard "western-style" financial institutions and all banks operate under the supervision of the Saudi Arabian Monetary Authority (SAMA). Saudi Arabia is not an offshore financial center. There are no free zones for manufacturing, although there are bonded transit areas for the transshipment of goods not entering the country. The money laundering and terrorist financing that does occur are not primarily related to narcotics proceeds in Saudi Arabia. There was no significant increase in financial crimes during 2004, and any market in smuggled goods does not appear to be related to the narcotics trade.

Saudi donors and unregulated charities have been a major source of financing to extremist and terrorist groups over the past 25 years. However, The Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission") found no evidence that either the Saudi Government, as an institution, or senior Saudi officials individually, funded al-Qaida. Following the al-Qaida bombings in Riyadh on May 12, 2003, the Government of Saudi Arabia has taken significant steps to help counteract terrorist financing.

In 2003, Saudi Arabia approved a new anti-money laundering law that for the first time contains criminal penalties for money laundering and terrorist financing. The law bans conducting commercial or financial transactions with persons or entities using pseudonyms or acting anonymously; requires financial institutions to maintain records of transactions for a minimum of ten years and adopt precautionary measures to uncover and prevent money laundering operations; requires banks and financial institutions to report suspicious transactions; authorizes government prosecutors to investigate money laundering and terrorist financing; and allows for the exchange of information and judicial actions against money laundering operations with countries with which Saudi Arabia has official agreements.

SAMA guidelines correspond to the FATF's Forty Recommendations. On May 27, 2003 SAMA issued updated anti-money laundering and counterterrorist finance guidelines for the Saudi banking system. The guidelines require that banks have mechanisms to monitor all types of "Specially Designated Nationals" as listed by SAMA; that fund transfer systems be capable of detecting specially designated nationals; that SAMA circulars on opening accounts and dealing with charity and donation collection be strictly adhered to; and that the banks be able to provide the remitter's identifying information for all outgoing transfers. The new guidelines also require banks to use software to profile customers to detect unusual transaction patterns; establish a monitoring threshold of SR 100,000; and develop internal control systems and compliance systems. SAMA also issued new "know your

customer" guidelines, requiring banks to freeze accounts of customers who do not provide updated account information. Saudi law prohibits non-resident individuals or corporations from opening bank accounts in Saudi Arabia without the specific authorization of the SAMA. There are no bank secrecy laws that prevent financial institutions from reporting client and ownership information to bank supervisors and law enforcement authorities. The Saudi media reported that during 2004, Saudi banks froze more than 250,000 accounts for non-compliance with anti-money laundering and terrorist finance laws. Funds are frozen on the basis of a request submitted from the Minister of Interior or the Minister of Foreign Affairs to the Minister of Finance and National Economy.

The Saudi Arabian Government (SAG) has established an anti-money laundering unit in SAMA and has required Saudi banks to have their own anti-money laundering units with specialized staff to work with SAMA and law enforcement authorities. The SAG has begun to staff a Financial Intelligence Unit (FIU) in the Security and Drug Control Department of the Ministry of the Interior. All banks are also required to report any suspicious transactions to the FIU. When fully operational, the Saudi FIU will collect and analyze suspicious transaction reports and other available information and decide to make referrals the Mabahith or other entities for action. It will also coordinate its activities with SAMA's anti-money laundering unit. The FIU will be staffed by officers from the Mabahith, SAMA, the Ministry of Commerce, and the Ministry of Interior's Bureau of Investigation and Prosecution. The SAG provides anti-money laundering training for bank employees, prosecutors, judges, customs officers and other government officials.

Hawala transactions outside banks and licensed moneychangers are illegal in Saudi Arabia. Reportedly, some money laundering cases that SAMA has investigated in the past decade involved the hawala system. In order to help counteract the appeal of hawala, particularly to many of the approximately six million expatriates living in Saudi Arabia, Saudi banks have taken the initiative and created fast, efficient, high quality, and cost-effective fund transfer systems that have proven capable of attracting customers accustomed to using hawalas. An important advantage for the authorities in combating potential money laundering and terrorist financing in this system is that the senders and recipients of fund transfers through this formal financial sector are clearly identified.

Contributions to charities in Saudi Arabia are usually Zakat, which is an Islamic religious duty with specified humanitarian purposes. However, over the past decade, according to a 2002 report to the United Nations Security Council, al-Qaida and other jihadist organizations collected between $300 and $500 million and the majority of those funds originated from Saudi charities and private donors. The 9/11 Commission Report noted that the SAG failed to supervise adequately Islamic charities in the country. To help address this problem, in 2002 Saudi Arabia announced its intention to establish a commission to oversee Saudi charities with foreign operations. In 2004, the SAG issued guidelines for the Commission for Relief and Charitable Work Abroad. As required by regulations in effect for over 20 years, domestic charities in Saudi Arabia are licensed, registered, audited, and supervised by the Ministry of Social Affairs. The Ministry has engaged outside accounting firms to perform annual audits of charities' books and has established an electronic database for tracking the operations of the charities they oversee. New banking rules implemented in 2003 that apply to charities include stipulations that accounts can only be opened in Saudi Riyals; there are enhanced customer identification requirements; there is one main consolidated account for each charity; there are no cash disbursements—payments may be made only by checks payable to the first beneficiary and deposited in a Saudi bank; the use of ATM and credit cards for charitable purposes will not be permitted; there will be no transfers outside of Saudi Arabia. It is unclear, however, whether such regulations apply to international charities.

Saudi Arabia participates in the activities of the Financial Action Task Force (FATF) through its membership in the Gulf Cooperation Council (GCC). In July 2004, reporting on the results of a mutual evaluation conducted in September 2003, the FATF concluded that the framework of Saudi Arabia's anti-money laundering regime met the general obligations of the FATF recommendations for

combating money laundering and financing of terrorism, but noted the need to implement these new laws and regulations.

Saudi Arabia also supported the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004; the SAG was one of the original charter signatories. The MENAFATF is a FATF-style regional body. The creation of the MENAFATF will be a critical element in the region's efforts to expedite the adoption and implementation of international anti-money laundering and counterterrorist financing standards.

Saudi Arabia is working to implement the UN Security Council Resolutions on terrorist financing. SAMA circulates to all financial institutions under its supervision the UNSCR 1267 Sanctions Committee's consolidated list. In January 2004, Saudi Arabia and the United States made a joint request to the UNSCR 1267 Sanctions Committee to designate the Kenya, Pakistan, Tanzania and Indonesia branches of the al Haramain Islamic Foundation as a supporter of terrorism. In June 2004, Saudi Arabia announced that it had completely dissolved the al Haramain Islamic Foundation. The SAG and U.S. worked bilaterally to investigate terrorist financing. Among other activities, in response to specific requests from the U.S., the SAG investigated financial activities for 41 individuals and found that none had financial activities in the Kingdom.

Saudi Arabia has signed but is not yet a party to the UN International Convention for the Suppression of the Financing of Terrorism. It ratified the UN Convention against Transnational Organized Crime on January 18, 2005.

The Government of Saudi Arabia should move rapidly to monitor and enforce the new anti-money laundering and terrorist finance laws, regulations and guidelines. Saudi Arabia can demonstrate its commitment to effective implementation by providing adequate budgets, equipment, and staffing for the FIU and the High Commission for Charities. As in many countries in the region, there is still an over-reliance on suspicious transaction reporting to generate money laundering investigations. Saudi Arabia's unwillingness to publicly disseminate statistics regarding money laundering prosecutions impedes the evaluation and design of enhancements to the judicial aspects of its AML system. Law enforcement agencies should take the initiative and proactively generate leads and investigations, and be able to follow the financial trails wherever they lead. Saudi Arabia should demonstrate its willingness to hold elites accountable. Charities identified with the elites must also be examined and rules enforced. Regarding the misuse of charities, loopholes remain including the ability of a group or individual previously affiliated with suspect charitable organizations to simply cease referring to itself as a charity, as well as with the status of international charities. Donations in the form of gold and other gifts need to be scrutinized. Saudi Arabia should take affirmative steps to close loopholes. It should become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Senegal

Senegal's banking system and formal and informal money-exchange systems are vulnerable to the laundering of proceeds from corruption, narcotics-trafficking, illegal gems and arms-trafficking, and trafficking in persons, all of which are prevalent in West Africa. A building boom in Dakar despite the relative scarcity of credit suggests that an increasing amount of funds with an uncertain provenance is available for property speculation. Approximately 15 foreign banks, including several French and African banks, have branches in Senegal. Senegal's larger financial institutions function alongside a thriving micro-credit sector and numerous non-traditional financial businesses handling remittances from overseas Senegalese in France, Italy, Spain and the United States. Senegal is not obviously linked to any offshore financial centers. Given the small customer pool, the number of casinos in Senegal (reportedly over 15) is striking.

Article 102 of Senegal's 1997 Drug Code criminalizes narcotics-related money laundering as a misdemeanor punishable by up to 10 years in prison. The Drug Code requires banks to report suspicious transactions believed to be linked to narcotics-trafficking and to keep records between one and ten years, depending on the type of record. The law authorizes the seizure of assets related to narcotics-trafficking. The last money laundering prosecution under this law was in 1999.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Action Group against Money Laundering (GIABA), based in Dakar, Senegal. GIABA recently hosted a self-evaluation exercise on anti-money laundering capabilities in conjunction with the International Monetary Fund and ECOWAS member states. A Senegalese magistrate is the acting head of GIABA. The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency, which is also linked to the euro. All bank deposits over approximately $7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information.

Senegal was the first WAEMU country to pass WAEMU-harmonized legislation establishing a Uniform Law on Money Laundering (the Uniform Law), approved by the National Assembly in October 2003. Previously, criminal prosecution of money laundering had been tied to Senegal's Drug Code. The new legislation makes money laundering/terrorist financing a crime in itself, separate from the criminal origins of the money. Banks and other financial institutions, including charitable and nonprofit entities, are required to know, record and report the identity of customers engaging in significant transactions, meaning those involving at least CFA 5,000,000 (approximately $10,000). The Uniform Law requires financial institutions to preserve records for at least ten years. Under the provisions of banking regulations, banks and financial institutions must provide, upon request from the BCEAO or Senegal's Banking Commission, any information relating to the list of accounts opened on behalf of suspected launderers, suspected terrorists, and/or suspected terrorist organizations and must notify the BCEAO of any request or the opening of an account relating to such person or organization. Banking secrecy cannot be invoked to protect suspicious clients.

The Uniform Law also mandates the establishment of a National Office for Financial Information Process (CENTIF), a Financial Intelligence Unit (FIU), that will work with banks and other financial institutions to establish a suspicious transaction reporting system and capacity for evaluating questionable transactions. All financial institutions, businesses, and professionals under the scope of the Uniform Law will be required to report suspicious transactions. Presently, foreign-owned banks in Senegal normally report questionable transactions to their home offices (usually Paris) for vetting. Senegal's FIU will have the legal authority to conduct criminal investigations. The CENTIF will have the authority to share information with other FIUs within the WAEMU as well as with the FIUs of non-WAEMU countries. The Government of Senegal (GOS) has yet to issue a decree directing ministries to second appropriate staff to the CENTIF.

Special units from police forces and "gendarmerie" can be created to investigate and prosecute cases against money laundering. Official statistics regarding the prosecution of financial crimes are unavailable. There have been no arrests and/or prosecutions for money laundering or terrorist financing since January 1, 2004.

The Dakar Industrial Free Trade Zone (ZFID) was established in 1974 to encourage foreign investors to set up intensive export-oriented companies. Its enabling statute has been extended until 2016, but only for companies already established within the zone. The ZFID is largely inactive with few companies present, although a U.S. pharmaceutical company has a manufacturing plant in the ZFID. Police forces and customs officials monitor activities in the free zone. Companies and individuals using the zone are identified and registered.

Terrorism financing is covered in the long-existing "Code Against Acts of Terrorism" which criminalizes the financing of terrorism as required by UNSCR 1373. This provision was incorporated in the Uniform Law. Modifications to the "Code Against Acts of Terrorism" are included in legislation on counterterrorism financing currently under consideration by the National Assembly. The UN 1267 Sanctions Committee consolidated list is circulated both by the GOS and by the BCEAO to commercial financial institutions. To date, no assets relating to terrorist entities have been identified. The WAEMU Council of Ministers issued a directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations designated by the UN 1267 Sanctions Committee. A pending law on financing terrorism would meet the stipulations of this directive

Senegalese authorities acknowledge the existence and use of indigenous alternative remittance systems that bypass, in whole or part, financial institutions. The authorities have established private foreign exchange bureaus to regulate the informal financial sector. No regulation currently governs remittances from the sale of gold and precious stones. There is no requirement to report cross-border currency transactions.

Senegal's Drug Code and Uniform Law include a system to freeze, seize and forfeit narcotics-related assets as well as assets derived from other serious crimes, such as money laundering. It also includes the seizure of instruments of crime such as conveyances used to transport narcotics, or property such as bank accounts, legitimate businesses or real estate. Substitute assets can be seized if relationship to the crime is proven. The Uniform Law allows for both civil and criminal forfeiture, and gives full power and resources to police to trace and seize assets. Financial institutions can freeze assets upon requests from officials from the Ministries of Interior and/or Justice, or from the BCEAO. The Ministry of Justice is responsible for the confiscation of frozen assets. Assets can be frozen for up to 20 years. The sharing of seized narcotics assets with other governments would be the result of case-by-case negotiations.

Senegal has entered into agreements with Tunisia, Morocco and France regarding mutual assistance in criminal matters. With the Uniform Law now in force in most WAEMU countries and with the establishment of GIABA, FIUs in WAEMU and ECOWAS countries will cooperate, exchange and share information. In general, the GOS has demonstrated its commitment and willingness to cooperate with the United States law enforcement agencies, although no formal mechanism exists. In the past the GOS has worked with INTERPOL and Spanish and Italian authorities on international anticrime operations.

Senegal is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Senegal also is a signatory to the African Union Convention on Terrorism Finance.

The Government of Senegal should continue to work with its counterparts in the Intergovernmental Action Group against Money Laundering (GIABA) and its partners in WAEMU to establish a comprehensive anti-money laundering regime in the region. Senegal should act timely to make its new Financial Intelligence Unit (FIU) a fully functioning organization, with adequate staffing and resources. Senegal should become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Serbia and Montenegro

At the crossroads of Europe and on the highway known as the "Balkan route," narcotics-trafficking; smuggling of persons, drugs, weapons and pirated goods; money laundering; and other criminal activities continue in Serbia and Montenegro (SAM, formerly the Federal Republic of Yugoslavia (FRY)). Serbia and Montenegro is located in Southeastern Europe (the Balkans), bordering the Adriatic Sea, between Albania and Bosnia and Herzegovina. SAM is a state union consisting of two

republics, the Republic of Serbia and the Republic of Montenegro. In the Republic of Serbia are two nominally autonomous provinces, Kosovo and Vojvodina; a United Nations Administration Mission (UNMIK) has administered Kosovo since 1999. The state union has a population of approximately 10.7 million, of which about 8 million live in Serbia, about 600,000 in Montenegro and slightly over two million in Kosovo. Each republic has a separate government and parliament. However, there is also a parliament on the federal level.

The country has a significant black market for smuggled goods. However, income from narcotics-trafficking is typically not used to support this black market. Rather, it is more typical for drug money to be laundered in the real estate market, which is one of the most popular ways to legalize criminal proceeds in SAM. Tax evasion and trade-based money laundering, in the form of over-and under-invoicing, are also another of the common methods used to launder money. According to government officials, the majority of criminal proceeds from narcotics-trafficking laundered in SAM are derived from illegal activities of the Kosovar "Narco-Mafia." Serbian officials also estimate that up to half of all financial transactions in SAM may be connected in some way to money laundering. Although SAM has made important progress in its fight against corruption and financial crimes by criminalizing money laundering and establishing financial intelligence units, substantial work remains to be done.

Neither republic has identified any activities relating to the financing of terrorism. Montenegro has criminalized the financing of terrorism and Serbia is in the process of amending its criminal code to address this issue.

State Union. In March 2002, the leadership of the FRY, Serbia, and Montenegro signed the Belgrade Agreement on restructuring the relationship between the two republics. On February 4, 2003, the FRY parliament voted to adopt a new Constitutional Charter that established the state union of "Serbia and Montenegro." Under this state union structure, most governmental authority previously addressed by federal Yugoslav authorities devolved to the individual republics. As a result, responsibility for the laws and institutions determining policies and legislation has shifted. Consequently, both the Republic of Serbia (Serbia) and the smaller Republic of Montenegro (Montenegro) have addressed money laundering and terrorism financing. However, each republic has done so separately in its own way. Banks in both republics have demonstrated remarkable tolerance for and compliance with the laws in their respective jurisdictions.

In 2001, the federal Yugoslav authorities prepared a national strategy to fight terrorism and established a national coordinating body. However, this body fell into abeyance when the FRY transformed into the state union in February 2003. Ratification of international Conventions and treaties currently lies at the State Union level. All relevant anti-money laundering/counterterrorist financing (AML/CTF) conventions have been ratified.

Serbia. The Yugoslav Federal Assembly adopted an Anti-Money Laundering Law (AML Law) in September 2001; it came into effect in July 2002. The AML Law defines money laundering to mean depositing, or introducing into the financial system in any other manner, money which has been acquired through illegal activity. This includes money derived from the gray market economy and from arms and narcotics-trafficking. Criminal penalties for money laundering violations range from six months' to eight years' imprisonment, while civil penalties range from 45,000 to 450,000 dinars ($650 to $6,500) per offense.

On July 18, 2003, Serbia passed a new law codifying the powers of the National Bank, decreasing its independence and establishing parliamentary control over its operations. The Bank has adopted AML supervision guidelines and is examining banks for compliance with the existing AML reporting requirements. One area of concern is the large number of currency exchanges located throughout Serbia that are reportedly structuring transactions for clients who want to avoid the reporting requirements. These currency exchanges are regulated by the National Bank, but an effective supervisory scheme to address this problem has not yet been put into place.

Entities subject to reporting requirements include commercial and savings banks and other financial credit institutions, the postal savings bank, the post office, commercial enterprises, all government entities, the National Bank of Yugoslavia and its clearing and payments department, foreign exchange bureaus, casinos, pawnshops, stock exchanges, and national lottery organizers. Covered entities are required to identify persons opening an account or if they are "establishing any other kind of lasting business cooperation with the client," and to report on every cash transaction exceeding 10,000 euros or 600,000 dinars, as well as any suspicious transaction. Similar reporting thresholds apply to insurance policies and cross-border currency transactions. The AML Law also provides for record keeping.

In March 2002, a Financial Intelligence Unit (FIU), the Administration for the Prevention of Money Laundering (FCPML), was established as an independent federal body by governmental decree; it became operational on July 1, 2002. At its founding, both the money laundering law and the FIU were operational at the federal level, with all laws applicable to both Serbia and Montenegro. On February 4, 2003, pursuant to the dissolution of the centralized federal state into the two republic entities, and pursuant to Article 13 of the Constitutional Charter and Implementation Law, the FCPML, up until then a federal FIU, became the FIU for the Serbian Republic. In July 2003, FCPML became a member of the Egmont Group, and has since begun active participation in information exchange with counterpart FIUs.

Despite some positive first steps, the Serbian FIU remains largely ineffective in addressing Serbia's money laundering problems, because of both inadequate funding and a lack of sufficient compliance mechanisms. Other than the memorandum of understanding the FIU signed with the National Bank of Serbia in 2004, the FIU has not formalized relationships with enforcement officials and other government or private institutions for cooperation and exchange of information. For 2003, the FIU reported the receipt of over 60,000 reports and the referral of 162 suspicious cases to law enforcement. However, the FIU has not issued indicators of suspicious activity for all sectors encompassed by the existing law. In addition, the FIU has no inspection authority and has not provided or sponsored adequate training programs for non-bank financial institutions. As a result, the accurate reporting of suspicious transactions is questionable. To cite one example, one of the largest banks in Serbia reported conducting over 15,000 cash transactions in one year. But this same bank had filed less than 10 suspicious transaction reports (STRs) during that same year. Serbia also has not yet obtained a conviction for money laundering.

A new draft money laundering law conforming with international standards, extending the list of covered entities to include attorneys and accountants, and harmonizing legislation with all European Union (EU) Directives, was under review and submitted to Parliament in the beginning of October 2003. The new law was approved by all of the relevant authorities, but then a parliamentary crisis broke out, and the procedure was suspended. On December 28, 2003, Serbia held a parliamentary election that brought to power Prime Minister Kostunica's government. In the last year, however, Kostunica's administration has failed to approve this draft law. To date, the draft law is still in Parliament. Although the draft law is fairly comprehensive, it still has some shortcomings. It does not require suspicious transaction reporting by attorneys (a FATF and EU recommendation), and it does not establish the FIU as a repository for information relating to the suspicions of terrorist financing, which is now a requirement for all Egmont members.

Serbia has no terrorist financing law consistent with the standards contained in international conventions, and its legislative and institutional framework for combating terrorist financing remains weak. Draft legislation is pending. According to the Serbian Criminal Code, business licenses of legal or natural persons may be revoked and business activities banned if the subject is found guilty of criminal activities, including narcotics-trafficking or terrorist financing. But, despite this fact, Serbia is constrained with regard to international assistance in investigating terrorist financing. This is because Serbia's police may not make use of the Mutual Legal Assistance Treaty (MLAT) process in terrorist

financing cases, due to the fact that under Serbian law, use of the MLAT process is restricted to crimes with penal sentences equal to or exceeding ten years (although the draft law reduces the requirement to four years). Under the current law, the maximum term for money laundering or terrorist financing is eight years. As a result, Serbia forfeits any available international assistance. Also presenting another obstacle is Serbia's Criminal Procedure Code, under which an MLAT request for assistance in investigating terrorist activities requires the approval of an investigative judge. However, investigative judges, for a number of reasons, often do not grant these requests. Serbia is currently in the process of amending its Criminal Procedure Code to bring it into conformity with Council of Europe standards.

The AML Law establishes special procedures for tracking funds related to terrorist financing. The Serbian FCPML is the authority charged with enforcing the UN terrorism sanction lists. Although it routinely checks for suspect accounts, it has found no evidence of terrorism financing within the banking system and no evidence of the usage of alternative remittance systems. The Department for Combating Organized Crime (UBPOK), in the Ministry of Interior, is the law enforcement body responsible for countering terrorism. UBPOK cooperates and shares information with its counterpart agencies in all of the countries bordering SAM.

Serbia has no asset seizure or forfeiture law. Actual asset seizures can only be carried out by court order.

The government has no encompassing AML/CFT strategy, and has failed to enact anti-money laundering legislation that is in full compliance with international standards. It also has not created a bureaucratic and legal framework that empowers the FIU to carry out its core mission. Terrorist financing laws have not been enacted and the ability to seize or freeze assets relating to terrorist financing, except after a criminal conviction using other statutes, does not exist under current law. As a result of the absence of a comprehensive anti-money laundering regime, no accurate statistical information or feedback regarding cases forwarded to local authorities or prosecutors is available to assess results or ensure transparency. Finally, the Finance Ministry has yet to grant the FIU a line item budget, so that it can effectively plan activities and operations.

Montenegro. It is important to note that considering its past record on AML issues, Montenegro has positively and significantly changed its stance on money laundering. In 1996, in an effort to lure needed funds, Montenegro proclaimed itself an offshore area and allowed financial intermediaries to do business-without controls-for a percentage of the profit. Hundreds of millions of dollars worth of money passed through Montenegrin offshore accounts annually. It is speculated that much of the money came from criminal activity.

In August 2002, the Central Bank of Montenegro (CBCG) issued a decree that requires banks and other financial institutions to report suspicious transactions, establish anti-money laundering control programs, and train their employees on money laundering matters. Also, in response to the overwhelming growth of its offshore sector during the past decade, the Montenegrin government mandated that all offshore banks must re-register, post a one million Eurobond or fee, and reestablish themselves as regular banks. To date, since none of the offshore entities has complied with this mandate, the Central Bank has deemed all offshore banks to be dissolved. The Finance Ministry has not released complete information about the actual disposition of the 400 offshore entities whose names they turned over to CBCG.

Money laundering is criminalized in a new Criminal Code, which was amended in June 2003 in order to enable the government to confiscate money and property involved in criminal activity. Additionally, according to the Code, business licenses of legal or natural persons may be revoked and business activities banned if the subject is found guilty of criminal activities, including narcotics-trafficking or terrorist financing. In April 2004, Montenegro further amended its Criminal Procedure Code to bring it into conformity with the standards of the Council of Europe.

Montenegro passed anti-money laundering legislation on September 24, 2003. The new law obliges banks, post offices, state entities, casinos, lotteries and betting houses, insurance companies, jewelers, travel agencies, auto and boat dealers, and stock exchange entities to file reports on all transactions exceeding 15,000 euros, as well as on any related transactions that aggregate 15,000 euros or more, even if each particular transaction does not exceed the threshold. Financial institutions are also obliged to report suspicious transactions, even if only a small amount of money is involved. Failure to report, according to the law, could result in fines up to 20,000 euros as well as sentences of up to 12 years. The new law establishes mandates for the collection and analysis of these reports by Montenegro's FIU, which also has the responsibility to disseminate these reports to the competent authorities for further action. The FIU is adequately staffed, but compliance mechanisms are as yet untested. The FIU, which has been fully operational since November 2003, is currently a candidate for Egmont membership in 2005.

Montenegro can seize and forfeit assets, but only in connection with a violation of another provision of the Criminal Code, generally money laundering, terrorism or terrorist finance. In September 2004, the Government of Montenegro seized over a million dollars in undeclared currency in connection with the arrest of two Chinese nationals attempting to enter Montenegro.

Amendments to Montenegro's laws on terrorism and terrorist financing were initiated in November 2004 and are expected to be adopted in January 2005. These amendments are designed to bring Montenegrin law into conformance with international standards. Responsibility for the detection and prevention of terrorist financing was transferred in 2004 from the CBCG to the FIU. The FIU promptly informs banks and other financial institutions of additions and changes to the lists of individuals and entities included on the consolidated list of the UNSCR 1267 Sanctions Committee. No terrorist financing has been detected within Montenegro.

Kosovo. Since 1999, the United Nations Interim Administration in Kosovo (UNMIK) has governed Kosovo. Therefore, it no longer falls within the jurisdiction of either Serbia or Montenegro. Recognizing that Kosovo could become a haven for money laundering as its neighbors tighten their anti-money laundering regimes, UNMIK determined that Kosovo must also adopt a strict approach to the fight against money laundering. Thus, on February 5, 2004, UNMIK issued Regulation 2004/2, "On the Deterrence of Money Laundering and Related Offenses." The Regulation became effective on March 1, 2004, with delayed effective dates for certain provisions within the regulation.

The Regulation defines the crime of money laundering as the knowing possession, acquisition, use, transfer or conversion of the proceeds of crime. Proceeds of crime is defined as any property derived from any criminal offense punishable by a year or more of imprisonment under the applicable law in Kosovo or under the law of the jurisdiction in which the criminal offense was committed. The crime of money laundering is punishable by up to 10 ten years confinement and a fine up to three times the value of the property laundered. The Regulation provides for both civil and criminal forfeiture of the proceeds of the money laundering or any property which facilitated the money laundering or predicate offense.

The Regulation also obliges banks, non-bank financial institutions (money remitters, securities dealers/brokers, insurance companies, foreign exchange businesses, issuers and sellers of traveler's checks, credit cards, money orders, bank checks, and electronic money), and covered professionals (attorneys, accountants, and licensed auditors) to identify their clients and conduct ongoing due diligence, report suspicious transactions and currency transactions greater than 10,000 euros to the KFIC, maintain records for five years, and maintain an anti-money laundering compliance program which includes the appointment of a compliance officer and mandates training of employees. The Regulation criminalizes tipping off and failure to file either the suspicious transaction report or the currency transaction report. The Regulation also mandates the reporting of the cross-border transportation of monetary instruments exceeding 10,000 euros.

The Regulation creates the Financial Intelligence Centre (KFIC) within the Police and Justice Pillar. The KFIC will receive and analyze the reports received from the various entities, create and maintain a database of all information collected, issue administrative directives, and exchange information upon requests with like foreign entities. The KFIC is functional but in its infancy.

The Regulation limits the receipt by non-governmental organizations (NGOs) of currency contributions to 1000 euros per day from a single source. NGOs cannot distribute greater than 5,000 euros to any single recipient in a single day. NGOs must maintain accounts that document all income and disbursements. The accounts shall identify income by source, amount, and manner of payment, such as currency or payment order, and identify disbursements by recipient, intended use of funds, and manner of payment. NGOs must maintain records for five years, report suspicious transactions to the KFIC and file annual reports.

The Regulation also provides for the widest possible cooperation with foreign jurisdictions with respect to information exchange, investigations and court proceedings in relation to temporary measures for securing property and orders for confiscation relating to instrumentalities of money laundering and proceeds of crime, and for purposes of prosecution of the perpetrators of money laundering and terrorist activity.

SAM has no laws governing its cooperation with other governments, related to narcotics, terrorism, or terrorist financing. Cooperation is instead based on participation in Interpol, bilateral cooperation agreements, and agreements concerning international legal assistance. There are no laws at all governing the sharing of confiscated assets with other countries, nor is any legislation under consideration; SAM may at this time enter into bilateral agreements for this purpose.

Serbia and Montenegro has a legal assistance arrangement with the United States, governed by the 1901 Convention on Extradition of Offenders. SAM has signed 34 bilateral agreements on mutual legal assistance with 26 countries: Albania, Algeria, Austria, Belgium, Bulgaria, the Czech Republic, Denmark, France, Greece, The Netherlands, Croatia, Iraq, Italy, Cyprus, Germany, Poland, Romania, Hungary, Mongolia, Russian Federation, Slovakia, Spain, Switzerland, Turkey, the United Kingdom, and the United States. These agreements authorize extradition of suspected terrorists. Both SAM and its constituent republics cooperate with their counterparts and neighbors. In April 2003, SAM joined eight other participants in the South Eastern Europe Cooperation Process, in adopting a joint "Belgrade Declaration" to call for the continuation of regional cooperation and the intensification of the fight against terrorism and organized crime. SAM worked with Interpol to set up an office for that organization in Belgrade as part of its efforts to contribute to the fight against terrorism and other transnational crimes.

Serbia and Montenegro is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. On October 9, 2003, SAM ratified the Council of Europe's Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. SAM has ratified eight of the 12 UN Conventions or Protocols dealing with terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism, although the domestic implementation procedures do not provide the framework for full application in either republic. In December 2003, SAM signed, but has not yet ratified, the UN Convention against Corruption. As a new member of the Council of Europe, SAM is a full and active member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), and underwent a first-round evaluation by a team from that Committee in October 2003.

Serbia should expand its anti-money laundering legislation to include all serious crimes and to provide for suspicious transaction reporting requirements for intermediaries. Montenegro should enact legislation expanding its anti-money laundering regime, including suspicious transaction reporting requirements, to non-bank financial institutions and intermediaries. Both republics should enact legislation to establish robust asset seizure and forfeiture regimes. Both Serbia and Montenegro should

ensure that sufficient resources are available for their FIUs and law enforcement agencies to work effectively and efficiently. Both should also continue to participate in international fora that offer training and technical assistance for police, customs, and judiciary officials involved with combating money laundering and terrorist financing. Serbia should criminalize all aspects of terrorist financing specifically and they should both implement a comprehensive framework to support an counterterrorism regime that comports with international standards. Kosovo should criminalize terrorist financing and implement its new anti-money laundering law.

Seychelles

Seychelles is a not a major financial center, but it does have a developed offshore financial sector, which makes the country vulnerable to money laundering.

The Government of Seychelles (GOS), in efforts to diversify its economy beyond tourism, has taken steps to develop an offshore financial sector to increase foreign exchange earnings. The GOS actively markets Seychelles as an offshore financial and business center that allows the registration of nonresident companies. There are currently over 4,800 registered international business companies (IBCs) in Seychelles that pay no taxes in Seychelles, and are not subject to foreign exchange controls. The Seychelles International Business Authority (SIBA), which acts as the central agency for the registration for IBCs, promotes the fact that IBCs need not file annual reports. The SIBA is part of the Ministry of International Trade, and also manages the Seychelles International Trade Zone.

In addition to IBCs, Seychelles permits offshore trusts (registered through a licensed trustee), offshore insurance companies, and offshore banking. Three offshore insurance companies have been licensed, but no mutual fund companies. The International Corporate Service Providers Act 2003, which is designed to regulate all the activities of the corporate service providers as well as the trustee service providers, entered into force in 2004. A major weakness of the Seychelles' offshore program is that it still permits the issuance of bearer shares, a feature that can facilitate money laundering by making it extremely difficult to identify the beneficial owners of an IBC. Seychelles officials stated in 2000 that they were reviewing the question of bearer shares and intended to outlaw them. In the interim, the GOS has indicated that it will not approve the issuance of any more bearer shares.

No offshore casinos or Internet gaming sites have yet been licensed; if they are, they will be subject to stringent legislation modeled on the Australian Internet Gaming Act. There are no cross-border currency reporting requirements, but the point of entry at Seychelles' international airport is under constant supervision by Customs and the Police, who search suspicious incoming or outgoing passengers.

In 1996, the GOS enacted the Anti-Money Laundering Act (AMLA), which criminalizes the laundering of funds from all serious crimes, requires financial institutions and individuals to report to the Central Bank transactions involving suspected cases of money laundering, and establishes safe harbor protection for individuals and institutions filing such reports. There are no bank secrecy laws in Seychelles. The AMLA imposes record keeping and customer identification requirements for financial institutions, and also provides for the forfeiture of the proceeds of crime.

Under the AMLA, money laundering controls are applied to non-banking financial institutions, including exchange houses, stock brokerages, and insurance agencies, but not to lawyers and accountants. No arrests and/or prosecutions have been made for money laundering and terrorist financing since January 1, 2003.

Under the AMLA, anyone who engages directly or indirectly in a transaction involving money or other property (or who receives, possesses, conceals, disposes of, or brings into Seychelles any money or property) associated with a crime, knowing or having reasonable grounds to know that the money or property is derived from an illegal activity, is guilty of money laundering. In addition, anyone who

aids, abets, procures, or conspires with another person to commit the crime, while knowing, or having reasonable grounds for knowing that the money was derived from an illegal activity, is likewise guilty of money laundering.

In 1998, the Central Bank of Seychelles issued a comprehensive set of guidance notes that further elucidated and strengthened the provisions of the AMLA. The Central Bank of the Seychelles receives and analyzes suspicious activity reports and disseminates them to the competent authorities. In November 2002 the Central Bank circulated to all local commercial banks a document on due diligence issued by the Basel Committee.

In December 2004, the Seychelles National Assembly enacted the Financial Institutions Bill 2004, which imposes more stringent rules on banking operations. The Bill, which was drafted in consultation with the International Monetary Fund, aims at ensuring greater transparency in financial transactions and regulating the financial activities of both domestic and offshore banks in line with international standards. One provisions of the new law requires that banks change their auditors every five years. Auditors must notify the Central Bank if they uncover criminal activity such as money laundering in the course of an audit.

In 2004, the GOS enacted the Prevention of Terrorism Bill 2004. The legislation recognizes the government's authority to identify, freeze, and seize terrorist finance-related assets. Currently the Mutual Assistance in Criminal Matters Act of 1995 empowers the Seychelles Central Authority to search and seize anything relevant to a proceeding or investigation relating to a criminal matter involving a serious offense under a written law of a requesting state.

The Prevention of Terrorism Bill strengthens the government's hand in this area. It specifically provides for the forfeiture of assets. Previously, the Seychelles authorities could work only with states that were members of the Commonwealth, or had a treaty for bilateral mutual legal assistance with the Seychelles regarding criminal matters. Under current legislation, assets used in the commission of a terrorist act can be seized, and legitimate businesses can be seized if used to launder drug money, support terrorist activity, or are otherwise related to criminal activities. Both civil and criminal forfeiture are allowed under current legislation. To date, no assets have been identified, frozen, or seized pertaining to terrorist financing, upon request of such a foreign state.

The transactions of charitable and non-profit entities are scrutinized by the authorities to prevent their misuse, and such systems as hawala are regulated.

The Government of Seychelles is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. The Seychelles is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The Seychelles has signed but not ratified the UN International Convention for the Suppression of the Financing of Terrorism. The Seychelles circulates to relevant authorities the updated lists of designations under Executive Order 13224. Seychelles should expand its anti-money laundering efforts by moving to immobilize bearer shares and requiring complete identification of beneficial owners of international business companies (IBCs). Seychelles should establish a financial intelligence unit to collect, analyze, and share financial data with foreign counterparts, in order to effectively combat money laundering and other financial crimes. Seychelles should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Seychelles should criminalize the financing of terrorism and actively participate in ESAAMLG.

Sierra Leone

Sierra Leone, which has a small commercial banking sector, is not a regional financial center. Loose oversight of financial institutions, weak regulations, rampant corruption, and a prevalent informal money-exchange system create an atmosphere conducive to money laundering. Given the importance

of the large diamond sector to the economy, the prevalence of money laundering in the diamond sectors of neighboring countries and the loose oversight of the financial sector, Sierra Leone's diamond sector is particularly vulnerable to money laundering. There is no available information for 2004. What follows is a repeat of the 2003.

There is no specific legislation concerning money laundering. However, the Ministry of Justice is in the process of developing such laws. Banks are required to record the identity of customers engaging in large currency transactions and to maintain adequate records necessary to reconstruct significant transactions in order to respond to government information requests. Banks are also required to report suspicious transactions, although they do not usually adhere to this requirement. Bank secrecy laws prevent the disclosure of client and ownership information except under court order.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Sierra Leone.

Sierra Leone is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Sierra Leone has signed, but has not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Sierra Leone should criminalize money laundering and terrorist financing, enforce existing financial laws and regulations, and provide legal authority for the seizure of criminal and terrorist assets.

Singapore

As a significant international financial and investment center, and in particular as a major offshore financial center, Singapore is attractive to potential launderers. Bank secrecy laws and the lack of routine currency reporting requirements make Singapore an attractive destination to foreign drug traffickers, other foreign criminals, and terrorist organizations and their supporters seeking to launder their money, and for flight capital. Money laundering occurs mainly in the offshore sector, but may also occur in the non-bank financial system, which includes large numbers of moneychangers and remittance agencies.

As a leading financial center in Southeast Asia, Singapore has been a key player in the regional effort to stop terrorist financing. Singapore has a sizeable offshore financial sector. In 2004, there were 111 commercial banks in Singapore, of which 47 were offshore banks, down slightly from 50 in December 2003. There are also 23 full banks and 36 wholesale banks in Singapore. All offshore banks are branches of foreign banks. Singapore does not permit shell banks, either in the domestic or offshore sectors. The Monetary Authority of Singapore (MAS), a semi-autonomous entity under the Ministry of Finance, serves as Singapore's Central Bank and financial sector regulator. There are no offshore trusts, although banks may open trust, nominee, and fiduciary accounts. All banks in Singapore, whether domestic or offshore, are subject to the same regulation, record keeping, and reporting requirements, including regarding money laundering and suspicious transactions.

In January 2005, as part of a draft revision of its overall anti-money laundering/counterfinancing of terrorism (AML/CFT) regulations for banks, the MAS proposed, subject to final approval, an amendment to its regulations proscribing banks from entering into, or continuing, correspondent banking relationships with shell banks—in line with the Revised Financial Action Task Force (FATF) Forty Recommendations adopted in June 2003. The new draft regulation also mandates originator information on cross-border wire transfers, in line with the FATF's Special Recommendation Seven on wire transfers. It also clarifies procedures for customer due diligence and includes a risk-based

approach to customer due diligence, as well as mandating enhanced customer due diligence for foreign politically exposed persons. It furthermore extends coverage of the regulations to include terrorist financing activities.

Any person who wishes to engage in business, whether local or foreign, must register under the Companies Act. Every Singapore-incorporated company must have at least two directors, one of whom must be a resident in Singapore, and one or more company secretaries, who must be resident in Singapore. There is no nationality requirement. A company incorporated in Singapore has the same status and powers as a natural person. Bearer shares are not permitted. Casinos and Internet gaming sites are currently illegal in Singapore. However, the government is considering lifting the ban on casinos for a specific development project. In December 2004, the Government of Singapore (GOS) invited international investors to submit proposals by February 28, 2005, to build an integrated resort with gambling facilities.

As a matter of policy, Singapore strongly opposes money laundering and terrorist financing. The Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act of 1999 (CDSA) criminalizes the laundering of proceeds from narcotics and 183 other serious offenses, including foreign offenses which would be serious offenses if they had been committed in Singapore. Singapore is in the process of reviewing its list of these offenses for consistency with Recommendation 1 of the FATF's Revised 40 Recommendations, and expects to have a final list by June 2005. Financial institutions must report suspicious transactions and positively identify customers engaging in large currency transactions. Financial institutions are required to maintain adequate records, to be able to respond quickly to GOS inquiries in money laundering cases. However, there are no reporting requirements on amounts of currency brought into or taken out of Singapore. Singapore is considering implementation of FATF Special Recommendation IX, which requires the detection of cross-border movement of currency and bearer negotiable instruments

Banking regulation is the responsibility of the Monetary Authority of Singapore. The MAS performs extensive prudential and regulatory checks on all applicants for banking licenses, including a check to see if the bank is under adequate home country banking supervision. Banks must have clearly identified directors. It is illegal to perform banking transactions without a license.

In 2000, MAS first issued a series of regulatory guidelines ("Notices") requiring banks to apply "know your customer" standards, adopt internal policies for staff compliance, and cooperate with Singapore enforcement agencies on money laundering cases. These Notices are regulatory in nature and are enforceable by prosecution. Similar guidelines exist for securities dealers and other financial service providers. Banks must obtain documentation, such as passports or identity cards, from all personal customers, so that the bank can verify their names, permanent contact addresses, dates of birth, and nationalities, and conduct inquiries into the bona fides of company customers. The regulations specifically require that financial institutions obtain evidence of the identity of the beneficial owners of offshore companies or trusts. The guidelines also mandate specific record keeping and reporting requirements, outline examples of suspicious transactions that should prompt reporting, and establish mandatory intra-company point-of-contact and staff training requirements. Similar guidelines and notices exist for finance companies, merchant banks, life insurers, brokers, securities dealers, investment advisors, and futures brokers and advisors. The MAS announced that it will also revise these Notices in line with the final form of the revised notice for banks.

The Suspicious Transaction Reporting Office (STRO) is Singapore's Financial Intelligence Unit (FIU). Part of the Singapore Police Force's Commercial Affairs Department, it began operating on January 10, 2000. To improve its suspicious transaction reporting, STRO has begun work on a computer system to allow electronic online submission of STRs, as well as the dissemination of AML/CFT material. It plans to encourage all financial institutions and relevant professions to eventually participate in this system.

Singapore is an important participant in the regional effort to stop terrorist financing in Southeast Asia. The Terrorism (Suppression of Financing) Act, passed in 2002, criminalizes terrorist financing, although the provisions of the Act are actually much broader. In addition to making it a criminal offense to deal with terrorist property (including financial assets), the Act criminalizes the provision or collection of any property (including financial assets) with the intention that the property be used, or having reasonable grounds to believe that the property will be used, to commit any terrorist act or for various terrorist purposes.

The Act also provides that any person in Singapore, and every citizen of Singapore outside Singapore, who has information about any transaction or proposed transaction in respect of terrorist property, or who has information that he/she believes might be of material assistance in preventing a terrorism financing offense, must immediately inform the police. The Act gives the authorities the power to freeze and seize terrorist assets. The Act, which supplements and extends interim legislation enacted in November 2001, took effect January 29, 2003.

In January 2003, the Singapore Government released a white paper describing its investigations into the Jemaah Islamiyah (JI) terrorist network. The government is known to have detained 39 persons since 2001 as suspected terrorists. Three persons have been released since then, two in September 2004 and one in January 2005, with restrictions placed on their associations and movements.

In April 2004, the International Monetary Fund and the World Bank Financial Sector Assessment Program (FSAP) team published an assessment of Singapore's financial sector, which included an evaluation of the AML/CFT regime. The IMF found that Singapore's ability to freeze terrorist related funds is comprehensive. The IMF also concluded that, while Singapore has not adopted the FATF approach of designating terrorist financing offenses as predicate crimes for money laundering, Singapore appears to meet the underlying obligations of the relevant FATF Special Recommendation Two on terrorist financing.

There are few restrictions on intergovernmental terrorist financing-related mutual legal assistance even in the absence of a Mutual Legal Assistance Treaty, because Singapore is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the IMF concluded. But the IMF urged Singapore to improve its mutual legal assistance, noting serious limitations on assistance with the provision of bank records, with search and seizure of evidence, on restraining proceeds of crime, and on the enforcement of foreign confiscation orders.

On the terrorist financing front, the MAS has broad powers to direct financial institutions to comply with international obligations. These include UN Security Council Resolutions 1267, 1333, 1373, 1390, and other similar resolutions. In 2002, the MAS issued regulations. to implement this authority. The regulations bar banks and financial institutions from providing resources and services of any kind which will benefit terrorists, and from doing "anything that . . . assists or promotes" terrorist financing. Financial institutions must notify the MAS immediately if they have in their possession, custody, or control any property belonging to terrorists or any information on transactions involving terrorists' funds. The regulations apply to all branches and offices of any financial institutions incorporated in Singapore, or incorporated outside of Singapore but which are located in Singapore. The regulations include a list of the entities and individuals on the UNSCR 1267 Sanctions Committee's consolidated list. Singapore updates the regulations periodically to include additional names as they are added by the UNSCR 1267 Sanctions Committee.

Alternative remittance systems exist, and are used mainly by the approximately 500,000 foreign workers in Singapore. All remittance agents, formal or informal, must be licensed and are subject to the same laws and regulations, including requirements for record keeping and the filing of suspicious transaction reports. In 2002, the regulations were strengthened. The firms now have to submit a financial statement every three months, and report the largest amount transmitted on a single day.

Firms must also answer questions about the way they conduct business and about their overseas partners. Informal networks, such as hawala, that are not licensed are considered illegal.

Charities in Singapore are subject to extensive government regulation, including close oversight and reporting requirements, and restrictions that limit the amount of funding which can be transferred out of Singapore. A total of 1,669 charities were registered as of December 31, 2003. All charities must register with the Commissioner of Charities, and must, as part of the registration process, submit governing documents outlining the charity's objectives, and particulars on all trustees. The Commissioner of Charities has the power to investigate charities, including authority to search and seize records, and to restrict the transactions into which the charity can enter, suspend charity staff or trustees, and/or establish a scheme for the administration of the charity. Charities must keep detailed accounting records, and retain them for at least seven years.

Under the Charities (Fund-raising Appeals for Foreign Charitable Purposes) Regulations 1994, any charity or person who wishes to conduct or participate in any fund raising for any foreign charitable purpose must apply for a permit. The applicant has to show that at least 80 percent of the funds raised will be used in Singapore, although the Commissioner of Charities has discretion to allow a lower percentage to be applied within Singapore. Permit holders are subject to additional record keeping and reporting requirements, including details on every item of expenditure disbursed, amounts transmitted to persons outside Singapore, and to whom the money was transmitted.

A total of 33 permits were issued in 2003 for fund raising for foreign charitable purposes. There are not restrictions or direct reporting requirements on foreign donations to charities in Singapore.

Singapore is party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism and has signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. Singapore is a member of the FATF, the Asia/Pacific Group on Money Laundering, the Egmont Group, and the Offshore Group of Banking Supervisors Singapore will host the June 2005 Plenary meeting of the FATF, marking the first time an FATF Plenary will take place in Southeast Asia.

To bolster law enforcement cooperation and facilitate information exchange, Singapore enacted the Mutual Assistance in Criminal Matters Act (MACMA) in March 2000. The MACMA provides for international cooperation on any of the 183 predicate "serious offenses" listed under the CDSA of 1999. The provisions of the MACMA apply to countries that have concluded treaties, memoranda of understanding, or other agreements with Singapore.

In November 2000 Singapore and the United States signed the Agreement Concerning the Investigation of Drug Trafficking Offenses and Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking. This was the first agreement concluded pursuant to the MACMA. This agreement, which entered into force in early 2001, facilitates the exchange of banking and corporate information on drug money laundering suspects and targets, including access to bank records. It also entails reciprocal honoring of seizure/forfeiture warrants. This agreement applies only to narcotics cases, and does not cover non-narcotics-related money laundering, terrorist financing, or financial fraud.

The Terrorism (Suppression of Financing) Act provides for mutual legal assistance in cases where there is no treaty, memorandum (MOU), or other agreement in force between Singapore and another country that is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Singapore's FIU has concluded MOUs concerning cooperation in the exchange of financial intelligence with counterparts in Australia, Belgium, Japan, and the United States, and continues to actively seek MOUs with additional FIUs.

In May 2003 the Singapore Government issued a regulation pursuant to the Terrorism Act and the MACMA that enables the government to provide legal assistance to the United States and the United

Kingdom in matters related to terrorism financing offenses. Singapore concluded a mutual legal assistance agreement with Hong Kong in 2003. In 2004, Singapore signed a treaty on mutual legal assistance in criminal matters with seven other members of ASEAN: Brunei, Cambodia, Indonesia, Laos, Malaysia, the Philippines and Vietnam. The treaty will come into effect after ratification by the respective governments.

The Government of Singapore should continue close monitoring of its domestic and offshore financial sectors. As a major financial center, it should also take measures to regulate and monitor large currency and bearer negotiable instrument movements into and out of the country, in line with the FATF's Ninth Special Recommendation, adopted in October 2004, that countries implement measures such as declaration systems, in order to detect cross-border currency smuggling. The conclusion of broad mutual legal assistance agreements is also important to further Singapore's ability to work internationally to counter money laundering and terrorist financing.

Slovak Republic

Slovakia is not considered an important regional financial center. The geographic, economic, and legal conditions that shape the money laundering environment in Slovakia are typical of those in other Central European transition economies. Slovakia's location along the major lines of communication connecting Western, Eastern, and Southeastern Europe makes it a transit country for smuggling and trafficking in narcotics, arms, stolen vehicles, and humans. Organized crime activity and the opportunities to use gray market channels also lead to a favorable money laundering environment. Financial crimes such as fraud, tax evasion, embezzlement, and illegal business activity have been quite problematic for Slovak authorities.

Slovakia's original anti-money laundering legislation, Act No. 249/1994 (later amended by Act No. 58/1996) came into effect in 1994. Article 252 of the Slovak Criminal Code, "Legalization of Proceeds from Criminal Activity," came into force at the same time. These measures criminalize money laundering for all serious crimes, and impose customer identification, record keeping, and suspicious transaction reporting requirements on banks. A money laundering conviction does not require a conviction for the predicate offense, and a predicate offense does not have to occur in Slovakia to be considered as such. The failure of a covered entity to report, as well as tipping off, are criminal offenses.

As a result of amendments made to the Slovak Civil Code in 2001, new anonymous passbook savings accounts are banned. All banks in Slovakia were ordered to stop offering new anonymous accounts. All owners of anonymous accounts were required to disclose their identity to the bank and to close the anonymous account by December 31, 2003. Owners of accounts that were not closed may withdraw money for an additional three-year non-interest-bearing grace period. However, funds remaining after January 1, 2007 will be confiscated and deposited in a fund for the administration of the Ministry of Finance, where they will be available for collection by the accountholder for another five years. As of January 1, 2007, bearer passbook accounts will cease to exist.

In 2000 the legislature approved modifications to existing anti-money laundering regulations, with the passage of Act No. 367/2000, "On Protection against the Legalization of Proceeds from Criminal Activities." The Act came into force on January 1, 2001. One of the most significant changes that Act No. 367/2000 introduces is in relation to the types of transactions subject to the reporting requirements. The law replaces the standard of "suspicious transactions" with an expanded definition of "unusual business activity." According to this modified definition, an unusual business activity is any transaction that could result in the legalization of income, the source of which is suspected to be criminal. Such transactions include the attempted disposal of income or property with the knowledge or suspicion that it was acquired through criminal activity in Slovakia or a third country. Designated transactions include the acquisition, possession, or use of real estate, moveable property, securities,

money, or any other property with monetary value, for the purpose of concealing or disguising its ownership.

As recommended in 2001 by the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) in its second-round evaluation of Slovakia, the Government of Slovakia (GOS) amended Act No. 367/2000 in order to address shortcomings of the original legislation, and in order to comply with European Directive 2001/97/EC. As a result, Slovakian legislation is now in full harmony with the Second European Union (EU) Directive. The FATF's 2002-3 Annual Report stated that the amended legislation provided a "basically sound preventive legal structure." Act No. 367/2000 expands the list of entities subject to reporting requirements to include foreign bank subsidiaries, the Slovak Export-Import Bank, non-bank financial institutions such as casinos, post offices, brokers, stock exchanges, commodity exchanges, securities markets, asset management companies, insurance companies, real estate companies, tax advisors, auditors, credit unions, leasing firms, auctioneers, foreign exchange houses, and pawnshops, all of which have been particularly susceptible to money laundering.

Amendments to Act No. 367/2000 in 2002 further extend reporting requirements to antique, art, and collectible brokers; dealers in precious metals or stones, or other high-value goods; legal advisors; consultants; securities dealers; foundations; financial managers and consultants; and accounting services. Covered persons are required to identify all customers, including legal entities, if they find that the customers prepared or conducted transactions deemed to be suspicious, or if a sum or related sums exceeding 15,000 euros within a 12-month period is involved. (Previous law had set the reporting threshold at 2,600 euros.) Insurance sellers must identify all clients whose premium exceeds 1,000 euros in a year or whose one-time premium exceeds 2,500 euros. Casinos are obligated to identify all customers. Transactions may be delayed by the covered entities up to 48 hours, with another 24-hour extension allowed if authorized by the Financial Police. If the suspicion turns out to be unfounded, the state assumes the burden of compensation for losses stemming from the delay.

Originally, Slovakia's Financial Intelligence Unit (FIU), the Financial Intelligence Unit of the Bureau of Organized Crime, was established under the Ministry of the Interior and was a part of the Bureau of Financial Police (BFP). However, as of January 2004, the BFP ceased to exist and its duties were assumed by the newly created Office to Fight Organized Crime (OFOC), which focuses on all forms of organized crime, including narcotics, money laundering, human trafficking, and prostitution. The OFOC has four regional units of financial police, each responsible for a different part of Slovakia (Bratislava, Eastern Slovakia, Western Slovakia, and Central Slovakia). After the abolition of the BFP, the FIU was re-organized and moved to the OFOC.

The FIU has five primary departments: Analytical, Unusual Business Transactions, Supervision of Obliged Entities, International Cooperation, and Property Checks. The FIU increased its administrative capacity by raising its staff level from 25 to 34 personnel and its analysts participate regularly in international and domestic fora related to combating money laundering. The FIU has jurisdictional responsibility over money laundering violations, receives and evaluates suspicious transaction reports (STRs), and collects additional information to establish the suspicion of money laundering. If justified, the unit forwards the case to one of the regional financial police units. Once enough information has been obtained to warrant suspicion that a criminal offense has occurred, the FIU takes appropriate measures, including asking a financial institution or bank to delay business or a financial transaction. The FIU can also submit the case to the state prosecutor's office for investigation and prosecution.

In 2003, the BFP (through the FIU) registered 318 allegations of financial crime worth an estimated value of Slovak koruny (SKK) 54.8 billion ($1.83 billion). The police formally investigated 251 of these allegations. The cases investigated had an approximate value of SKK 34.3 billion ($1.14 billion). The police prosecuted 123 of the cases and convicted 72 entities. Also in 2003, the BFP received 489

reports alleging suspicious business operations totaling SKK 9.2 billion ($307 million). On the basis of these 489 reports, 88 money laundering investigations were initiated by the police, resulting in the referral of 38 cases to the courts and 33 prosecutions. The BFP also conducted 23 on-site inspections of covered entities during 2003. Ten of these inspections resulted in the levying of fines totaling SKK 1,610,000 ($54,000).

In the first eleven months of 2004, the OFOC (through the FIU) received 738 reports alleging unusual financial transactions worth a total of SKK 19.3 billion ($643 million). It submitted 20 proposals totaling SKK 46.4 million ($1.54 million) for criminal prosecution and 55 proposals for tax prosecution. In addition, the regional police units submitted 107 proposals for criminal prosecutions. The OFOC started 69 on-site inspections (24 are completed) of covered persons and levied penalties totaling SKK 2.41 million ($80,300) in 23 cases.

In 2003, a law amending and supplementing the Criminal Procedure Code and Criminal Code entered into force. It provides law enforcement with the authority to conduct "sting operations" and introduces provisions regarding corporate criminal liability and "crown" witnesses. A "crown witness" (a criminal who voluntarily opts to cooperate with law enforcement bodies) could be granted immunity or receive a shortened sentence. This rule does not apply to those that organized or instigated the crime.

In late 2003, the Slovak cabinet approved a law on measures against entities that acquired property through illegal income (also known as the Law on Proving the Origin of Property). According to the draft law, an undocumented increase in property exceeding the minimum monthly wage multiplied by 200 would be scrutinized and would be considered possibly illegal. Anyone who has suspicions about possibly illegally acquired property may report it to the police, who are then obliged to investigate the allegations, ultimately reporting to the Office of the Attorney General if findings are conclusive. The Attorney General's Office may then order the property to be confiscated. In January 2004, the Ministry of Justice withdrew the draft law from Parliament when it was evident it would not be approved.

Slovakia has responded to the problem of the financing of terrorism by amending its money laundering law with Act No. 445/2002, which criminalizes terrorist financing and obliges covered entities to report transactions possibly linked to terrorist financing. All competent authorities in the Slovak Republic have full power to freeze or confiscate terrorist assets in accordance with UNSCR 1373. According to act no. 367/2000 and its later amendment, financial institutions are required to report to the regional financial police when they freeze or identify suspected terrorist-linked assets. The GOS agreed to freeze immediately all accounts owned by entities on the UNSCR 1267 Sanctions Committee's and EU's (but not the United States') consolidated lists. No terrorist finance-related accounts have been frozen or seized in Slovakia, but were a terrorism-related account to be identified, the Financial Police would hold any related financial transaction for up to 48 hours, and then gather evidence to freeze the account and seize any assets. The GOS is now a signatory to all 12 of the UN Conventions concerning the fight against terrorism. However, as reported in MONEYVAL 2004 member states' self-assessment questionnaire, Slovakia is still not fully compliant with the FATF's Special Recommendations on Terrorist Financing, having received in 2004 from MONEYVAL a rating of "partial compliance" with regard to Special Recommendation I (Implementation of UNSCR 1373) and Special Recommendation VII (enhanced scrutiny of transfers lacking originator information).

The GOS is a party to the UN International Convention for the Suppression of the Financing of Terrorism. The provisions of the Convention have been incorporated into amendments of the Bank Act, Penal Code, and Act No. 367/2000. However, Slovakia elected to pursue several optional terms of the convention that were fully incorporated in March 2003. The FIU has memoranda of understanding (MOUs) with the FIUs of Slovenia, Monaco, Ukraine, Australia, Belgium, Poland, and

the Czech Republic. The GOS also hopes to sign MOUs with Albania and Taiwan in 2005. Slovakia's FIU is the responsible authority for international exchange of information regarding money laundering under the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

Slovakia is a party to the European Convention on Mutual Legal Assistance; the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the 1988 UN Drug Convention; and the UN Convention against Transnational Organized Crime. It also has signed the UN Convention against Corruption. Slovakia became a member of the Organization for Economic Cooperation and Development (OECD) in December 2000, thereby expanding its opportunities for multilateral engagement. Slovakia is a member of the Council of Europe and participates in MONEYVAL. Slovakia sends experts to conduct mutual evaluations on fellow member countries; it also underwent mutual evaluations by this group in 1998 and 2001. Slovakia is a member of the Egmont Group.

The Government of Slovakia should continue to improve its anti-money laundering regime. Continued implementation of the provisions of Slovakia's anti-money laundering legislation will give the Slovak financial system greater protection, by helping it prevent and detect money laundering in all financial sectors. Slovakia should also improve supervision of some non-bank sectors to ensure reporting requirements are followed. Slovakia should provide adequate resources to assure that its FIU, law enforcement, and prosecutorial agencies are adequately funded and trained to effectively perform their various responsibilities.

Slovenia

While not a major money laundering country, Slovenia's economic stability and location on the Balkan drug route offer attractive opportunities for money laundering. Narcotics-trafficking, especially heroin via the "Balkan route" smuggled by mainly Albanian and Serbian nationals, is a growing problem and the main source of illegal proceeds. Other significant sources of illegal proceeds are fraud, trafficking in weapons and persons, and currency and securities counterfeiting, as well as extraterritorial offenses such as tax evasion, tax and VAT fraud, and corruption. Organized crime is believed to be involved in both predicate crimes and laundering operations. Money laundering often tends to be undertaken by citizens of the neighboring countries and those of the former Soviet Union, and occurs through the banking system, foreign exchange houses, real estate transactions, and cross-border currency transport.

The Penal Code criminalizes money laundering and the financing of terrorism. A change made to Slovenia's Penal Code, in 2004, increases the imprisonment penalty for money laundering from three to five years. Negligent money laundering is also criminalized.

Slovenia's Law on the Prevention of Money Laundering (LPML) was enacted in 1994 and amended in 2001 and 2002. The October 2001 amendments update the original law by, among other provisions, expanding the OMLP's sources of available financial information, and requiring mandatory client identification for transactions exceeding 3 million Slovenian tolars (approximately $14,400). December 2001 saw the passage of a new law that increased the power of supervisory authorities to prohibit the establishment of new bearer passbook accounts and phased out already existing bearer passbook accounts. Further amendments to the law, which extend reporting obligations to lawyers, law firms, notaries, auditors and tax advisors, auctioneers, art dealers, gaming houses, and lottery concessions, were passed and entered into force in July 2002. Additional identification requirements, most notable of which is the requirement to identify beneficial owners, were also implemented. Due to the nature of their business, certain professions (lawyers, notaries, auditors, accountants, and tax advisors) are required only to file suspicious transaction reports (STRs) and are exempt from currency transaction reporting requirements. Records must be retained for a minimum of ten years. There are

nine understatutory regulations in force providing detailed measures for the implementation of the LPML. Slovenian legislation is now harmonized with the provisions outlined in the Second EU Directive.

Financial supervisory bodies include the Bank of Slovenia, the Securities Market Agency, the Insurance Supervisory Agency, the Office for Gaming Supervision, the Slovene Audit Institute, and the supervisory body responsible for the oversight of tax advisory services. The Bank of Slovenia has supervisory power over bureaux de change, and in February 2003 issued a handbook for those bodies complete with reporting requirements, auditing procedures, and indicators.

Slovenia's Financial Intelligence Unit (FIU), the Office for Money Laundering Prevention (OMLP), an administrative FIU, was established in 1995 within Slovenia's Ministry of Finance. The FIU has a staff of 17. The 2002 amendments to the LPML gave OMLP more power and latitude in opening cases and sharing information. The amount of time during which transactions can be held is increased from 48 to 72 hours. The OMLP used its powers in six instances to temporarily suspend transactions with a total combined value of $3,704,352. In its nine years of operation, OMLP has opened 764 suspicious cases and closed 655 cases. Foreign nationals were involved in more than half of these cases. In 2004, OMLP opened 112 new cases of suspected money laundering and closed 88 cases. Nine of the 88 cases were forwarded to the Police and/or Public Prosecution. In addition, 25 cases regarding suspicion of other serious criminal offenses (according to Article 22 of the LPML) were sent to the police and other competent bodies for further investigation. Two judgments have been finalized, but in both cases, due to procedural reasons, the defendants were acquitted.

Several additional cases are currently pending in the court system. The existence of a large backlog of cases in the courts continues to be a major factor impeding Slovenia's anti-money laundering regime. Law enforcement authorities, prosecutors, and judges all lack experience with regard to pursuing financial crimes, including money laundering.

The Ministry of Justice has been authorized to form a decision on whether a new law on mutual legal assistance in criminal matters will be drafted, which may include also the assets sharing provisions.

New changes and amendments (primarily focused on refining provisions regarding the financing of terrorism) are expected to be implemented after the Government of Slovenia's (GOS's) adoption of the European Union's (EU's) Third Money Laundering Directive during the second half of 2005.

The 1902 extradition treaty between the United States and the Kingdom of Serbia remains in force between the United States and Slovenia. Slovenia became a member of the EU on May 1, 2004, and is actively involved in regional efforts to combat money laundering and terrorism financing, working throughout the Balkans and Eastern Europe, especially with Serbia, Montenegro, Ukraine, Macedonia, and Russia. With regard to international cooperation, Slovenia (especially the OMLP) has a very positive reputation, having conducted a regional counternarcotics conference with Croatian counterparts, and having hosted a regional anti-money laundering conference for eight of its Balkan neighbors in October 2004.

Slovenia is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), and has undergone a mutual evaluation by the Committee, as well as lending its own experts to evaluate other member countries. The OMLP is a member of the Egmont Group. Slovenia also actively participates in other multilateral programs combating money laundering and terrorism financing. Slovenia is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and ratified the Civil Law Convention on Corruption in July 2003. Slovenia is also party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. In July 2003 Slovenia signed the European Convention on the Suppression of Terrorism.

The Government of Slovenia should continue to work with its law enforcement and judicial authorities to increase the levels of action and experience in pursuing financial crime. Slovenia should provide specific training to provide law enforcement, prosecutors, and judges with a better understanding of money laundering and other financial crimes so that they will be able to effectively investigate and prosecute cases of money laundering.

Solomon Islands

The Solomon Islands is not a regional financial center. The Islands' banking system is small. The Parliament criminalized money laundering in 2002 with the passage of the Anti-Money Laundering Act and the Proceeds of Crime Act. The Acts provide mechanisms designed to prevent the movement of funds for terrorist purposes and to enhance the exchange of financial intelligence with other countries. Implementation of the Acts has been slow, but Parliament did act to establish a Financial Intelligence Unit (FIU) at the Central Bank in late 2004. The presence of RAMSI-affiliated Australian and New Zealand civil servants in key positions throughout the government has further aided the adoption of better banking practices.

The Solomon Islands is not a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, or the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of the Solomon Islands should become a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. It should provide the recently established FIU with sufficient staff and resources to effectively carry out its mission.

South Africa

South Africa's position as the major financial center in the region, its relatively sophisticated banking and financial sector, and its large cash-based market, all make it a very attractive target for transnational and domestic crime syndicates. Nigerian, Pakistani, and Indian drug traffickers, Chinese Triads and Taiwanese groups, and the Russian Mafia, have all been identified as operating in South Africa, along with native South African criminal groups. Although the links between different types of crime have been observed throughout the region, money laundering is primarily related to the illicit narcotics trade. Other common types of crimes related to money laundering are: fraud, theft, corruption, currency speculation, illicit dealings in precious metals and diamonds, human trafficking, and smuggling. Most criminal organizations are also involved in legitimate business operations. There is a significant black market for smuggled goods. South Africa is not an offshore financial center.

The Government of South Africa (GOSA) estimates that between $2 and $8 billion is laundered each year through South African financial institutions. The Proceeds of Crime Act (No. 76 of 1996) criminalized money laundering for all serious crimes. This Act was supplemented by the Prevention of Organized Crime Act (No. 121 of 1998), which confirms the criminal character of money laundering, mandates the reporting of suspicious transactions, and provides a "safe harbor" for good faith compliance. Violation of this Act carries a fine of up to Rand 100 million (approximately $16,667,330) or imprisonment for up to 30 years. Subsequent regulations direct that the reports be sent to the Commercial Crime Unit of the South African Police Service. Both of these acts contain criminal and civil forfeiture provisions.

On November 11, 2004, the Parliament passed the Protection of Constitutional Democracy Against Terrorist and Related Activities Act (POCDATARA), which specifically criminalizes terrorist activity and terrorist financing. The Act would make it easier to identify, freeze, and seize assets related to money laundering. Significantly, the Act (which, pending Presidential signature, would take effect in

early 2005) will be applicable to charitable and non-profit organizations operating in South Africa, although there is no information that these groups have been linked to terrorist financing.

In November 2001, the President signed the Financial Intelligence Centre Act (FICA) into law. Pursuant to the FICA, South Africa established both the Financial Intelligence Centre (FIC) and the Money Laundering Advisory Council to advise the Minister of Finance on policies and measures to combat money laundering. The mandate of the FIC is to coordinate policy and efforts to counter money laundering activities. The FIC similarly acts as a centralized repository of information and statistics on money laundering. The FIC began operating in February 2003. In July 2003, the FIC was admitted as a member of the Egmont Group of financial intelligence units.

The FICA requires a wide range of financial institutions and businesses to identify customers, maintain records of transactions for at least five years, appoint compliance officers to train employees to comply with the law, and report transactions of a suspicious or unusual nature. Such businesses include companies and firms considered particularly vulnerable to money laundering activities, such as banks, life insurance companies, foreign exchange dealers, casinos, and real estate agents. If the FIC has reasonable grounds to suspect that a transaction involves the proceeds of criminal activities, the FIC will forward this information to the investigative and prosecutorial authorities. If there is suspicion of terrorist financing, that information is to be forwarded to the National Intelligence Service. There are no bank secrecy laws in effect that prevent the disclosure of ownership information to bank supervisors and law enforcement authorities. However, very few actual cases have been prosecuted to date.

From March 2003-March 2004, the FIC received 7,480 suspicious transaction reports (STRs), the vast majority from money remitters (4,079) and banks (2,732). This number was above what had been projected. Ninety percent of the STRs were sent electronically. No information is available on how many of these STRs led to criminal investigations, but the number is believed to be very low. In addition, the quality and consistency of the STRs was uneven, probably due to the fact that not all of South Africa's banks have yet implemented internal anti-money laundering training programs. Many banks believe the reporting requirements hamper their efforts to attract new customers. In particular, retroactive know your customer (KYC) requirements mean that account holders who do not present identifying documents in person risk having their accounts frozen. The National Treasury has extended the staggered timetable for fully implementing KYC (higher-risk clients first) to September 30, 2006.

The FIC made progress in 2004 in building its capabilities and in establishing its credibility with the South African law enforcement community. During its first full year of operation, it received 105 information requests from local law enforcement and 56 from international law enforcement agencies. The FIC plans to obtain further analytical training for its staff, particularly in the area of detecting terrorist financing in the absence of specific intelligence.

Because of the cash-driven nature of the South African economy, alternative remittance systems that bypass the formal financial sector exist, used largely by the strong local Islamic community. Currently, there is no legal obligation requiring alternative remittance systems to report cash transactions.

The Financial Action Task Force (FATF) conducted a mutual evaluation of South Africa in 2003 and made several recommendations regarding controls on cross-border currency movement, thresholds and amendments to the Exchange Control Act. Those recommendations have yet to be adopted.

South Africa has cooperated with the United States in exchanging information related to money laundering and terrorist financing. The two nations have a Mutual Legal Assistance Treaty and a bilateral Extradition Treaty. In June 2003, South Africa became the first African nation to be admitted into the Financial Action Task Force. South Africa is also an active member of the Eastern and

Southern African Anti-Money Laundering Group (ESAAMLG), having signed the memorandum of understanding in 2003.

The GOSA is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime (ratified in February 2004).

The Government of South Africa should implement the FATF recommendations to establish better control over cross-border currency movement. It should begin to regulate the country's alternative remittance systems. It should monitor and make available the number of criminal investigations resulting from STRs, and it should increase the number of actual money laundering prosecutions. It should enact and fully implement the new law against terrorist activity and terrorist financing.

Spain

Money laundered in Spain is primarily from the proceeds of the Colombian cocaine trade, although money laundered through other Latin American countries also plays a role. Colombian organizations use several methods to move money from European drug sales out of Spain. Airline personnel traveling between Spain and Latin America carry out money. Colombian companies purchase goods in Asia and sell them legally at cartel-run stores in Europe. Credit card balances are paid in Spanish banks for charges made in Latin America, or money deposited in Spanish banks is withdrawn by ATM cards in Colombia. Additionally, wire transfers continue to be a common way of getting funds out of Spain.

Drug proceeds from other regions enter Spain as well. Hashish proceeds come from Morocco and heroin money enters from Turkey. The majority of money that enters Spain to be laundered is smuggled across the border in three ways. Bulk cash is carried in travelers' luggage or hidden on their bodies when arriving at international airports; shipping containers loaded with currency enter through Spanish ports (such as Algeciras); or, money is brought in by small craft along Spain's long coastline. The informal non-bank outlets (such as "Locutorios"), which make small international transfers for the immigrant community, continue to be used to move money in and out of Spain. Regulators also suspect the presence of "hawala"-like networks in the Islamic community.

Tax evasion in internal markets and smuggling of goods along the coastline continue to be sources of illicit funds in Spain. Spanish authorities believe that tax evasion in the cell phone and property industries is the most serious problem. The smuggling of electronics and tobacco from Gibraltar remains an ongoing issue. Although little of the money laundered in Spain is believed to be used for terrorist financing, money from the extortion of businesses in the Basque region is moved through the financial system and used to finance the Basque terrorist group ETA.

The Government of Spain (GOS) remains committed to combating narcotics-trafficking, terrorism, and financial crimes, and continues to work hard to tighten financial controls. The criminalization of money laundering was added to the penal code in 1988 when laundering the proceeds from narcotics-trafficking was made a criminal offense. In 1995 the law was expanded to cover all serious crimes that required a prison sentence greater than three years. Amendments to the code on November 25, 2003, which took effect on October 1, 2004, made all forms of money laundering financial crimes. To date, there have not been any cases of Spanish officials being involved in money laundering in Spain.

The penal code can also apply to individuals in financial firms if their institutions have been used for financial crimes. An amendment to the penal code in 1991 made such persons culpable for both fraudulent acts and negligence connected with money laundering.

Businesses and financial service suppliers operating in Spain or targeting Spanish markets are subject to the law, Ley de Servicios de la Sociedad de Informacion y de Comercio Electronico (LSSICE), that

came into force on October 12, 2002, for Internet marketing and distribution. The new law requires businesses to register their domain names, company registry, physical address, and other company details. Financial sector businesses such as online banks must still send written contracts to new customers for signature and obtain physical proof of their identity, in order to comply with existing banking regulations.

Royal Decree 998/2003 of July 5, 2003, modified the structure of the Ministry of Interior to facilitate more active combating of drug-trafficking. This law creates an Advisory Committee on Observation that will attempt to follow the use of technologies by criminal organizations and money launderers and to take measures to ensure that Spanish law enforcement authorities are able to meet the new challenges.

Specific measures to prevent money laundering were written to regulate the legal entities in the financial sector and individuals moving large sums of cash, in December 1993 (Law No. 19/1993), as an expansion to the criminal code that previously applied only to physical persons. The regulations for enactment were established by Royal Decree 925/1995, which set the standards for regulation of the financial system. The regulations were amended in 2003 and cover money laundering linked to all serious crimes. The financial sector is required to identify customers, keep records of transactions, and report suspicious financial transactions. Spanish banks are required by law to maintain fiscal information for five years and mercantile records for six years.

The money laundering law applies to most entities active in the financial system, including banks, mutual savings associations, credit companies, insurance companies, financial advisers, brokerage and securities firms, postal services, currency exchange outlets, casinos, and individuals and unofficial financial institutions exchanging or transmitting money (alternative remittance systems). The 2003 amendments add lawyers and notaries as covered entities. Previously, notaries and lawyers were required to report suspicious cases, but now they are considered part of the financial system that is under the supervision of appropriate regulators.

Law 19/2003 regulating the movements of capital and foreign transactions implements the European Union (EU) Money Laundering Directive. The law obligates financial institutions to make monthly reports on large transactions. Banks are required to report all international transfers greater than 30,000 euros. The law also requires the declaration and reporting of internal transfers of funds greater than 80,500 euros. Individuals traveling internationally are required to report the importation or exportation of currency greater than 6,000 euros. Law 19/2003 allows the seizure of up to 100 percent of the currency if illegal activity under financial crimes ordinances can be proven. Spanish authorities claim they have seen a drop in cash couriers since the law's enactment in July 2003. For cases where the money cannot be connected to criminal activity, and has not been declared, the authorities may seize the money until the origin of the funds is proven.

The Commission for the Prevention of Money Laundering and Financial Crimes (CPBC) coordinates the fight against money laundering in Spain. The Secretary of State for Economy heads the commission and all of the agencies involved in the prevention of money laundering participate. The representatives include the National Drug Plan Office, the Ministry of Economy, the Federal Prosecutors (Fiscalia), Customs, the Spanish National Police, the Guardia Civil, CNMV (equivalent to the SEC), the Treasury, the Bank of Spain, and the Director General of Insurance and Pension Funds. Any member of the Commission may request an investigation, should suspicious activity be brought to his or her attention.

The CPBC delegates responsibility to two additional organizations. The first is a secretariat in the Treasury, located in the Ministry of Economy. Following investigation and a guilty verdict by a court, this regulating body carries out penalties. Sanctions can include closure, fines, account freezes, or seizures of assets. Law 19/2003 allows seizures of assets of third parties in criminal transactions, and a seizure of real estate in an amount equivalent to the illegal profit.

The second organization is the Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC), which serves as Spain's financial intelligence unit. SEPBLAC receives and analyzes suspicious transaction reports (STRs) and currency transaction reports (CTRs). SEPBLAC has the primary responsibility for any investigation in money laundering cases and directly supervises the anti-money laundering procedures of banks and financial institutions. Incriminating information is turned over to the federal prosecutors for prosecution. SEPBLAC received 1,351 STRs in 2002, 1,598 STRs in 2003, and 2,414 STRs in 2004. In addition, SEPBLAC received 205,252 CTRs in 2002, 294,508 CTRs in 2003, and 331,856 CTRs in 2004.

The Fund of Seized Goods of Narcotics Traffickers receives seized assets. This agency was established under the National Drug Plan. The proceeds from the funds are divided, with half going to drug treatment programs and half to a foundation that supports the officers fighting narcotics-trafficking. Seizures of assets involving more than one country, and the division of the assets, depend on the relationship with the country in question. EU working groups will determine how to divide the proceeds for member countries. Outside of the EU, bilateral commissions are formed with countries that are members of Financial Action Task Force (FATF), FATF-like bodies, and the Egmont Group, to deal with the division of seized assets. With other countries, negotiations are conducted on an ad hoc basis.

Terrorist financing issues are governed by a separate code of law and commission, the Commission of Vigilance of Terrorist Finance Activities (CVAFT). This commission was created under Law 12/2003 on the Prevention and Blocking of the Financing of Terrorism. The commission is headed by the Ministry of Interior, and includes representatives from the Fiscalia and Ministries of Justice and Economy. SEPBLAC will serve as the Executive Service and as the Secretariat for this Commission. Currently, only the head of CVAFT can request information in terrorist financing cases, so other members must rely on the commission head to begin an investigation.

Crimes of terrorism are defined in Article 571 of the Penal Code, and penalties are set forth in Articles 572 and 574. Sanctions range from ten to thirty years' imprisonment with longer terms if the terrorist actions were directed against government officials. The Spanish authorities' ability to freeze accounts granted in the most recent law is more aggressive than that of most of their European counterparts. Though many laws are transposed from European Union (EU) directives, Law 12/2003 on the prevention and freezing of terrorist financing goes beyond EU requirements. However, the implementing regulations for this law have not been written, and it has not been used. Once in full effect, this law will allow administrative freezing of suspect assets without a judge's order.

All legal charities are placed on a register maintained by the Ministry of Justice. Responsibility for policing registered charities lies with the Ministry of Public Administration. If the charity fails to comply with the requirements, sanctions or other criminal charges may be levied.

Spain is a member of the FATF, and co-chairs the FATF Terrorist Finance Working Group. Spain is a participating and cooperating nation to the South American Financial Action Task Force (GAFISUD), and a cooperating and supporting nation to the Caribbean Financial Action Task Force (CFATF). Spain is a major provider of counterterrorism assistance. The GOS is a party to the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. Spain is also a party to the 1988 UN Drug Convention. SEPBLAC is a member of the Egmont Group and is currently chairing one of the Egmont Committee working groups.

The GOS has signed criminal mutual legal assistance agreements with Argentina, Australia, Canada, Chile, the Dominican Republic, Mexico, Morocco, Uruguay, and the United States. Spain's Mutual Legal Assistance Treaty with the United States has been in effect since 1993, and provides for sharing of seized assets, provided the request is made to the Spanish court hearing the case, rather than administratively. Spain also has entered into bilateral agreements for cooperation and information exchange on money laundering issues with Bolivia, Chile, El Salvador, France, Israel, Italy, Malta,

Mexico, Panama, Portugal, Russia, Turkey, Venezuela, Uruguay and the United States. SEPBLAC has also entered into bilateral agreements for cooperation and information exchange on money laundering issues with Andorra, Argentina, Australia, Belgium, Brazil, Bulgaria, Colombia, Finland, France, Guatemala, Italy, Korea, Mexico, Monaco, Panama, Peru, Poland, Portugal, Romania, Ukraine, Venezuela and the United States. Spain actively collaborates with Europol, supplying and exchanging information on terrorist groups. U.S. law enforcement agencies reported excellent cooperation with their Spanish counterparts in 2004. U.S. customs works closely with Spanish customs, Spanish prosecutors, the national police corps and the Civil Guard. The Drug Enforcement Administration works closely with SEPBLAC, the national police and the Civil Guard. These organizations regularly share information. Official documents however, will only be transferred if requested by a court.

The scale of the money laundering industry and the sophisticated methods used by criminals create a very large law enforcement problem in Spain. The Government of Spain makes every effort to eliminate financial crime in the country. Spain should continue the strong enforcement of its anti-money laundering program and its leadership in the international arena. It should consider whether additional measures are required to address possible money laundering in the stock market to ensure that the sector is not used for financial crimes and should fully implement Law 12/2003 to allow administrative freezing of suspect assets.

Sri Lanka

Sri Lanka is neither an important regional financial center nor a preferred center for money laundering. Money laundering currently is not a criminal offense. There are strict bank secrecy laws, under which the Government of Sri Lanka is required to obtain a court order to obtain banking information on bank customers. The Central Bank introduced regulations on customer due diligence in a December 2001 bid to tackle money laundering and terrorist financing in the absence of a specific legal framework. These regulations apply to commercial banks and licensed specialized banks coming under the Central Bank. The Government is in the process of finalizing draft legislation to deal with money laundering and terrorist financing. There are three draft laws under discussion: a law to prohibit money laundering and to provide for measures to combat money laundering; a law to give effect to the UN International Convention for the Suppression of the Financing of Terrorism; and a financial transaction reporting law modeled on those in the Commonwealth which will provide, among other things, for the establishment of a financial intelligence unit. There has been a delay in finalizing the legislation as the GSL debates what sort of presumptions to establish with respect to innocence or guilt. Currently, financial transactions relating to terrorism and narcotics are illegal under Central Bank regulations and banking laws.

The definition of money laundering, under the proposed anti-money laundering law covers (as predicate offenses) the offenses under existing and proposed laws on narcotics, terrorism prevention, bribery, firearms, exchange control, transnational organized crime, cyber crimes, child protection and trafficking of persons and any other offense punishable by death or imprisonment of seven years or more. The offense of money laundering involves receiving, possessing, concealing, investing, disposing of, importing, exporting, or dealing in any property or proceeds derived or realized from any unlawful activity covered by the law. Under the sentencing provisions of the proposed anti-money laundering law, persons convicted will be liable for a fine and imprisonment for a period of 5-20 years. Under the sentencing provisions of the proposed counterterrorist financing law, persons convicted will be liable for a fine and imprisonment for a period of 15-20 years. Under the proposed laws, both money laundering and terrorist financing would be extraditable offenses.

Many areas of concern exist with respect to Sri Lanka's current anti-money laundering efforts. The Central Bank continues to allow the operation of bearer certificates of deposits. In July 2003, in order to limit money laundering through bearer certificates, the Central Bank required banks to maintain a

record of purchasers of these certificates. Another area of concern relates to a 2003 tax amnesty, under which Sri Lankan individuals and companies could declare previously undisclosed wealth accrued from any source and receive immunity from a range of taxes. The amnesty was revised recently, so that immunity is now only available with respect to the payment of income tax on relevant funds. Casinos, jewelry shops and dealers in gems are also areas of concern, as there is no law to regulate their operations. Sri Lanka has also become a transit point for illegal migration of Sri Lankans and other Asian nationals to Europe, North America and the Gulf.

Sri Lanka has an indigenous alternative remittance system in the form of informal money transfer operations. Many Sri Lankan migrant workers, mainly in the Middle East, use a hawala-like system to remit their earnings. Various payments out of Sri Lanka are also made using this system. Sri Lankan commercial banks are increasing their presence and services in the Middle East in order to cater to this clientele. Trafficking of drugs generates significant amounts of criminal proceeds, and those proceeds are also readily transported using this system. Drug proceeds are laundered through various methods, including investment in real estate.

Sri Lanka is not considered an offshore financial center. Offshore banking units are allowed to operate as a part of a commercial bank operating in an overseas country in order to facilitate trade finance. They are subject to Central Bank supervision. Bearer shares are not permitted for offshore banks and foreign-owned companies. Sri Lanka has 10 free trade zones, also called export-processing zones, administered by the state- owned Board of Investment (BOI). The free trade zones house export-manufacturing operations. Only companies approved by the BOI are allowed to operate inside the zones. There are no indications that these free trade zones are being used in trade-based money laundering schemes or terrorist financing.

Sri Lanka is a party to the UN International Convention for the Suppression of the Financing of Terrorism and to the 1988 UN Drug Convention. Sri Lanka has signed but not ratified the UN Convention against Transnational Organized Crime. Sri Lanka is a member of the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) working group on Counter-Terrorism and Transnational Crime formed in July 2004. The working group had its first meeting in December 2004 and aims to serve as a platform for regional cooperation to prevent and suppress terrorism and transnational crime.

The Mutual Assistance in Criminal Matters Act of 2002 provides for cooperation in criminal matters with Commonwealth countries. According to the law, additional bilateral agreements on mutual assistance in criminal matters are required for extending provisions of the act to non-Commonwealth countries. Under the proposed law to give effect to the UN International Convention for the Suppression of the Financing of Terrorism, the government is required to co-operate and provide assistance to states party to the Convention with regard to investigations and prosecutions under the law. The Central Bank of Sri Lanka has circulated the list of individuals and entities that have been included on the UNSCR 1267 Sanctions Committee's consolidated list with instructions to identify, freeze and seize terrorist assets. To date, no such assets have been identified.

Terrorist financing is an offense punishable by imprisonment for a period of five to ten year. Regulations under the United Nations Act No. 45 of 1968 provide for the freezing and forfeiture of assets of financiers of terrorism. There is no specific provision in law for the freezing and forfeiture of narcotics-related assets. The trafficking, possessing, importing or exporting of narcotics is punishable by death or life imprisonment under the Poisons, Opium and Dangerous Drugs Ordinance (OPDDO). Draft amendments to OPDDO, and new money laundering and terrorist financing legislation include asset forfeiture and seizure provisions for narcotics related crimes, money laundering and terrorist financing.

The Government of Sri Lanka should act on the three draft laws referred to above and initiate a comprehensive anti-money laundering program that has as its foundation anti-money laundering and

counterterrorist financing laws. The property and proceeds arising out of all serious crime should be included as predicate offenses for money laundering. The practice of permitting bearer certificates of deposit should be terminated. There should be a formalized system of reporting suspicious transactions from financial institutions to a Financial Intelligence Unit (FIU). Casinos should also be made subject to financial intelligence reporting to the FIU. Sri Lanka should devote adequate resources to train police and customs officials to recognize and investigate different forms of money laundering, including alternative remittance systems. Sri Lanka should ratify the UN Convention against Transnational Organized Crime.

St. Kitts and Nevis

The Government of St. Kitts and Nevis (GOSKN) is a federation composed of two islands in the Eastern Caribbean, but each island has the authority to organize its own financial structure. The federation is at major risk for corruption and money laundering, due to the high volume of narcotics-trafficking activity through and around the islands and the presence of known traffickers on the islands. An inadequately regulated economic citizenship program adds to the problem.

Most of the offshore financial activity in the federation is concentrated in Nevis, in which there is one offshore bank (a wholly owned subsidiary of a domestic bank), approximately 15,000 international business companies (IBCs), and 950 trusts. The Nevis domestic structure consists of five domestic banks, four domestic insurance companies (all of which are subsidiaries of St. Kitts companies), and two money remitters. There are also 50 trust and company service providers. In 2003 St. Kitts had four domestic banks, 120 credit unions, four domestic insurance companies, two money remitters, and 15 company service providers. There are also four trusts, one casino, and 450 exempt companies. Applicants may apply as an IBC for an Internet gaming license; however, none were issued in 2003. The GOSKN did not release statistics for 2004. St. Kitts claims to have no Internet gaming operations.

The Proceeds of Crime Act No. 16 of 2000 criminalizes money laundering for serious offenses (defined to include more than drug offenses) and imposes penalties ranging from imprisonment to monetary fines. The Act also overrides secrecy provisions that may have constituted obstacles to the access of administrative and judicial authorities to information with respect to account holders or beneficial owners. Other measures designed to remedy shortcomings in St. Kitts and Nevis' anti-money laundering regime include the Financial Services Commission Act No. 17 of 2000, the Nevis Offshore Banking (Amendment) Ordinance No. 3 of 2000, the Anti-Money Laundering Regulations No. 15 of 2001, the Companies (Amendment) Act No. 14 of 2001, the Anti-Money Laundering (Amendment) Regulations No. 36 of 2001, the Nevis Business Corporation (Amendment) Ordinance No. 3 of 2001, and the Nevis Offshore Banking (Amendment) Ordinance No. 4 of 2001.

A regional stock exchange, common to the members of the Organization of Eastern Caribbean States and supervised by a regional regulator, is located in St. Kitts. The Eastern Caribbean Central Bank has direct responsibility for regulating and supervising the offshore bank in Nevis, as it does for the entire domestic sector of St. Kitts and Nevis (SKN), and for making recommendations regarding approval of offshore bank licenses. The St. Kitts and Nevis Financial Services Commission, with regulators on both islands, regulates non-bank financial institutions for anti-money laundering compliance.

The GOSKN also issued regulations requiring financial institutions to identify their customers, to maintain a record of transactions, to report suspicious transactions, and to establish anti-money laundering training programs. The Financial Services Commission has issued guidance notes on the prevention of money laundering, pursuant to the Anti-Money Laundering Regulations. The Commission's Regulator is authorized to carry out anti-money laundering examinations. The GOSKN has separated the offshore marketing and regulatory functions. In particular, an offshore Marketing and Development Department, separate from the Financial Services Commission, was established in April 2001. Legislation requires certain identifying information to be maintained about bearer

certificates, including the name and address of the bearer of the certificate, as well as its beneficial owner. In addition to these measures, Nevis issued regulations aimed at facilitating the identification of beneficial owners of corporations and corporate shareholders.

The Financial Intelligence Unit Act No. 15 of 2000 authorizes the creation of the Financial Intelligence Unit (FIU). The FIU began operations in 2001 and has a new director, deputy director, and four police officers. The FIU receives, collects, and investigates suspicious activity reports (SARs). The FIU is also charged with liaising with foreign jurisdictions. By November 2003, the FIU had received 77 SARs. No figures were released for 2004. During its first two years of operation the FIU received over 100 SARs and froze over $1.6 million.

Financial Services (Exchange of Information) Regulations were promulgated in 2002. These regulations define the parameters for the exchange of information between domestic regulatory agencies and foreign regulatory agencies. Financial services officials in SKN have been seeking to educate relevant stakeholders as to their responsibilities related to anti-money laundering, using radio, television, newspapers, and seminars. The GOSKN encouraged the founding of an association of compliance officers within relevant financial institutions, and provided training in anti-money laundering to government financial services personnel. In 2003, the Nevis island administration announced plans to strengthen regulatory oversight of service providers.

St. Kitts and Nevis enacted the Anti-Terrorism Act No. 21, effective November 27, 2002. Sections 12 and 15 of the Act criminalize terrorist financing. The Act implements various UN Conventions against terrorism. The GOSKN has some existing controls that apply to alternative remittance systems, but has undertaken no initiatives that apply directly to the potential terrorist misuse of charitable and nonprofit entities. St. Kitts and Nevis circulates lists of terrorists and terrorist entities to all financial institutions. To date, no accounts associated with terrorists or terrorist entities have been found in SKN.

A mutual legal assistance treaty between SVN and the United States entered into force in early 2000. St. Kitts and Nevis is a member of the Caribbean Financial Action Task Force (CFATF) and the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). St. Kitts and Nevis is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism, and on May 21, 2004, ratified the UN Convention against Transnational Organized Crime.

The Government of St. Kitts and Nevis continues to be vulnerable to money laundering and other financial crimes. St. Kitts and Nevis should continue to devote sufficient resources to effectively implement its anti-money laundering regime. Specifically, St. Kitts and Nevis should determine the number of Internet gaming sites present on the islands. Oversight of these entities is crucial, as they are vulnerable to abuse by criminal and terrorist groups. Additionally, St. Kitts and Nevis should curtail its economic citizenship program.

St. Lucia

St. Lucia has developed an offshore financial service center that could potentially make the island more vulnerable to money laundering and other financial crimes.

Currently, St. Lucia has five offshore banks, 1,438 international business companies, 33 international trusts, 17 international insurance companies, two money remitters, three mutual fund administrators, 9 registered agents and 3 registered trustees (service providers) and six domestic banks. St. Lucia has a free trade zone. The Government of St. Lucia (GOSL) also is considering the establishment of gaming enterprises.

The 1993 Proceeds of Crime Act criminalizes money laundering with respect to narcotics. The Proceeds of Crime Act also provides for a voluntary system of reporting account information to the

police or prosecutor when such information may be relevant to an investigation or prosecution. In addition, the Act requires financial institutions to retain information on new accounts and transactions for seven years. In September 2003, legislation was adopted that extends anti-money laundering compliance requirements to credit unions, money remitters and pawnbrokers, as well as strengthens criminal penalties for money laundering.

Many of the 1993 Proceeds of Crime Act provisions are superseded by the 1999 Money Laundering (Prevention) Act (ML Prevention Act), which criminalizes the laundering of proceeds with respect to 15 prescribed offenses, including narcotics-trafficking, corruption, fraud, terrorism, gambling and robbery. The ML Prevention Act mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the ML Prevention Act imposes a duty on financial institutions to take "reasonable measures" to establish the identity of customers, and requires accounts to be maintained in the true name of the holder. It also requires an institution to take reasonable measures to identify the underlying beneficial owner when an agent, trustee or nominee operates an account. These obligations apply to domestic and offshore financial institutions, including credit unions, trust companies, and insurance companies. In April 2000, the Financial Services Supervision Unit issued detailed guidance notes, entitled "Minimum Due Diligence Checks, to be conducted by Registered Agents and Trustees."

Pursuant to the ML Prevention Act, the Money Laundering (Prevention) Authority (the Authority) was established in early 2000. The Authority consists of five persons "who have sound knowledge of the law, banking or finance." The Authority's functions include receipt of suspicious transaction reports, subsequent investigation of the transactions, dissemination of information within (e.g., to the Director of Public Prosecutions) or outside of St. Lucia, and monitoring of compliance with the law. The ML Prevention Act imposes a duty on the Authority to cooperate with competent foreign authorities. Assistance includes the provision of documents, testimony, conduct of examinations, execution of search and seizure orders, and the provision of information and evidentiary items. The Authority has a number of regulatory powers, including the right to enter the premises of a financial institution during normal working hours to inspect transaction records or copy relevant documentation, to issue guidelines to financial institutions, and to instruct a financial institution to facilitate an investigation by the Authority.

In 1999, the GOSL also enacted a comprehensive inventory of offshore legislation, consisting of the International Business Companies (IBC) Act, the Registered Agent and Trustee Licensing Act, the International Trusts Act, the International Insurance Act, the Mutual Funds Act and the International Banks Act. An IBC may be incorporated under the IBC Act. Only a person licensed under the Registered Agent and Trustee Licensing Act as a licensee may apply to the Registrar of IBCs to incorporate and register a company as an IBC. The registration process involves submission of the memorandum and articles of the company by the registered agent, payment of the prescribed fee and the Registrar's determination of compliance with the requirements of the IBC Act. IBCs can be registered online through the GOSL's web page. IBCs intending to engage in banking, insurance or mutual funds business may not be registered without the approval of the Minister responsible for international financial services. An IBC may be struck off the register on the grounds of carrying on business against the public interest.

The Financial Intelligence Authority Act No. 17 of 2002 authorizes the establishment of a Financial Intelligence Unit (FIU) for St. Lucia, which became operational in October 2003. Some functions of the Authority have been transferred to the new FIU. The FIU is able to compel the production of information necessary to investigate possible offenses under the 1993 Proceeds of Crime Act and the ML Prevention Act. Failure to provide information to the FIU is a crime, punishable by a fine or up to ten years imprisonment. The Financial Intelligence Authority Act permits the sharing of information obtained by the FIU with foreign FIUs. The Caribbean Anti-Money Laundering Program (CALP) has trained St. Lucia's FIU personnel. In September 2003, legislation was adopted merging the Authority

with the FIU. In December 2004, the FIU received 25 suspicious transaction reports. There have been no money laundering convictions to date in St. Lucia. However, there is a money laundering case pending.

The GOSL established the Committee on Financial Services in 2001. The Committee, which meets monthly, is designed to safeguard St. Lucia's financial services sector. The Committee is composed of the Minister of Finance, the Attorney General, the Solicitor General, the Director of Public Prosecutions, the Director of Financial Services, the Registrar of Business Companies, the Commissioner of Police, the Deputy Permanent Secretary of the Ministry of Commerce, the police officer in charge of the Special Branch, the Comptroller of Inland Revenue and others. The GOSL announced in 2003 its intention to form an integrated regulatory unit to supervise the onshore and offshore financial institutions the GOSL currently regulates. The Eastern Caribbean Central Bank regulates St. Lucia's domestic banking sector.

Counterterrorism and counterterrorist financing legislation is pending before the St. Lucia Parliament. In 2002, St. Lucia signed the Inter-American Convention Against Terrorism, which includes counterterrorist financing provisions. St. Lucia circulates lists of terrorists and terrorist entities to all financial institutions. To date, no accounts associated with terrorists or terrorist entities have been found in St. Lucia. The GOSL has not taken any specific initiatives focused on the misuse of charitable and nonprofit entities.

As a member of the Caribbean Financial Action Task Force (CFATF), St. Lucia underwent a First Round Mutual Evaluation immediately prior to the establishment of its offshore sector. St. Lucia underwent its Second Round evaluation in September 2003. St. Lucia is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. In February 2000, St. Lucia and the United States brought into force a Mutual Legal Assistance Treaty. St. Lucia also has a Tax Information Exchange Agreement with the United States. The GOSL has been cooperative with the USG in financial crime investigations. St. Lucia is a party to the 1988 UN Drug Convention and, on September 26, 2001, signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. The GOSL has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of St. Lucia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and adopt counterterrorism financing legislation. St. Lucia should continue to enhance and implement its money laundering legislation and programs.

St. Vincent and the Grenadines

St. Vincent and the Grenadines remains vulnerable to money laundering, other financial crimes, and the facilitation of terrorist financing, as a result of the rapid expansion and inadequate regulation of its offshore sector. The offshore sector includes 11 offshore banks, 6,276 international business corporations, 11 offshore insurance companies and 153 international trusts. The domestic sector comprises two commercial banks, a development bank, two savings and loan banks, a building society, 13 insurance companies, 10 credit unions, and two money remitters. There are no free trade zones in St. Vincent and the Grenadines (SVG) nor have any Internet gaming licenses been issued.

The Eastern Caribbean Central Bank (ECCB) supervises SVG's four domestic banks. Beginning in October 2001 with an administrative agreement, and finalized in the International Banks (Amendment) Act No. 30 of 2002, the Government of St. Vincent and the Grenadines (GOSVG) gave the ECCB increasing authority to review and make recommendations regarding approval of offshore bank license applications, and to directly supervise the offshore banks in cooperation with the GOSVG's Offshore Finance Authority (OFA). The agreement includes provisions for joint on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore

banks. The OFA alone continues to supervise and regulate the other offshore sector entities; however, its staff exercises only rudimentary controls over these institutions. The GOSVG has strengthened the structure and staffing of the OFA by appointing five new members to the OFA board. This brings the total to 12 staffers to regulate offshore insurance and mutual funds.

In June 2003, the Financial Action Task Force (FATF) recognized that the GOSVG, through enactment and implementation of appropriate legal reforms, had sufficiently addressed deficiencies identified by the FATF in 2000, and removed it from the list of Non-Cooperative Countries or Territories (NCCT). With SVG's removal from the NCCT list, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) lifted its advisory, which had instructed all U.S. financial institutions to "give enhanced scrutiny" to all transactions involving St. Vincent and the Grenadines. The FATF encouraged the GOSVG to consider tightening provisions relating to the granting of exemptions from customer identification requirements.

Since July 2000, the GOSVG has passed substantial legislation, primarily the International Banks (Amendment) Act No. 7 of 2000 that deals with the authorization and regulation requirements for offshore banks as well as with the rules regarding the transfer of shares and beneficial interest. The GOSVG also enacted the International Banks (Amendment) Act of October 2000, which enables the Offshore Finance Inspector to have access to the name or title of a customer account and any other confidential information about the customer that is in the possession of a licensee. The GOSVG prepared a further amendment to the International Banks Act with a view to improving licensing procedures and better regulating the offshore banking sector.

The GOSVG enacted the Proceeds of Crime and Money Laundering (Prevention) Act in December 2001 and the Proceeds of Crime (Money Laundering) Regulations in January 2002. Subsequent amendments further strengthen provisions of the Act and the Regulations. Among other measures, the Act criminalizes money laundering and imposes on financial institutions and regulated businesses a requirement to report suspicious transactions likely to be related to money laundering or the proceeds of crime. The related regulations establish mandatory record keeping rules and limited customer identification/verification requirements.

The GOSVG enacted the International Business Companies Amendment Act No. 26 of 2002, which became effective on May 27, 2002, to immobilize and register bearer shares. The GOSVG also revoked the Confidentiality Act and passed the Exchange of Information Act No. 29 of 2002 to authorize and facilitate the exchange of information, particularly among regulatory bodies. In April 2001, the GOSVG revoked its economic citizenship program, which provided the legal basis to sell citizenship and passports, although there were no reports of passports having been issued under the program.

The Financial Intelligence Unit Act No. 38 of 2001 (FIU Act) establishes the Financial Intelligence Unit (FIU) that began operation in May 2002. The FIU Act allows for the exchange of information with foreign FIUs. An amendment to the FIU Act permits the sharing of information even at the investigative or intelligence stage. The FIU has a staff of 14 and became a member of the Egmont Group in June 2003. As of October 2004, the FIU had received 88 suspicious activity reports for the year and almost 400 since its inception. In November 2004, the FIU began an anti-money laundering /counterterrorist finance training initiative at the financial institutions.

There have been no money laundering convictions, but the GOSVG has frozen approximately $1.5 million and confiscated approximately $40,000. Officials also cooperated with a U.S. investigation of a major suspected money launderer in 2002. In 2003, the GOSVG reintroduced a customs declaration form to be completed by incoming travelers. Incoming travelers are required to declare currency over approximately $3,800.

The GOSVG enacted the United Nations Terrorism Measures Act No. 34, effective August 2, 2002. Sections 3 and 4 of the Act criminalize terrorist financing. The GOSVG has not undertaken any specific initiatives focused on the misuse of charitable and nonprofit entities. The GOSVG circulates lists of terrorists and terrorist entities to all financial institutions in SVG. To date, no accounts associated with terrorists have been found.

The GOSVG is a member of the Caribbean Financial Action Task Force, and underwent its Second Round mutual evaluation in November 2002. In addition, the GOSVG is a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). The GOSVG is a party to the 1988 UN Drug Convention and acceded to the Inter-American Convention against Corruption in 2001. The GOSVG signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. The GOSVG is a party to the UN International Convention for the Suppression of the Financing of Terrorism and is deemed to be partially compliant with its requirements. An updated extradition treaty and a Mutual Legal Assistance Treaty between the United States and the GOSVG entered into force in September 1999. The FIU executes the Mutual Legal Assistance Treaty requests.

The Government of St. Vincent and the Grenadines should address all remaining concerns raised by the international community in regard to its anti-money laundering regime. These include the areas of customer identification, money remitters, outstanding bearer shares, and money laundering prosecutions. St. Vincent and the Grenadines should continue to provide training to its regulatory, law enforcement, and Financial Intelligence Unit personnel in money laundering operations and investigations. St. Vincent and the Grenadines also should ensure that it properly supervises the offshore sector. St. Vincent and the Grenadines should pass counterterrorist financing legislation that will provide the authority to identify, freeze and seize terrorist assets.

Suriname

Suriname is not a regional financial center. Narcotics-related money laundering occurs primarily through unregulated private sector activities, specifically casinos, gold mining and car dealerships. Narcotics-related money laundering is closely linked to transnational criminal activity related to the transshipment of Colombian cocaine and is believed to occur through both the non-banking financial system (i.e., money exchange businesses or cambios) and through a variety of other means including, but not limited to, the sale of gold purchased with illicit money and the manipulation of commercial and state-controlled bank accounts. Both local drug-trafficking organizations and organized crime are believed to control the money laundering proceeds. Suriname does not have an offshore sector nor free trade zones.

Although Suriname's overall anti-money laundering regime still remains weak, it made significant progress in 2004. A package of anti-money laundering legislation passed in 2002 by the Government of Suriname (GOS) is based on recommendations made by the Caribbean Financial Action Task Force (CFATF). This legislation addresses multiple issues including (a) criminalizing money laundering, (b) establishing a Financial Intelligence Unit (FIU) to track and report on unusual and suspicious financial transactions, and (c) requiring financial service providers to store information on clients for seven years and to confirm the identities of clients, individual or corporate, before completing requested financial services. The legislation includes a due diligence section making individual bankers responsible if their institution is laundering money, and ensures the protection of bankers and others with respect to their cooperation with law enforcement officials. The law, "Reporting of Unusual Transactions," enacted in September 2002, entered into force in March 2003. This law requires financial institutions, other intermediaries and natural legal persons who conduct financial services to report suspicious financial transactions to the FIU.

In addition, there is an amendment to the criminal code allowing authorities to confiscate illegally obtained proceeds and assets obtained partly or completely through criminal offenses. There are no provisions for civil forfeiture, and there is no legal mechanism that designates the proceeds gained by the sale of forfeited goods to be used directly for law enforcement efforts.

The Central Bank issued guidelines for the prevention of money laundering in 1996 that contain a definition of a suspicious transaction as any transaction that deviates from the usual account and customer activities and that are not "normal" daily banking business. These guidelines are not mandatory.

The FIU opened an office in early 2003, and personnel received extensive training in 2004. The FIU, which falls under the auspices of the Attorney General's office, is tasked with identifying, recording and reporting the identity of customers engaging in suspicious financial transactions. After an initial rough start, when the head of the FIU resigned effective January 2004 after less than six months in office, the FIU is making progress under a new director.

Suriname's financial regime was challenged in early 2004 by a currency change which dropped three zeros from the currency and changed the name from the Surinamese Guilder to the Surinamese Dollar. Anticipating problems, the Central Bank required that suspicious transactions be reported/investigated. The FIU, however, did not detect any suspicious transactions from commercial banks related to the exploitation of the change in currency. The FIU, however, did not receive information from currency exchange cambios.

Suriname's money laundering regime was further enhanced in 2004 with the establishment of a Financial Investigation Team (FOT) within the Attorney General's office. The FOT is responsible for investigating suspicious transactions discovered by the FIU. The results of the investigation are then sent to the police and prosecutor's office to be used as prosecutorial evidence. In November a Surinamese judge convicted a money laundering suspect for the first time in a landmark court case, marking the first successful implementation of Suriname's 2002 anti-money laundering law. Both the FIU and FOT were instrumental in providing sufficient evidence to ensure a conviction. The suspect, whose country of origin is unknown, received a seven-year prison sentence for intentional money laundering and attempting to export a small amount of cocaine.

Resource constraints and in particular a severe shortage of judges will be a limiting factor in expanding this judicial success. A new class of nine judges, in training, will partially redress the problem, but they will not complete training for another four to five years.

The GOS has not criminalized terrorist financing. However, GOS officials are working with the Caribbean Anti-Money Laundering Program to draft legislation requiring transparency in the financial sector that would contain specific provisions for terrorist financing.

The GOS has an agreement with the Netherlands on extradition and legal assistance with regard to criminal matters, but extradition of Surinamese nationals is prohibited. Suriname also has bilateral treaties and cooperation agreements with the United States, on narcotics-trafficking, and with Colombia, France and Netherlands Antilles on transnational organized crime. Suriname is a member of the CFATF and the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). Suriname is party to the 1988 UN Drug Convention and signed the Inter American Convention against Terrorism in June 2002, but has not yet ratified it.

The Government of Suriname should continue its efforts to fully implement its anti-money laundering legislation, particularly through expansion of the Financial Intelligence Unit (FIU) and Financial Investigation Team (FOT) and further training of personnel. Suriname should criminalize terrorist financing and become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Swaziland

Swaziland is a growing regional financial center. International narcotics-trafficking, primarily in marijuana, continues to grow in Swaziland. The country's proximity to South Africa, lack of effective counternarcotics legislation, limited enforcement resources, relatively open society and developed economic infrastructure make it attractive for trafficking organizations and increase the risk for money laundering.

The Central Bank of Swaziland and the Ministry of Finance are currently drafting an amendment to the Money laundering Act of 2001 (the Act). Although the Act criminalizes money laundering for specified predicate offenses, including narcotics-trafficking, kidnapping, counterfeiting, extortion, fraud, and arms trafficking, it does not adequately address processes and procedures for the police to follow when money laundering is suspected. The penalty for money laundering is six years imprisonment, a fine amounting to roughly $3,500, or both. The Act establishes a currency reporting requirement, requires banks to report suspicious transactions to the Central Bank, and provides conditions when assets may be frozen and forfeited. The Act also requires banks to retain records for five years, to improve the ability to trace suspicious transactions and patterns.

On November 16, 2004, the Central Bank of Swaziland and the Bankers Association of Swaziland issued a general statement on anti-money laundering regarding the importance of positive identification in banking. The statement says that Swaziland's financial institutions will not conduct transactions with any customers failing to furnish proof of their identity and that service shall not be provided when there is any reason to suspect that money laundering may be involved. By June 30, 2005, all existing customers of Swaziland's financial institutions will need to present current information to establish their actual identity.

To assist the banking community with tracking suspicious transactions, the Central Bank distributed anti-money laundering guidelines to all banks in late 2002. As of December 2004, the Central Bank received fewer than 10 reports of suspicious transactions. The police bear responsibility for investigating such cases, but no investigations have taken place—one reason the Central Bank and the Ministry of Finance are amending the 2001 Act. The police also would be responsible for seizing any assets related to money laundering, but no seizures have taken place under the Act.

Members of the Royal Swaziland Police Service (RSPS) have noted that they lack the ability to understand and monitor small businesses. The RSPS has little liaison or cooperation with those ministries of the Government of the Kingdom of Swaziland (GKOS) involved with regulating businesses and business owners. Their expressed concerns in this arena include a perceived escalation in the number of foreign business owners throughout Swaziland. While the RSPS is becoming aware that businesses, such as used car lots, cellular and electronic shops, and sundries stores, are commonly used throughout the world as fronts and/or laundering mechanisms, the RSPS lacks the inter-departmental infrastructure and agreements to address this growing concern. Simply stated, the small business sector in Swaziland has been traditionally overlooked as a very real potential money laundering and support element for drug traffickers and terrorist groups. More inter-departmental and inter-ministerial cooperation is needed in order to properly assess and address this vulnerability.

The Act allows for providing assistance to foreign countries that have entered into mutual assistance treaties with the GKOS. An amendment to the Act will allow for Swaziland to comply with regional agreements and international conventions.

Swaziland is party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GKOS has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Swaziland is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. Swaziland served as President of ESAAMLG from August 2002 to August 2003.

The Government of the Kingdom of the Swaziland (GKOS) should criminalize terrorist financing. Swaziland should also establish an anti-money laundering regime consistent with international standards, including a financial intelligence unit capable of sharing information with foreign law enforcement and regulatory officials. The Kingdom of the Swaziland should provide the appropriate resources and training to its law enforcement personnel to allow them to adequately perform their duties.

Sweden

Sweden does not appear to have a significant money laundering problem. Swedish anti-money laundering legislation includes all serious crimes, and the money laundering controls allow Sweden to fulfill the recommendations of the Hague Forfeiture Convention. The 2004 Transparency International Corruption Perception Index lists Sweden as the sixth (perceived) least corrupt country. Sweden relies on transparency of institutions to keep corruption at bay; however the focus on corruption has been increasing over the past few years. In January of 2004, two Swedish consultants were convicted of bribing foreign public officials at the World Bank. The court's decision has been appealed, but this decision marks the first bribery case of a foreign public official ruled on in a Swedish court.

Among the Nordic countries, Sweden has the highest number of money laundering reports. One reason is that Sweden, in comparison with other Nordic countries, has more currency exchange offices, which appear to be the preferred mechanism for money laundering. Other financial institutions, such as postal giro companies, are also used to launder money. A new trend identified by the Financial Police concerns large cash withdrawals by entrepreneurs on the illegal labor market, especially in the construction and cleaning business sectors. The money primarily emanates from narcotics, tax fraud, economic crimes and robbery.

Swedish law requires banks, credit market companies, securities businesses, exchange offices, remittance dealers, insurance brokers, life insurance companies, and casinos to report suspicious activity to the police Financial Intelligence Unit (FIU). The law also requires financial institutions, insurance companies, securities firms, currency exchange houses, providers of electronic money, and money transfer companies to verify customer identification, inquire into a transaction's background, and verify identities for each transaction, particularly in the case of new customers and involving amounts above SEK 110,000 (approximately $16,300). Banks and financial institutions are obliged to observe and report to the police transactions that are suspected to include funds that will be used to finance serious crimes. Swedish law does not allow individual officers of covered institutions to be penalized for noncompliance; however, the Swedish Supervisory Authority has the ability to sanction noncompliant institutions.

Sweden implemented new regulations to further comply with the 1991 European Union (EU) Directive on Money Laundering approved in 2001. According to the new regulations the FIU is entitled to demand customer information from accounting firms; law firms; tax counselors; casinos; real estate brokers; dealers in antiques, jewelry, and art; companies buying and selling new and used vehicles; and firms dealing with gambling and the sale of lottery tickets. The new regulation came into effect on January 1, 2005.

Sweden's FIU received 4,155 suspicious transaction reports in 2001, a 60 percent increase from 2000 due to the implementation of the EU's Anti-Money Laundering Directive through Swedish law, which requires bureaux de change to report suspicious activity. The FIU received 8,008 suspicious transaction reports in 2002, 10,000 reports in 2003, and 9,929 reports in 2004. The Financial Police believe that increase in suspicious activity is attributed to Baltic countries' entrance into the EU.

The number of prosecutions in Sweden has been relatively low. In 2003, only four cases were brought to trial and resulted in conviction. During 2004, the number was similar. Suspected money laundering

in Sweden requires a full investigation of the initial crimes to fully establish the origin of the money. This has proven to be a difficult and resource-consuming effort, which results in fewer prosecutions. The law on money laundering stipulates six months to two years in prison. The average time in prison for perpetrators convicted of money laundering is around one year.

Sweden ratified the International Convention for the Suppression of the Financing of Terrorism on June 6, 2002, and on July 1, 2002, a new act on penalties for financing serious crimes entered into force. According to the act, it is a punishable crime to collect, provide, or receive money or other funds with the intention that they be used, or with the knowledge that they are to be used, to commit actions that constitute offenses under the international counterterrorism conventions. Attempts to commit such crimes are also punishable. Sweden has had two cases under this law but neither went to trial. One reason was that the actual amount involved was too low to prosecute. Another reason related to difficulties in prosecuting under the law. The prosecutor has to be able to prove intent to fund not only a particular organization, but also the intent to fund a terrorist activity. Three Swedish citizens were put on the terrorist list by the U.S., and then approved by the UN and later also by the EU, since they had connections to the bank al-Barakhaat. Two have been taken off the list but the third, Ahmed Yusuf, is still on the list.

Swedish law also provides for the seizure of assets derived from drug-related activity, however, it is not possible to stop a transaction based solely on suspicions of unlawful activity. Law enforcement officials may only seize the assets of an organization or individual that is the subject of an ongoing criminal investigation. Freezing of assets based on UN Security Council Resolutions is carried out by implementation of EC law. UN and international sanctions can be imposed through the 1995 Sanctions Act, however, the Swedish government does not have the authority to identify potential sources of terrorist financing and to disrupt them on its own without a decision by the EU or UN.

Sweden has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision." Sweden is a member of the Financial Action Task Force (FATF), serving as the Chair for 2004, and the Council of Europe. Its FIU is a member of the Egmont Group. Sweden is a party to the 1988 UN Drug Convention and on April 30, 2004, ratified the UN Convention against Transnational Organized Crime. It is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Sweden has signed, but not yet ratified, the UN Convention against Corruption.

The Government of Sweden should continue to expand its anti-money laundering/counterterrorist financing regime. Sweden should adopt reporting requirements for the cross-border transportation of currency or monetary instruments. Sweden should ensure that legislation is enacted to extend suspicious transaction reporting requirements to intermediaries, such as attorneys, accountants, and financial advisors and to ease the difficulties proving and prosecuting the crime of money laundering.

Switzerland

Switzerland is a major international financial center, with some 370 banks maintaining headquarters there. In addition, approximately 12,000 to 15,000 fiduciaries function as non-bank financial institutions. Narcotics-related money laundering proceeds are largely controlled by foreign drug-trafficking organizations. Authorities suspect that Switzerland is vulnerable at the layering and integration stages. Switzerland's central geographic location; relative political, social, and monetary stability; wide range and sophistication of available financial services; and long tradition of bank secrecy are all factors that make Switzerland a major international financial center. These same factors make Switzerland attractive to potential money launderers. However, Swiss authorities are aware of this and are sensitive to the size of the Swiss private banking industry relative to the size of the economy, and waive bank secrecy rules in the prosecution of money laundering and other criminal

cases. Deposits in Swiss institutions represent an estimated $2.9 trillion, with foreigners accounting for over half of the input into the financial system; this amount is 12 times the GDP of the country.

Reporting indicates that criminals attempt to launder proceeds in Switzerland from a wide range of illegal activities conducted worldwide, particularly narcotics-trafficking and corruption. Switzerland's extensive market in fine arts is also used to launder money. Although both Swiss and foreign individuals or entities conduct money laundering activities in Switzerland, narcotics-related money laundering operations are largely controlled by foreign narcotics-trafficking organizations, often from the Balkans or Eastern Europe. For example, some of the money generated by Albanian narcotics-trafficking rings in Switzerland goes to armed Albanian extremists in the Balkans.

Switzerland ranks fifth in the highly profitable artwork trading market. It exported $877 million worth of artwork worldwide in 2003, and another $786 million from January to October 2004. Generating about $951 billion a year in turnover, the Swiss market offers lucrative opportunities for organized crime to transfer stolen art or to use art to launder criminal funds. The United States is by far Switzerland's most important trading partner, and purchased $442 million of "Swiss" works of art in 2003, and $332 million from January to October 2004. Because art works, which may have been smuggled into Switzerland, can legally be re-exported as genuine Swiss artwork after five years, the Swiss art market is especially attractive for unethical transactions.

Switzerland has duty free zones. The Customs authorities supervise the admission into and the removal from customs warehouses. Warehoused goods may only undergo manipulations necessary for their maintenance, or such as repacking, splitting, sorting, mixing, sampling and removal of the external packaging. Any further manipulation is subject to authorization. Goods may not be manufactured in the duty free zones. Swiss law has full force in the duty free zones, for example, export laws on strategic goods, war material, and medicinal products, as well as laws relating to anti-money laundering prohibitions, etc. all apply. In view of the fact that Customs may and frequently does enter any customs warehouse area they choose, they believe they would be aware of the nature of any "value added" activity taking place in duty free zones.

In December 2001, the Swiss Federal Council (Cabinet) agreed to consider expanding the scope of the 1998 federal anti-money laundering (AML) law to include art and jewelry dealers. The revised AML bill will be discussed in January 2005 in the context of the Financial Action Task Force (FATF) Forty Recommendations. In the meantime, AML regulations have been extended to cover art dealers to the extent that they are acting specifically as "financial intermediaries" between a seller and a buyer.

Additionally, on June 17, 2003, the parliament adopted a bill on the transfer of cultural goods, which regulates the return of looted cultural objects. The new legislation, which is expected to come into force by April 2005, extends the timeframe from the current five years to meet the UN International Standards of 30 years, as defined in the 71970 UNESCO Convention. It also will enable police forces to search bonded warehouses and art galleries.

Money laundering is a criminal offense. Switzerland has significant AML legislation in place, making banks and other financial intermediaries subject to strict know your customer and reporting requirements. Switzerland has also implemented legislation for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets. Legislation that aligns the Swiss supervisory arrangements with the Basel Committee's "Core Principles for Effective Banking Supervision" is contained in the Swiss Money Laundering Act.

The current money laundering laws and regulations have been extended to non-bank financial institutions. Consequently, all non-bank financial intermediaries are required to either join an accredited self-regulatory organization (SRO), or come under the direct supervision of the Money Laundering Control Authority (MLCA) of the Federal Finance Department. The MLCA was formed in 1998 to oversee anti-money laundering laws in the non-banking sector. The SROs must be

independent of the management of the intermediaries they supervise and must enforce compliance with due diligence obligations. Noncompliance can result in a fine or a revoked license. About 7,000 fiduciaries operate in this previously unregulated arena. The MLCA has shown willingness to take action against financial intermediaries: in 2003, the MLCA ordered the official liquidation of five financial intermediaries and the removal from the commercial register of two others, because they failed to comply with AML regulations. Reporting regulations on international money transactions, applicable to money transmitters in particular, have been tightened as well.

In December 2002, the new money laundering ordinances of the Swiss Federal Banking Commission were adopted; these became effective on July 1, 2003. These new regulations, aimed at the banking and securities industries, codify a risk-based approach to suspicious transaction and client identification and install a global know your customer (KYC) risk management program for all banks, including those with branches and subsidiaries abroad. In the case of higher-risk business relationships, additional investigation by the financial intermediary is required. The changes also require increased due diligence in the cases of politically exposed persons by ensuring that decisions to commence relationships with such persons be undertaken by the senior executive body of a firm. Additionally, the ordinance mandates computer-based transaction monitoring systems for all but the smallest financial intermediaries. All cross-border wire transfers must contain details about the funds remitters. The provisions of the ordinance also address Swiss supervision of subsidiaries belonging to a consolidated group of financial intermediaries (for which information channels must be established). All provisions apply to correspondent banking relationships as well. Shell banks-banks with no physical presence at their place of incorporation-may not maintain any correspondent bank accounts.

In October 2003, the Swiss Cabinet mandated an interdepartmental working group led by the Ministry of Finance to review Switzerland's compliance with the revised FATF Forty Recommendations. In December 2003, the MLCA effected a new money laundering ordinance which implements the revised Recommendations. The FATF is expected to review implementation by early 2005.

In July 2003, the government-sponsored Zimmerli Commission, charged by the Finance Ministry with examining reform of finance market regulators, presented 46 recommendations. Most notably, the Committee recommended merging the Federal Banking Commission and the Federal Office for Private Insurance, or the banking and insurance sectors, into a single, integrated financial market supervision body, to be known as FINMA. In November 2004, the Cabinet instructed the Finance Ministry to draft a parliamentary bill providing for the establishment of the FINMA. Under the Cabinet's proposal, the MLCA would also be included within the FINMA. The draft bill is scheduled for submission to Parliament by the end of 2005. The proposed changes are extremely far-reaching

In June 2004, the Cabinet submitted draft legislation to Parliament on auditing reform. The draft revision more tightly delineates the duties of auditing firms of large corporations and strengthens provisions on auditors' independence to prevent conflicts of interest. The draft legislation also provides for a public monitoring body of auditors to ensure that only sufficiently qualified experts perform auditing services.

Switzerland's banking industry offers the same account services for both residents and nonresidents. These can be opened through various intermediaries who advertise their services. As part of Switzerland's international financial services, banks offer certain well-regulated offshore services, including permitting nonresidents to form offshore companies to conduct business, which can be used for tax reduction purposes.

The Swiss Commercial Law does not recognize any offshore mechanism per se and its provisions apply equally to residents and nonresidents. The stock company and the limited liability company are two standard forms of incorporation offered by Swiss Commercial Law. The financial intermediary is required to verify the identity of the beneficial owner of the stock company and must also be informed

of any change regarding the beneficial owner. Bearer shares may be issued by stock companies but not by limited liability companies.

Swiss casino operators have joined counterparts from Greece, Austria, Finland, Spain, Portugal, and the United Kingdom to form a new Casino Operators' Association. Among the stated priorities for the group are addressing anti-money laundering issues and responsible gaming practices.

The Money Laundering Reporting Office Switzerland (MROS) is Switzerland's Financial Intelligence Unit (FIU). All financial intermediaries (banks, insurers, fund managers, currency exchange houses, securities brokers, etc.) are legally obliged to establish customer identity when forming a business relationship. They also must notify the MROS, or a government authorized supervisory body, if a transaction appears suspicious. In March 2004, MROS released figures for the previous year: In 2003, money laundering cases rose 32 percent over 2002 figures, with more than 860 reports of suspicious transactions (STRs) worth approximately $460 million. As in 2002, the majority of reports came from the non-banking sector, probably due to the stricter reporting regulations directed at non-banking financial intermediaries. However, while the percentage of STRs coming from banks has decreased, the actual number of STRs from the banks has continued to increase.

The Government of Switzerland has made it a key foreign policy goal to correct the country's image as a haven for illicit banking services. The Swiss believe that their system of self-regulation, which incorporates a "culture of cooperation" between regulators and banks, equals or exceeds that of other countries. The primary interest of the Swiss system is to avert bad risks by countering them at the account-opening phase, where due diligence and KYC address the issues, rather than relying on an early-warning system on all filed transactions. The Convention on Due Diligence is very comprehensive, requiring the identification of the client and the beneficial owner, who needs to be a physical person. Because of the due diligence approach the Swiss have taken, there are fewer STRs filed than in other countries, but the ones that are filed lead to the opening of criminal investigations 75 percent of the time. In January 2003, Switzerland won a battle when the European Union backed away from demands that Switzerland scrap banking secrecy. Despite the measures that Switzerland has taken, it is likely to endure more criticism from other countries for its continued banking secrecy laws and its refusal to look upon tax evasion as a crime.

The banking community cooperates with enforcement efforts. The Oversight Commission of the Swiss Bankers Association fined Credit Suisse for inadequate due diligence in connection with a total of $214 million deposited in the bank by former Nigerian dictator Sani Abacha. Swiss press reports put the fine at $500,000 (SFr. 750,000 at the time), making it the largest fine ever imposed by the Commission. The recipient of the fine will be the International Red Cross Committee, a Swiss organization.

Under the 2002 Efficiency Bill, the Swiss Attorney General is vested with the power to prosecute crimes addressed by Article 340bis of the Swiss Penal Code, which also covers money laundering offenses. Formerly, the individual cantons were charged with investigating money laundering offenses on their own. Additional legislation, effective January 1, 2002, increased the effectiveness of the prosecution of organized crime, money laundering, corruption, and other white-collar crime, by increasing the personnel and financing of the criminal police section of the federal police office. The law confers on the federal police and Attorney General's office the authority to take over cases that have international dimensions, involve several cantons, or which deal with money laundering, organized crime, corruption, and white collar crime.

If financial institutions determine that assets were derived from criminal activity, the assets must be frozen immediately until a prosecutor decides on further action. Under Swiss law, suspect assets may be frozen for up to five days while a prosecutor investigates the suspicious activity. Switzerland cooperates with the United States to trace and seize assets, and has shared a large amount of funds

seized with the U.S. Government (USG) and other governments. The Government of Switzerland has worked closely with the USG on numerous money laundering cases.

In addition, legislation permits "spontaneous transmittal"-allowing the Swiss investigating magistrate to signal to foreign law enforcement authorities the existence of evidence in Switzerland. The Swiss used this provision in 2001 to signal Peru that they had uncovered accounts linked to former Peruvian presidential advisor Vladimiro Montesinos. On March 31, 2003, the Swiss Federal Court rejected an appeal by Raul Salinas, brother of a former president of Mexico and main suspect in a major money laundering affair, to release millions of dollars blocked on 10 different Swiss bank accounts. In December 2004, Swiss judicial authorities handed over to Argentinean authorities banking information, in the context of criminal investigations, against former Defense Minister Oscar Camilion and former Air Force chief Juan Paulik. Camilion was forced to resign in June 1996.

During 2002, the Swiss Federal Council presented a bill to the Nationalrat, Switzerland's lower house, that addresses a number of terrorism issues surrounding ratification of the UN terrorism conventions. This bill includes a provision on terrorist financing that introduces criminal liability for legal persons involved in terrorism financing. The Swiss House was scheduled to consider it in the first half of 2003. The amended Swiss penal code makes terrorism financing a predicate offense for money laundering. Changes in the Criminal Code in 2003 also make terrorism financing a predicate offense in money laundering, and expand the scope of application to legal persons.

The ordinances adopted in December 2002 also include new rules against terrorism financing, stating that instruments currently used to prevent money laundering are also applicable to the prevention of terrorism financing; if a financial intermediary investigates the background of an unusual or suspicious transaction, and linkages with a terrorist organization are revealed, the institution must report the matter to the FIU immediately.

Since September 11, 2001, Swiss authorities have been alerting Swiss banks and non-bank financial intermediaries to check their records and accounts against lists of persons and entities with links to terrorism. The accounts of these individuals and entities are to be reported to the Ministry of Justice as suspicious transactions. Based on the "State Security" clause of the Swiss Constitution, the authorities have ordered banks and other financial institutions to freeze assets of organizations and individuals designated by the UNSCR 1267 Sanctions Committee. In the 2003 reporting period, MROS received reports of five cases possibly linked to the funding of terrorism. The total amount of money involved was $115,000. All the reports involved individuals and institutions appearing on the USG lists. The five reports were transmitted to the Swiss Attorney General in Berne.

Along with USG and UN lists, the Swiss Economic and Finance Ministries have drawn up their own list of approximately 44 individuals and entities connected with international terrorism or its financing. Swiss authorities have thus far blocked about 82 accounts totaling $25 million from individuals or companies linked to Usama Bin Ladin and al-Qaida under UN resolutions. The Swiss Attorney General also separately froze 41 accounts representing about $25 million, on the grounds that they were related to terrorism financing, but the extent to which these funds overlap with the UN lists has yet to be determined. In January 2003, the Swiss Ministry of Justice handed over banking information to U.S. authorities, following a legal assistance request issued in April 2002. The request related to a bank transfer of $1.4 million, addressed to the Benevolence International Foundation, a Chicago-based Islamic foundation designated as a terrorist financier. The transfer originated from a Swiss bank account whose account holder was a company located in the Virgin Islands. The firm had initially lodged a complaint against this decision to the supreme Swiss federal court but was turned down in November 2002.

Switzerland has ratified the Council of Europe (COE) Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Switzerland has signed, but not yet ratified, the UN

Convention against Transnational Organized Crime and the UN Convention against Corruption. To date, Switzerland has not ratified the 1988 UN Drug Convention.

Swiss authorities cooperate with counterpart bodies from other countries. Requests for cooperation with Liechtenstein, Switzerland's closest neighbor both culturally and geographically, have tripled. Switzerland has a Mutual Legal Assistance Treaty in place with the United States, and Swiss law allows authorities to furnish information to U.S. regulatory agencies, provided it is kept confidential and used for supervisory purposes. The U.S.-Swiss extradition treaty permits extradition for any unlawful act punishable by imprisonment in both countries. Switzerland is a member of the FATF, the Egmont Group and the Basel Committee on Banking Supervision.

The Government of Switzerland should extend its anti-money laundering program to include dealers in high-end goods. Switzerland can also continue to improve on its anti-money laundering regime, as it has been doing, and address deficiencies that it finds, as well as continuing to work toward full implementation of its anti-money laundering/counterterrorist financing regime.

Syria

Due to its relatively undeveloped banking sector, Syria is not a likely center for money laundering via the formal financial sector. From the time that private banks were nationalized in the early 1960s, and prior to last year, Syria's entire financial system was owned and operated by the state. However, in January 2004, private banks began operating in Syria. Currently three private banks are open for business. The existing public banks remain inefficient and highly regulated, and focus almost exclusively on financing public enterprises. Until late 2004, several foreign banks had been operating in Syrian duty-free zones without direct supervision by the Government of Syria (SARG). The SARG, however, recently began applying banking controls and regulatory oversight to these banks.

The U.S. Department of State designated Syria as a State Sponsor of Terrorism in 1979. In May 2004, the U.S. Department of the Treasury designated the Commercial Bank of Syria (CBS), along with its subsidiary, the Syrian Lebanese Commercial Bank, as a financial institution of "primary money laundering concern," pursuant to Section 311 of the USA Patriot Act. This designation remains in place, but the final rulemaking on the implementation of the special measure against CBS has not been issued, pending further discussions between the U.S. Government and the Government of Syria (SARG). In September 2004, U.S. and Syrian officials met to discuss deficiencies in SARG banking regulations. The U.S. Government later suggested remedial actions that Syria could take to conform to international banking standards, particularly those outlined in the recommendations of the Financial Action Task Force (FATF).

The Government of Syria strictly controls foreign currency flows out of the country, contributing to the use of alternative and "informal" systems of moving money or transferring value. Syrian businessmen usually depend on banks in neighboring Lebanon and Jordan to transact a full range of banking services. The private sector routinely uses foreign currency to finance imports, generally by using letters of credit from Lebanon and Europe. Due to foreign exchange controls, the private sector also has restricted access to foreign currency. Illicit proceeds from the narcotics trade may flow through Syria, but they are usually moved to Lebanon for laundering purposes. As a result, the primary money laundering vulnerability in Syria is not necessarily through financial institutions but through alternative remittance systems such as hawala, trade-based money laundering, and currency smuggling. Such money laundering methodologies are often used to finance terrorism throughout the region and elsewhere. The opening of private banks is a positive development in terms of modernization of Syria's financial sector, but at the same time it makes the banking system increasingly vulnerable to money laundering, at least until such time as the SARG completes the implementation of measures to facilitate its oversight of financial transactions.

Due to a distrust of public banks, strict currency restrictions, and displeasure with the official exchange rate, most Syrians prefer to utilize informal banking systems to transfer currency into, around, and out of Syria, sometimes by physically moving cash via Syrian bus and shipping companies with offices in the region. Relatives, friends and colleagues often provide a similar service using foreign bank accounts, particularly in Lebanon. In instances where no relative or friend is available and/or the amount to be transferred is too high, a few money changers, well known to the business community and operating with tacit SARG approval, also provide a means of depositing hard currency in overseas accounts. These mechanisms are a form of hawala.

The government-controlled banking system in Syria consists of the Central Bank of Syria and five public banks, each specializing in one aspect of economic activity: the Commercial Bank of Syria, the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank. These banks have in the past employed a rigid interest rate structure that discourages savings deposits, particularly during periods of inflation. Until January 2004, when the first private banks opened, only the Commercial Bank of Syria was been permitted to provide commercial banking services. As the sole legal trader of foreign currencies, the Commercial Bank also effectively controlled all legal foreign trade and all foreign currency transactions.

In addition to monopolizing the exchange of foreign currencies, the SARG maintains one of the last remaining fixed, multiple exchange rate systems in the world, employing different rates depending on the nature of the transaction. There are reports that the SARG may take steps toward eliminating the multiple exchange rate system in 2005. Until it is changed, however, this inefficient system contributes to the use of alternative methods of transferring value outside the state-controlled banking system. There are reports that such transactions occur with the tacit approval, if not involvement, of SARG officials. A large percentage of Lebanon's banking services involve Syrian accounts.

In April 2001, Law No. 28 legalized private banking. That same month, Law No. 29 established rules on bank secrecy. The first private banks opened in January 2004, but the services they provide are limited under current governmental regulations. Much still needs to be done to fundamentally restructure the banking sector, particularly in terms of either suspending or amending existing regulations that prohibit the three established private banks from operating fully. The SARG continues to work on detailed regulations that will govern the operation of private banks. These private banks must have a 51 percent Syrian ownership (individual or consortium), while non-Syrian banks interested in investing in this new financial sector often finance the other 49 percent.

In September 2003, Syria passed Legislative Decree No. 59, criminalizing money laundering and creating an Anti-Money Laundering Commission. While this was an important movement in principle toward addressing vulnerabilities in the banking sector, particularly the new vulnerabilities arising from the opening of private banks, it is not yet clear what relationship the commission will have with financial institutions or whether the commission will hold effective investigative powers. In December 2004, the SARG prohibited private bank representation on the Anti-Money Laundering Commission, in order to ease conflict-of-interest concerns.

Syria is a party to the 1988 UN Drug Convention. It is also in the process of becoming a party to the UN International Convention for the Suppression of the Financing of Terrorism. It signed the UN Convention against Transnational Organized Crime (in 2000), but has not yet ratified it. Syria is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004. The MENAFATF is a FATF-style regional body. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors.

The Government of Syria should immediately stop all support of terrorist organizations. It should continue to implement comprehensive anti-money laundering and counterterrorism finance legislation that adheres to international standards, including the creation of an independent Financial Intelligence

Unit (FIU). Syria should then take meaningful steps to enforce the law and follow-up rules and regulations governing the banking sector. Syria should ratify both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Taiwan

Taiwan's modern financial sector and its role as a hub for international trade make it attractive to money laundering. Its location astride international shipping lanes makes it vulnerable to transnational crimes such as narcotics-trafficking and smuggling. The use of alternative remittance systems or "underground banking" is a money laundering vulnerability. There is a significant volume of informal financial activity through unregulated non-bank channels. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes linked to SARs include financial crimes, corruption, narcotics, and other general crimes, in that order.

Taiwan's anti-money laundering legislation is embodied in the Money Laundering Control Act (MLCA) of April 23, 1997. Its major provisions include a list of predicate offenses for money laundering, customer identification and record keeping requirements, disclosure of suspicious transactions, international cooperation, and the creation of a financial intelligence unit, the Money Laundering Prevention Center (MLPC).

The Legislative Yuan amended the MLCA in 2003 to expand the list of predicate crimes for money laundering, widen the range of institutions subject to suspicious transaction reporting, and mandate compulsory reporting of significant currency transactions of over New Taiwan (NT)$1 million (approximately $30,000) to the MLPC. Between August 2003, when the amended MLCA came into force, and May 31, 2004, the MLPC received over one million such reports on currency transactions—with 99 percent of them reported electronically. Also as a result of the amendments, the list of institutions subject to reporting requirements was expanded, to include casinos, automobile dealers, jewelers, boat and plane dealers, real estate brokers, credit cooperatives, consulting companies, insurance companies, and securities dealers, as well as traditional financial institutions.

The time limit for reporting cash transactions of over NT$1 million is within five business days. Banks were also barred from informing customers that a suspicious transaction report had been filed. In addition, two new articles were added to the MLCA, granting prosecutors and judges the power to freeze assets related to suspicious transactions, and giving law enforcement more powers related to asset forfeiture and the sharing of confiscated assets. In terms of reporting requirements, financial institutions are required to identify, record, and report the identities of customers engaging in significant or suspicious transactions. There is no threshold amount specified for filing suspicious transaction reports. Reports of suspicious transactions must be submitted to the MLPC within 10 business days after the transaction took place.

Institutions are also required to maintain records necessary to reconstruct significant transactions, for an adequate amount of time. Bank secrecy laws are overridden by anti-money laundering legislation, allowing the MPLC to access all relevant financial account information. Financial institutions are held responsible if they do not report suspicious transactions. In May 2004, the Ministry of Finance also required banks to demand two types of identification and to keep copies when bank accounts are opened upon request for a third party, in order to prove the true identity of the account holder. Individual bankers can be fined NT$200,000-1 million ($6,000-30,000) for not following the MLPA.

All foreign financial institutions and offshore banking units follow the same regulations as domestic financial entities. Offshore banks, international businesses, and shell companies must comply with the disclosure regulations from the Central Bank, Bureau of Monetary Affairs (BOMA), and MLPC.

These supervisory agencies conduct background checks on applicants for banking and business licenses. Offshore casinos and Internet gambling sites are illegal.

From January to September 2004, Taiwan investigated 505 cases of possible money laundering. Among these cases, 442 were economic crimes, seven involved government corruption, and seven were narcotics-related crimes. Total money laundering during this period amounted to NT$1.244 billion (about $38 million). Of the 505 cases investigated, 287 involved money laundering via bank transactions, 213 involved postal remittances and savings banks, and one case involved a credit union.

Individuals are required to report currency transported into or out of Taiwan in excess of NT$60,000 (approximately $1,765), $5,000, or $5,000 worth of foreign currency. Starting in March 2004, over 6,000 Chinese renminbi ($725) must also be reported. When foreign currency in excess of NT$500,000 (approximately $14,700) is brought into or out of Taiwan, the bank customer is required to report the transfer to the Central Bank, though there is no requirement for Central Bank approval prior to the transaction. Prior approval is required, however, for exchanges between New Taiwan dollars and foreign exchange when the amount exceeds $5 million for an individual resident and $50 million for a corporate entity.

Starting in September 2003, the Directorate General of Customs was responsible for providing the MLPC on a monthly basis with electronic records of travelers entering and exiting the country carrying any single foreign currency amounting to NT$1.5 million. Among the 542 cases reported between September 2003 and June 2004, the center said it had found several cases that might involve illegal underground banking activities, and these were under investigation.

The authorities on Taiwan are actively involved in countering the financing of terrorism. In 2003, a new "Counter-Terrorism Action Law" (CTAL) was drafted, although as of January 2005 it is still pending legislative approval. The new law would explicitly designate the financing of terrorism as a major crime. Under the proposed CTAL, the National Police Administration, the MJIB, and the Coast Guard would be able to seize terrorist assets even without a criminal case in Taiwan. Also, in emergency situations, law enforcement agencies would be able to freeze assets for three days without a court order.

Assets and income obtained from terrorist-related crimes could also be permanently confiscated under the CTAL, unless the assets could be identified as belonging to victims of the crimes. Taiwan officials currently have the authority to freeze and/or seize terrorist-related financial assets under the MLCA promulgated in 1996 and amended in February 2003 to cover terrorist finance activities. Under the Act, the prosecutor in a criminal case can initiate freezing assets, or without criminal charges, the freezing/seizure can be done in response to a request made under a treaty or international agreement.

The Bureau of Monetary Affairs (BOMA) has circulated to all domestic and foreign financial institutions in Taiwan the names of individuals and entities included on the UNSCR 1267 Sanctions Committee's consolidated list. Taiwan and the United States have established procedures to exchange records concerning suspicious terrorist financial activities. After receiving financial terrorist lists from the American Institute in Taiwan, BOMA conveys the list to relevant financial institutions.

Banks are required to file a report on cash remittances if the remitter/remittee is on a terrorist list. In accordance with UN Security Council Resolution 1373, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism. identified to date. In 2004, there was one suspected terrorist finance case reported. Subsequent investigation determined that the suspect was not a terrorist or a financier of terrorism.

Alternative remittance systems, or underground banks, are considered to be operating in violation of Banking Law Article 29. Authorities on Taiwan consider these entities to be unregulated financial institutions. Foreign labor employment brokers are authorized to use banks to remit income earned by foreign workers to their home countries. These remittances are not regulated or reported. Thus, money

laundering regulations are not imposed on these foreign labor employment brokers. However, if the brokers accept money in Taiwan dollars for delivery overseas in another currency, they are violating Taiwan law.

It is also illegal for small shops to accept money in Taiwan dollars and remit it overseas. Violators are subject to a maximum of three years in prison, and/or forfeiture of the remittance and/or a fine equal to the remittance amount. Authorities on Taiwan do not believe that charitable and nonprofit organizations in Taiwan are being used as conduits for the financing of terrorism, and there are currently no plans to investigate such entities further for terrorist financing. Such organizations are already required to register with the government.

Taiwan's only free trade zone began operation in Keelung on October 1, 2004. Entities wanting to operate in the free trade zones must submit applications to the port authorities. Entities can conduct simple processing of commodities in the zone and re-export them without inspection by customs. There is no indication that the zone is used in money laundering schemes or by financiers of terrorism. Keelung port authority has a panel composed of members from various enforcement agencies to conduct checks of commodities, transportation, and accounting. According to Taiwan's Banking Law and Securities Trading Law, in order for financial institutions to conduct foreign currency operations, Taiwan's Central Bank must first approve the institution to for this function. The financial institutions must then submit an application to port authorities to establish an offshore banking unit in the free-trade zone.

Taiwan has established drug-related asset seizure and forfeiture regulations, which state that according to treaties or agreements, Taiwan's Ministry of Justice shall share seized assets with foreign official agencies, private institutions or international parties which provide Taiwan with assistance in investigations or enforcement. Assets of drug traffickers, including instruments of crime and intangible property, can be seized along with legitimate businesses used to launder money. The injured parties can be compensated with seized assets. The Ministry of Justice distributes other seized assets to the prosecutor's office, police or other anti-money laundering agencies. The law does not allow for civil forfeiture. In January-September 2004, total seized assets reached NT$20 million (about $660,000).

A mutual legal assistance agreement between the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO) entered into force in March 2002. It provides a basis for the law enforcement agencies of the territories represented by AIT and TECRO to cooperate in investigations and prosecutions for narcotics-trafficking, money laundering (including the financing of terrorism), and other financial crimes.

Although Taiwan is not a UN member and cannot be a party to the 1988 UN Drug Convention, the authorities on Taiwan have passed and implemented laws in compliance with the goals and objectives of the Convention. Similarly, Taiwan cannot be a party to the UN International Convention for the Suppression of the Financing of Terrorism, as a nonmember of the United Nations, but it has agreed unilaterally to abide by its provisions. Taiwan is a founding member of the Asia/Pacific Group on Money Laundering (APG) and actively participates in the Group's meetings. The MLPC is a member of the Egmont Group. In 2003, thirty-six information exchanges took place between Taiwan and international counterparts, including the United States, related to money laundering investigations.

Over the past five years, Taiwan has created and implemented an anti-money laundering regime that comports with international standards. The MLCA amendments of 2003 address a number of vulnerabilities, especially in the area of asset forfeiture. The authorities on Taiwan should continue to strengthen the existing anti-money laundering regime as they implement the new measures. Taiwan should endeavor to pass the proposed Counter-Terrorism Action Law to better address terrorist financing issues. The authorities on Taiwan should also enact legislation that would promulgate regulations regarding alternate remittance systems.

Tajikistan

Tajikistan is not a major financial center in the region and does not have a developed banking system. Prosecutions for financial criminal activity are unusual, although the ringleaders of the Ponzi bead-scheme that defrauded hundreds of people out of tens of thousands of dollars in 2003 were convicted in 2004 and sentenced to terms ranging from eight to twenty years. Tajikistan is not an offshore center, but offshore zones are often used while concluding deals with foreign enterprises. Foreign banks operate in the country, including an Iranian bank.

Domestic goods smuggling is a concern in Tajikistan. Consumer goods, mostly apparel and low-cost household appliances, are smuggled to avoid customs duties and local taxes. In most cases, goods such as tobacco, alcohol, and fuel are not "officially" imported to Tajikistan. For example, a shipment transiting Tajikistan intended for Kazakhstan or Afghanistan never reaches the destination country. While there is certainly a market for smuggled goods, there is little evidence that most items are financed with narcotics money, with the exception of imported cars and other luxury items.

The Tajik Criminal Code of May 21, 1998, Art. 574-Legalization (laundering) of Illegally Obtained Income prohibits money laundering. This prohibition includes not only narcotics money laundering, but also circumvention of other financial currency controls (for example, removal of currency into the offshore zone, unlawful usage of a charity, insurance companies, etc.).

The Law on Banking Activity of May 23, 1998 (No.648 AMOPT NO. 10, 1998)-Art. 32 addresses banking secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement authorities for domestic and offshore financial services companies. While the Government of Tajikistan (GOT) has not yet addressed the problem of international transportation of illegally sourced currency and monetary instruments, and has a long way to go to meet "due diligence" standards, it has instituted cross-border currency reporting requirements. Travelers may depart with a maximum amount of $2,000 without any certifying document. When amounts exceed $2,000, an authorized exchange office issues a certificate of transaction for purchase of currency (USD), a.k.a. "form 377," and then the head office (bank) issues a "Ruhsatnoma"—permission to take the cash out of the country. Travelers may enter Tajikistan with unlimited quantities.

Banks are not required to know, record, or report the identity of customers engaging in significant transactions unless criminal proceedings have been undertaken against a specific individual or organization. Some civil proceedings can also trigger this scrutiny. For example, in civil or administrative proceedings, a court can request information about accounts or the nature and value of property kept in bank safes, or request information which is considered to be a "bank secret" in cases when the bank's client represents one of the sides in the proceedings, if asset forfeiture can be applied, or in inheritance cases. Banks and other financial institutions also are not required to maintain records to reconstruct activity. Financial institutions make no regular reports of transactions or other activity, and reporting officers have no special legal protections with respect to cooperating with law enforcement. There is no legal mechanism to insure law enforcement's access to the information related to illegal financial operations.

Money laundering controls are applied to all financial institutions, including exchange offices, brokerages, etc., that are licensed by the National Bank and subject to the same laws as banks. There have been no arrests or prosecutions for money laundering or terrorist financing since January 1, 2002.

Although negotiations are underway for developing an asset seizure program, the GOT does not currently have any asset-seizure mechanisms. The main barriers to implementing such a program are corruption and the underdeveloped legal system. The GOT passed Criminal Code, Art. 57, stating that asset forfeiture is possible but also specified exceptions. A program is being developed to allow the Drug Control Agency to use this law as one means of achieving self-sustainability.

The Tajiks used asset forfeiture procedures in the case of former Commander of the Presidential Guard General Gaffor Mirzoev, who was arrested in August this year and charged with a number of crimes: illegal storage of weapons, murder, illegal commercial activity, illegal appropriation of state property and its use for personal benefit. In November, the Supreme Economic Court passed a resolution to transfer Dushanbe Meat Processing Plant, Entertainment Complex "Jomi Jamshed," and the shop "Kooperator" located in Kulyob from Mirzoev's Company "Mirzoi Rahmon" to the jurisdiction of the Tajik State Committee for Management of State-owned Property, after the Prosecutor General's Office established that these entities had been privatized illegally.

The GOT has criminalized terrorist financing, as covered by the above-mentioned general money laundering statute. Terrorist finance is considered to be a "serious crime." There were no reported cases of suspected terrorist assets being frozen in 2004 because no known terrorist assets were discovered.

Several laws have been adopted, e.g.: Civil Code, Art. 284—Illegal Transactions with Precious Metals, Gems and Gold—to address the misuse of gold, precious metals and gems. The GOT has not addressed alternative remittance systems. Remittances from labor migrants are mainly from Russia and other NIS countries, and are seasonal. The GOT has waived a 30 percent fee on bank transfers, making remittances sent via banks more effective.

Tajikistan and the U.S. Government have not yet reached an agreement for a mechanism for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious criminal investigations, and no negotiations are currently underway. However, the U.S. Government regularly sends information regarding designated individuals and organizations subject to asset forfeiture to the Tajik Ministry of Foreign Affairs (MFA). The MFA distributes this information to the Ministries of Security, Finance, and Interior, and other governmental structures, which conduct appropriate checks. The GOT has not adopted laws or regulations that ensure the availability of adequate records in connection with narcotics, terrorism, terrorist financing or other investigations. Two GOT officials participated in the Roundtable Conference on legislative reforms to combat money laundering and terrorist financing, in Tashkent, Uzbekistan, in July 2004.

Despite a primitive banking system and the use of a barter system in many rural areas, Tajikistan signed the CIS Agreement on the Legal Assistance and Cooperation on Civil, Family and Criminal Cases of January 22, 1993, and is a member of the CIS Counterterrorism Center. The GOT signed the UN International Convention for the Suppression of the Financing of Terrorism in November 2001, but has not yet ratified it. Tajikistan is a party to the UN Convention against Transnational Organized Crime and a charter member of the new Eurasian Group on Combating Money Laundering and Financing of Terrorism, a FATF Style Regional Body established in October 2004.

The Government of Tajikistan should enact and implement anti-money laundering and counterterrorist financing legislation that comports with international standards. Additionally, mechanisms to share information among financial institutions, regulatory authorities and law enforcement entities should be developed to promote the successful prosecution of financial crime cases. Tajikistan should ratify the UN International Convention for the Suppression of the Financing of Terrorism.

Tanzania

Tanzania is not considered an important regional financial center, but is vulnerable to money laundering because of the weaknesses of its financial institutions and law enforcement capabilities. A weak financial sector and an under-trained, under-funded law enforcement apparatus make such crimes difficult to track and prosecute. Officials have noted that some real estate and used car businesses are used for money laundering purposes. Government officials have also cited the emerging

casino industry as an area of concern for money laundering. Money laundering is more likely to occur in the informal non-bank financial sector, as the formal sector is still relatively undeveloped. The prevalence of hawala and the threat of terrorist organizations on the unregulated island of Zanzibar make Zanzibar an area of concern. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash smuggling. The most likely sources of illicit funds include Asia and the Middle East, and to a lesser extent Europe. Such transactions rarely include significant amounts of U.S. currency.

The Proceeds of Crime Act of 1991 criminalizes narcotics-related money laundering. However, the Act does not adequately define money laundering, and it has only been used to prosecute corruption cases. The law obliges financial institutions to maintain records of financial transactions exceeding 100,000 shillings (approximately $109) for a period of 10 years. If the institution has reasonable grounds to believe that a transaction relates to money laundering, it may communicate this information to the police for investigation, although such reporting is not required. The Central Bank has issued regulations requiring financial institutions to file suspicious transaction reports (STRs), but this requirement is not being enforced, and no mechanism exists for receiving and analyzing the STRs. Financial institution employees are legally protected from liability stemming from reporting suspicious transactions. Current law does not hold financial institutions responsible if they are found to have been used to launder money.

The 2002 Prevention of Terrorism Act criminalizes terrorist financing. It also requires all financial institutions to inform the government each quarter as to whether any of their assets or transactions may be associated with a terrorist group, although the implementing regulations for this provision have not yet been drafted. Under the Act, the government may seize assets associated with terrorist groups. The Bank of Tanzania (the Central Bank) circulates to Tanzanian financial institutions the list of individuals and entities on the UNSCR 1267 Sanction Committee's consolidated list, but to date no assets have been frozen under this provision. The Government of Tanzania (GOT) did take action in 2004 against one charitable organization on the list by closing its offices and deporting its foreign directors. However, it is not clear whether Tanzania has the investigative capacity to identify and seize related assets. Tanzania has cooperated with the United States in investigating and combating terrorism. Tanzanian officials have consistently cooperated in the exchange of counterterrorism information with U.S. authorities.

The GOT became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2003. Tanzania is a party to the 1988 UN Drug Convention and has signed the UN Convention against Transnational Organized Crime. Tanzania is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), which was founded in 1999. The GOT continues to play a leading role in the operation of this FATF-style regional body and has detailed personnel to the ESAAMLG Secretariat, located in donated office space in Dar es Salaam. Tanzania also continues to host the ESAAMLG task force meetings held each March.

In line with Tanzania's commitment to supporting the ESAAMLG, Tanzania has created a multi-disciplinary committee on money laundering and a drafting committee that has prepared new anti-money laundering legislation. A Tanzanian Ministry of Finance official stated in August 2004 that the drafting committee was in the process of receiving comments on the language of its bill from stakeholders, and that the bill would likely be presented to the Parliament in January 2005. The proposed legislation provides for the creation of a Financial Intelligence Unit (FIU) that will collect mandatory suspicious transaction reporting from financial institutions, and will be empowered to share this information with other FIUs and foreign law enforcement agencies.

The Government of Tanzania should maintain the momentum towards enacting its anti-money laundering law. It should continue to work through Southern African Anti-Money Laundering Group

(ESAAMLG) to establish a Financial Intelligence Unit (FIU) and develop a comprehensive anti-money laundering regime that comports with international standards.

Thailand

Thailand is vulnerable to money laundering as a result of a significant underground economy and cross-border crime problems with illicit narcotics, contraband, and smuggling. Thailand continues to remain vulnerable to money launderers. Money laundering occurs in both the banking and non-banking systems. Over the last decade, there has been a considerable decrease in the amount of heroin produced in the Golden Triangle region of Burma, Laos, and Thailand. However, drug traffickers still use Thailand's banking system to hide and move their proceeds. It is a key destination, transit and source country for organized international migrant smuggling and trafficking in persons. Thailand is a major production and distribution center for counterfeit goods of all types, including the production and sale of fraudulent travel documents. The underground banking system is widely used for money laundering. Illegal gambling, prostitution, and underground lotteries are a significant part of Thailand's sizeable underground economy. There is a black market for smuggled goods for the purpose of evading customs duties. With the acceleration in economic growth, tax evasion has reportedly increased, and significant financial and securities fraud has been reported. Public sector corruption, particularly in criminal justice institutions, remains a major problem. Thailand experienced an increase in financial crimes in 2004.

Thailand's anti-money laundering legislation, the Anti-Money Laundering Act (AMLA) B.E. 2542 (1999), criminalizes money laundering for the following predicate offenses: narcotics-trafficking, trafficking in women or children for sexual purposes, fraud, financial institution fraud, public corruption, customs evasion, extortion, and blackmail. It also provided for the establishment of an Anti-Money Laundering Office (AMLO). On August 11, 2003, as permitted by the Thai constitution, the Royal Thai Government (RTG) issued two Emergency Decrees to enact measures related to terrorist financing, that had been under consideration by the Executive Branch and Parliament for over a year and a half. The first of these Decrees amended Section 135 of the Penal Code to establish terrorism as a criminal offense. The second Decree amended Section 3 of the AMLA to add the newly established offense of terrorism as an eighth predicate offense for money laundering. The Decrees took effect when they were published. Parliament endorsed their status as legal acts in April 2004. The current list of predicate offenses in the AMLA does not comport with international best practices, as provided in Recommendations 1 and 2 of the Forty Recommendations of the Financial Action Task Force (June 2003), to apply the crime of money laundering to all serious offenses or with the minimum list of acceptable designated categories of offenses. Additionally, the definition of "property involved in an offense" in the AMLA is limited to proceeds of predicate offenses and does not extend to instrumentalities of a predicate offense or a money laundering offense.

The AMLA requires customer identification, record keeping, the reporting of large and suspicious transactions, and provides for the civil forfeiture of property involved in a money laundering offense. Financial institutions are also required to keep customer identification and specific transaction records for a period of five years from the date the account was closed, or from the date the transaction occurred, whichever is longer. Reporting individuals (banks and others) that cooperate with law enforcement entities are protected. Thailand does not have secrecy laws that prevent disclosure of client and ownership information of bank accounts to supervisors and law enforcement authorities. The AMLA gives the anti-money laundering office the authority to compel a financial institution to disclose such information.

In early 2004, the Thai cabinet approved amendments to the AMLA to create an asset forfeiture fund, authorize asset sharing, and add the following additional predicate offenses: weapons smuggling, illegal gambling, government procurement fraud, crimes affecting natural resources and the

environment, intellectual property rights infringement, and Money Exchange Control Act violations. These amendments have been under consideration by the Council of State and are expected to be submitted to the Parliament in early 2005. Active consideration is being given to adding eight additional predicate offenses to the anti-money laundering statute, to include offenses related to natural resources, currency exchange, stock market manipulation, gambling, firearms, conspiracy in awarding government contracts, labor fraud, and tax evasion. Since October 27, 2000, there have been 68 convictions under the AMLA. Cases are proceeding for civil forfeiture against property involved in drug trafficking, prostitution, public fraud and embezzlement, customs evasion, and corruption offenses.

The Bank of Thailand regulates financial institutions in Thailand, but bank examiners are prohibited, except under limited circumstances, from examining the financial transactions of a private individual. This prohibition acts as an impediment to the BOT's auditing of a financial institution's compliance with the AMLA or BOT regulations. Besides this lack of power to conduct transactional testing, BOT does not currently examine its financial institutions for anti-money laundering compliance. The BOT is working closely with AMLO and had hoped to begin such examinations in 2004. The BOT has now agreed that AMLO should be responsible for on and off site audits for AMLA compliance. The target date for such examinations has now slipped to early 2005.

Financial institutions (such as banks, finance companies, savings cooperatives, etc.), land registration offices, and persons who act as solicitors for investors, are required to report significant cash, property, and suspicious transactions. Reporting requirements for most financial transactions (including purchases of securities and insurance) exceeding two million baht (approximately $52,000), and property transactions exceeding five million baht (approximately $130,000), have been in place since October 2000. However, AMLO has been considering a proposal to lower the threshold for reporting cash transactions to 400,000 baht ($10,500). The proposal is not yet in effect and the likelihood of its adoption is in doubt, since (in early February 2005) the Prime Minister publicly expressed his opposition to it. The AMLO is also drafting amendments requiring gold and jewelry shop owners and used car dealers to report transactions over 400,000 baht ($10,500), and is consulting with private industry, but those amendments have also been opposed by affected industries as too cumbersome and unnecessary, and are under review by the Prime Minister.

The various land offices are also required to report on any transaction involving property of five million baht or greater, or a cash payment of two million baht or greater, for the purchase of real property. The Stock Exchange of Thailand (SET) requires securities dealers to have know-your-customer procedures; however, the SET does not check anti-money laundering compliance during its reviews. The Department of Insurance (DOI) is responsible for the supervision of insurance companies, which are covered under the AMLA definition of a financial institution, but there are no anti-money laundering regulations for the insurance industry. Similarly, the Cooperative Promotion Department (CPD) is responsible for supervision of credit cooperatives, which are required under the Cooperatives Act to register with the CPD. Currently, around 6,000 cooperatives are registered, with approximately 1,348 thrift and credit cooperatives engaged in financial business. Thrift and credit cooperatives are engaged in deposit taking and providing loans to the members, and are covered under the definition of a financial institution, but as with the securities and insurance sectors, there are no anti-money laundering compliance mechanisms currently in place.

Licenses were first granted to Thai and foreign financial institutions to establish Bangkok International Banking Facilities (BIBFs), in March 1993. BIBFs may perform a number of financial and investment banking services, but can only raise funds offshore (through deposits and borrowing) for lending in Thailand or offshore. The United Nations Drug Control Program and the World Bank listed BIBFs as potentially vulnerable to money laundering activities, because they serve as transit points for funds. Thailand's 44 BIBFs are now subject to the AMLA.

Thailand acknowledges the existence and use of alternative remittance systems (hawala, etc.) that attempt to circumvent financial institutions. There is a general provision in the AMLA that makes it a crime to transfer, or to receive a transfer, that represents the proceeds of a specified criminal offense (including terrorism). Within the Asia Pacific Economic Council (APEC), Thailand is working with several other countries on a study of alternative remittance systems. Moneychangers frequently act as illegal remittance agents. Remittance agents, including informal remittance businesses, require a license from the Ministry of Finance. Operating a money transfer business also requires a license. The Ministry of Finance issued the Notification to Authorized Persons on July 30, 2004, and to Money Transfer Agents August 4, 2004. The Bank of Thailand issued a Notice to the Competent Officer on the Procedures and Guidelines to operate as Authorized Persons dated August 6, 2004, and to Money Transfer Agent dated August 6, 2004. These new guidelines of BOT and MOF became effective on August 11, 2004. Before the grant of a license, both money changers and money transfer agents are subject to onsite examination by the BOT, which also consults with AMLO on the applicants criminal history and AML record. Licensed agents are also subject to monthly transaction reporting and a 3-year record maintenance requirement. At present, there are about 270 authorized moneychangers and five remittance agents. There is no limitation on the amount of foreign currency that a person can take in or out of Thailand. A customer can transfer an unlimited amount of money through a commercial bank, with the required supporting documentation. At present, moneychangers have to report financial transactions to the Anti-Money Laundering Office (AMLO), while remittance agents do not. As part of the August 6, 2004 notice, the Bank of Thailand limited the annual transaction volume for agents to $60,000 for offices in the Bangkok area and $30,000 for offices located in other areas.

The BOT does not have any regulations that give it explicit authorization to control charitable donations, but it is working with AMLO to monitor these transactions under the Exchange Control Act of 1942. With respect to charities, The Bank of Thailand (BOT) does not have regulation that gives it explicit authorization to control charitable donations. However, the BOT is working with the Anti-Money Laundering Office to monitor these transactions under the Exchange Control Act of 1942.

The AMLA created the Anti-Money Laundering Office (AMLO), which became fully operational in 2001. AMLO is Thailand's Financial Intelligence Unit (FIU). When first established, AMLO reported directly to the Prime Minister. In October 2002, a reorganization of the executive branch took place, and AMLO was designated as an independent agency under the Ministry of Justice. AMLO receives, analyzes, and processes suspicious and large transaction reports, as required by the AMLA. From January through September 2003, the AMLO received 636,129 currency transaction reports and 84,967 suspicious transaction reports.

In addition, the AMLO is responsible for investigating money laundering cases for civil forfeiture purposes and for the custody, management, and disposal of seized and forfeited property. The AMLO is also tasked with providing training to the public and private sectors concerning the provisions of the AMLA. The law also created the Transaction Committee, which operates within AMLO to review and approve disclosure requests to financial institutions and asset restraint/seizure requests. The AMLA also established the Anti-Money Laundering Board, which is comprised of ministerial-level officials and agency heads and serves as an advisory board that meets periodically to set national policy on money laundering issues and to propose relevant ministerial regulations. From October 2003 to October 2004, AMLO filed 362 cases of civil asset forfeiture involving assets worth 3.771 billion baht. Of these, forfeiture judgments have been entered in 152 cases involving 418 million baht. In pursuing its civil forfeiture investigations, AMLO has received valuable cooperation from financial institutions, particularly the commercial banks.

In 2004, the Prime Minister's "Regulations on Payment of Incentives and Rewards in Proceedings Against Assets Under the Anti-Money Laundering Act" went into effect in Thailand. Under this system, investigators from AMLO and other investigative agencies can receive personal payments from the property they seize in money laundering cases. The system that Thailand has created

undermines the integrity of its AML regime and may impede international cooperation. After domestic and international criticism of this system, the Ministry of Justice is considering alternatives to personal commissions from seizures, including the creation of a forfeiture fund for the forfeited proceeds to be dedicated to various programs, rather than personal purposes.

In criminal cases, the forfeiture and seizure of assets is governed by the 1991 Act on Measures for the Suppression of Offenders in an Offense relating to Narcotics ("Assets Forfeiture Law"). The Property Examination Committee has filed 1,865 cases with assets valued at 1.64 billion baht ($4 million) and 1,644 cases are on trial. Two hundred million baht ($5,000,000) have been confiscated and sent to the Narcotics Control Fund.

As part of a general reorganization of the Executive Branch, the Thai Parliament has authorized the establishment in the Ministry of Justice of a new criminal investigative agency, the Department of Special Investigations (DSI), separate from the Royal Thai Police Office. On November 24, 2003, Parliament approved legislation defining DSI's organization, authorities, and responsibilities. The latter include responsibility for investigating the criminal offense of money laundering (as distinct from civil asset forfeiture actions carried out by AMLO), and for many of the money laundering predicates defined by the AMLA, now including terrorism. The DSI, AMLO, and the Royal Thai police all have the authority to identify, freeze, and/or forfeit terrorist finance- related assets.

Thailand is a party to the 1988 UN Drug Convention. In September 2004, Thailand became a party to the UN International Convention for the Suppression of the Financing of Terrorism. It has signed (December 2000), but not yet ratified, the UN Convention against Transnational Organized Crime. It has also signed (December 2003) the UN Convention against Corruption. In April 2005, Thailand will host the 11th United Nations Crime Congress, which will emphasize counterterrorism as one of its principal themes. The RTG has issued instructions to all authorities to comply with UNSCR 1267, including the freezing of funds or financial resources belonging to the Taliban and the al-Qaida network. To date, Thailand has not identified, frozen, and/or seized any assets linked to individuals or entities included on the UNSCR 1267 Sanctions Committee consolidated list. However, AMLO has identified some suspicious transaction reports derived from financial institutions and has initiated cases that may involve terrorist activities using non-governmental or non-profit organizations as a front. Thailand has a Mutual Legal Assistance Treaty (MLAT) with a number of countries, including the United States. It has a memorandum of understanding on law enforcement issues with an additional number of other countries. Thailand became a member of the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body, in April 2001. The AMLO joined the FATF's Egmont Group of financial intelligence units in June 2001.

The Government of Thailand should continue to implement its anti-money laundering program. The BOT and AMLO have agreed that AMLO will be responsible for both offsite and onsite supervision of banks to ensure that Financial Institutions comply with requirements of AMLA and AMLO regulations. Until the RTG provides a viable mechanism for all of its financial institutions to be examined for compliance with the AMLA, Thailand's anti-money laundering regime will not comport with international standards. It is therefore important that BOT/AMLO compliance examinations begin early in 2005 and that other relevant agencies (SET, DOI, and CPD) be working with AMLO to establish policies and procedures for supervisory oversight of AML/CFT compliance. The RTG should develop and implement anti-money laundering regulations for exchange businesses, and should take additional measures to address the vulnerabilities presented by its alternative remittance systems. The RTG to further strengthen its anti-money laundering regime against crime, particularly by expanding its list of predicate offenses to include a broader base of serious financial crimes, such as arms/weapons trafficking, alien smuggling, and environmental crimes, as well as making the "structuring" of transactions a criminal offense. It should extend the law to cover instrumentalities. Thailand should ratify the UN Convention against Transnational Organized Crime. Thailand should also immediately rescind its new rewards program for AMLO investigators who seize assets under the

anti-money laundering laws, and for agents of other agencies that engage in such practices, as it gives the appearance of impropriety, can imperil successful prosecutions, and will eventually impede international cooperation and undermine public support for Thailand's forfeiture regime and its credibility.

Togo

Togo's poor financial infrastructure makes it an unlikely venue for money laundering through its financial institutions. Its porous borders, however, make it a transshipment point in the regional and sub-regional trade in narcotics. Togo's 1998 drug law criminalizes narcotics-related money laundering and penalizes offenses with up to 20 years in prison. However, there have never been any arrests for money laundering. Financial institutions are required to monitor and report monetary transactions above a threshold appropriate to the local economic situation, and must maintain records of such transactions and supply them to government authorities on request. Financial institutions are legally protected in respect to their cooperation with law enforcement authorities. Due diligence legislation applies to bankers and other professionals, although no arrests have been made for violations of this law.

The Government of Togo (GOT) has the legal authority to seize assets associated with narcotics-trafficking. In 2001, President Eyadema created the national Anti-Corruption Commission to combat corruption and money laundering.

Terrorist financing is not a criminal offense in Togo, although draft legislation is pending. The GOT has circulated to Togolese financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. The GOT closely regulates charities and other nongovernmental organizations.

In August 2004, the UN Office of Drug and Crimes (UNODC) and the GOT organized a workshop to review the Togolese penal code. UNODC recommended that Togo either amend the penal code or pass separate laws on terrorism to comply with UN terrorism resolutions.

The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency. All bank deposits over approximately $7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, issued a directive requesting that each member country set up a national committee under their Minister of Finance to deal with financial information as it relates to money laundering. The BCEAO is to be in charge of coordinating such committees. Each member country is now responsible for putting legislation into place to implement this directive, and the legislation is expected to be harmonized regionally.

The WAEMU Council of Ministers issued another directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any person or organization on the UN 1267 Sanctions Committee's consolidated list.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Action Group against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Togo. In July 2002, Togo participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against narcotics-trafficking, terrorism, and money laundering.

Togo is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. On November 27, 2003 Togo signed, but has not yet ratified, the UN Convention against Transnational Organized Crime.

The Government of Togo should criminalize money laundering for all serious crimes, criminalize terrorist financing, and enforce existing laws and regulations.

Tonga

Tonga is an archipelago, located in the South Pacific, about two-thirds of the way from Hawaii to New Zealand. Tourism is the second largest source of hard currency earnings following remittances. Tonga is neither a financial center nor an offshore jurisdiction. An additional source of revenue is the registry of approximately 65 ships from 25 countries, including the United States. Tonga became a party to the UN International Convention for the Suppression of the Financing of Terrorism in December 2002.

The Reserve Bank of Tonga is the primary authority in charge of coordinating the identification of suspicious financial transactions for further investigation. Tonga has not yet established a Financial Intelligence Unit (FIU), however the Reserve Bank is responsible for conducting on site exams of Commercial banks procedures, and training staff members to spot suspicious transactions. Commercial banks are currently required to report suspicious Financial Transaction Reports (FTRs) to the Reserve Bank of Tonga. Since this requirement was instituted in 2002, there have been 5 suspicious transactions referred to the Reserve Bank for further investigation. There have been no prosecutions to date.

Tonga has proposed, but not yet enacted, new legislation to criminalize money laundering and terrorist financing. Cabinet and Parliament will consider amendments to the Money Laundering and Proceeds Act of 2000 in the middle of 2005.

Representatives from Tonga have participated in the Asia/Pacific Group on Money Laundering (APG) anti-money laundering workshops and attended seminars conducted by the Egmont Group. Tonga plans to submit an application to join the APG in 2005. Representatives from Tonga also attended several seminars in Fiji that were related to combating money laundering.

In a 2003 report to the UN Counter-Terrorism Committee, Tonga reported that its Government Committee on Money Laundering and the Financing of Terrorism was working on proposed new legislation and amendments to bring its legislative framework into line with international best practices. Tonga failed to act on that legislation in 2004.

The Government of Tonga should quickly enact legislation that specifically criminalizes money laundering and the financing of terrorism and establishes a Financial Intelligence Unit (FIU). It should follow through with its plan to join the Asia/Pacific Group on Money Laundering. It should also sign and ratify the UN Convention against Transnational Organized Crime.

Trinidad and Tobago

Trinidad and Tobago has a well-developed and modern banking sector that makes it an increasingly significant regional financial center. Trinidad and Tobago (T&T) is not an offshore financial center. Illegal drug-trafficking proceeds are not known to be an important source of laundered funds in T&T, although they are implicated in some money laundering. Criminal proceeds laundered in T&T are derived primarily from domestic criminal activity and from the activity of nationals involved in crime abroad. While there is no significant black market for smuggled goods in T&T, drug money continues to support the importation of illegal arms into the country.

Financial crimes in general are increasing, particularly those involving the use of fraudulent checks and related instruments in the banking sector. Trinidad and Tobago's financial institutions are not

known to engage in current transactions involving international illegal drug-trafficking proceeds that significantly affect the United States.

The Proceeds of Crime Act of 2000 (POCA) expands money laundering predicate offenses to include all serious crimes. The POCA requires financial institutions to proactively report suspicious transactions, and banks and financial institutions are required to maintain records necessary to reconstruct transactions for a number of years. Secrecy laws are limited to standard client confidentiality provisions. Failure to comply with POCA's record keeping and reporting requirements can result in a fine of TT 250,000 (approximately $40,000) and imprisonment for two years for summary conviction, and a fine of TT 3,000,000 (approximately $500,000) and seven years imprisonment for conviction on indictment. Upon summary conviction for money laundering, an offender can be liable for a fine of TT 25,000,000 (approximately $4,000,000) and 25 years imprisonment. Under the POCA, any officer who aids and abets the money laundering activities of an institution can be convicted of money laundering. In addition, the POCA protects individuals who cooperate in money laundering law enforcement investigations. The POCA also enables the courts to seize the proceeds of all serious crimes, although only one property has been seized under the Act.

The Central Bank has set anti-money laundering guidelines, including due diligence provisions that apply to all financial institutions subject to the 1993 Financial Institutions Act. These include banks, finance companies, leasing corporations, merchant banks, mortgage institutions, unit trusts, credit card businesses, financial services businesses and financial intermediaries. In 2004, the Central Bank updated these guidelines, setting new minimum standards for compliance with existing regulations and informing stakeholders on proposed legislation. The Central Bank will bring large credit unions under its supervision by 2005. Also in 2004, the Government of Trinidad and Tobago (GOTT) established a fledgling Tax Fraud Investigations unit in its Inland Revenue Division to address tax evasion and non/underreported income that may have its source from money laundering activities.

GOTT customs regulations require that any sum above approximately $3,000 (in currency or monetary instruments) entering or leaving the country be declared. GOTT Customs may restrain cash above approximately $10,000 for 96 hours, or longer with judicial approval, pending the determination of their legitimate source. The Financial Investigations Unit (FIU) maintains a database of these transactions and analyzes them for evidence of money laundering.

There are six free trade zones in T&T where exporting of services and manufactured products, and re-exportation of manufactured products take place. There is no evidence that these zones are involved in money laundering schemes, and companies operating in these zones are required to submit quarterly tax returns and yearly audited financial statements. These companies must present their bona fides and are subject to background checks prior to being allowed to operate in these zones.

The GOTT has legislation in place that allows it to trace, freeze, and seize assets, including bank accounts. Authorities may also seize legitimate businesses if they are used to launder drug money. However, the GOTT can only restrain assets through due process at the level of the High Court—it cannot freeze assets "without undue delay," and the law only allows for criminal forfeiture of assets, not civil forfeiture.

Since January 1, 2003, the GOTT has conducted 189 financial investigations, and has issued seven production orders and eight foreign intelligence requests. To date, traffickers, organized crime organizations and terrorist organizations have not taken any retaliatory actions related to money laundering/terrorist financing investigations. In 2004, the GOTT charged one person with laundering the proceeds of fraud and seized TT 131,618 (approximately $22,000) in related assets. In previous years, the GOTT seized a total of TT 6 million ($1 million) and restrained TT 1 million (approximately $167,000).

Some legal loopholes exist that allow traffickers and supporters/financiers of terrorists or terrorist organizations to shield their assets. These include the absence of financial obligations regulations and FIU legislation, the ability of attorneys to operate accounts in their client's names, the absence of suspicious transaction reporting (STR) requirements for attorneys and accountants, and legal rules that prevent courts from confiscating assets received after a defendant's sentencing.

Opposition party intransigence has stalled legislation specifically aimed at criminalizing terrorism financing, but Parliament will debate this bill again in 2005. The GOTT is developing regulations for financial sector supervision that acknowledge and monitor alternative remittance systems. The banking system has also reported the suspicious use of charitable or nonprofit entities. The GOTT has circulated the UN 1267 Sanctions Committee's consolidated lists to its financial institutions. The GOTT has also circulated the United States' list of Specially Designated Global Terrorists and other relevant EU lists. There has not yet been any identified evidence of terrorist financing in T&T.

In 1999, a MLAT with the United States entered into force, and in 2000, the United States and GOTT signed a joint statement on law enforcement cooperation, which pledges in part to expand cooperation on the detection and prosecution of money laundering and related criminal activities. While there is no mechanism in place with the United States Government (USG) for the exchange of crime and terrorism-related information, the GOTT has cooperated regularly with the USG and other governments' law enforcement agencies on issues involving drug-trafficking, terrorism, terrorist financing and other criminal investigations. The GOTT does not have legislation that specifically authorizes the sharing of forfeited assets with other countries, but has done so in the past on a case-by-case basis through bilateral agreements.

Trinidad and Tobago is a party to the 1988 UN Drug Convention and the 1992 Kingston Declaration on Money Laundering. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. It has not yet signed the UN International Convention for the Suppression of the Financing of Terrorism. T&T is a member of the Caribbean Financial Action Task Force (CFATF), which is headquartered in Port of Spain. It underwent a second round CFATF mutual evaluation in 2002, and will undergo a third round evaluation in April 2005. Trinidad and Tobago is also a member of the OAS Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD).

The Government of Trinidad and Tobago should continue to work toward full implementation of its anti-money laundering laws and the improvement of its anti-money laundering/counterterrorist financing regime. Trinidad and Tobago should enact suspicious transaction reporting requirements and expand coverage of the laws to include intermediaries, such as attorneys and accountants, and exchange houses. Trinidad and Tobago also should became a party the UN International Convention for the Suppression of the Financing of Terrorism and criminalize terrorist financing.

Tunisia

Tunisia is not considered an important regional financial center due in large part to the very strict control exercised by the Central Bank over all aspects of financial transactions and the general non-convertibility of the Tunisian dinar. There is an offshore financial sector. There is no discernible money laundering activity reported to be occurring in Tunisia through formal financial institutions.

In December 2003, the Tunisian Parliament passed Law No. 2003-75, a comprehensive counterterrorism and anti-money laundering law, to support international counterterrorism efforts and to establish more severe sentences for individuals convicted of terrorist acts. This law makes it a crime to provide financial assistance or any other type of support to terrorist activities, and provides for the freezing of assets. Those suspected of violating the law can be exempted from charges, however, if they report a planned terrorist action to authorities.

Money laundering is punishable where false information is proffered relating to the illicit origin of property or income arising directly or indirectly from an offense. Money laundering also includes investing, depositing, transferring or safekeeping of property or income resulting from an offense. The law imposes obligations on financial institutions relating to identity checks, verification of transactions of suspect persons, record keeping and the declaration of transactions above certain monetary limits. The Ministry of Finance oversees operations to combat money laundering and terrorist financing.

Tunisia's 1992 Law (No. 92-52) against narcotics-trafficking also includes provisions that contribute to the combating of money laundering. Under Articles 2 and 30, anyone aiding in narcotic operations or transfers of proceeds in connection with these operations, including financial institutions, can be punished.

The Tunisian penal code also allows for the sequestering, confiscating, or seizure of assets and property in certain situations, including narcotics-trafficking and terrorist activities. The definition of "assets" is quite broad and could cover any number of financial or physical assets. Financial assets are traced by the Central Bank and the Economic Enforcement Agency, each of which has broad powers for investigating and seizing financial assets. Tunisia has no legal provisions for sharing seized criminal assets with other governments.

Financial institutions are required to gather full identifying information for personal and business accounts. In addition, all supporting documentation must be maintained for 10 years. Only certain categories of individuals and businesses are allowed to open foreign currency or convertible dinar accounts and all of these accounts are monitored by the Central Bank. Because there is no law against money laundering in general, there is no obligation for a financial institution to report suspicious activities or provisions for holding bankers responsible if their institution is used for money laundering. However, the prevailing practice is for institutions to verbally report any unusual activity to the Central Bank, which will notify the investigative Economic Enforcement Agency. There are no "secret" or numbered accounts allowed in Tunisia.

Offshore financial institutions are held to the same regulatory standards as onshore institutions. Offshore institutions undergo the same due diligence process as onshore banks and are licensed only after the Central Bank investigates their references and the Ministry of Finance approves their application. Tunisian law also makes provisions for "moral integrity" checks of major shareholders, directors, and officers of financial institutions at any time doubts may arise. Anonymous directors are not allowed. Tunisia currently has 8 offshore banks. There is foreign participation in over 2,600 Tunisian companies (2003 figures). There are several casinos in Tunisia, but Tunisians are not permitted to use them. The export of Tunisian dinars, by either residents or nonresidents, is strictly prohibited. Bearer financial instruments or shares are prohibited (Act No. 35 of 2000).

Although the Tunisian government maintains that there are no alternative fund transfer systems, since all fund transfers must go through the banks or National Post Office, it is precisely due to these restrictions and currency exchange controls that there are underground methods of moving money or transferring value in and out of the country. While a significant black market in consumer goods does exist in the country, there is no evidence that this trade is funded by illicit proceeds. Residents are generally prohibited from holding or exporting foreign currency except in certain cases (travel or business needs, etc.) Nonresidents entering Tunisia with foreign currency or other instruments are required to declare the total amount if they wish to re-export a portion (not exceeding 1,000 dinar or approximately $840) or deposit any of the money in a Tunisian bank. Nonresidents do not need to declare currency exports under 1,000 dinar. Customs may at any time require declarations for gold or securities.

Tunisia is a founding member of the Middle East North Africa Financial Action Task Force (MENAFATF) based in Bahrain and approved in November 2004 by the governments of Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, Syria, Tunisia,

United Arab Emirates, and Yemen. The MENAFATF is a FATF-style regional body that will address money laundering and terrorist financing related issues and work to raise compliance standards throughout the region to meet international standards.

Tunisia is a party to both the 1988 UN Drug Convention and the 1999 UN International Convention for the Suppression of Financing of Terrorism. It has signed and ratified the UN Convention against Transnational Organized Crime. The Central Bank has circulated the UN 1267 Sanctions Committee's consolidated list to all of its financial institutions. To date no terrorist assets have been identified in Tunisia. Tunisia has varying bilateral agreements on "criminal matters" with 29 countries and is party to 12 international agreements on counterterrorism.

The Government of Tunisia should continue its efforts to implement its comprehensive 2003 legislation. It should establish a Financial Intelligence Unit (FIU) and require financial institutions to report suspicious transactions to that unit.

Turkey

Turkey is an important regional financial center, particularly for Central Asia and the Caucasus, as well as for the Middle East and Eastern Europe. Turkey is not an offshore financial center. It continues to be a major transit route for Southwest Asian opiates moving to Europe. However, local narcotics-trafficking organizations are reportedly responsible for only a small portion of the total funds laundered in Turkey.

A substantial percentage of money laundering that takes place in Turkey appears to involve tax evasion, and informed observers estimate that as much as 50 percent of the economy is unregistered. Since tax evasion is such a large problem, the Government of Turkey (GOT) is in the process of reforming its tax administration, with the goal of improving tax collection. There is no significant black market for smuggled goods in Turkey. There are 21 free trade zones operating in Turkey, but there is no evidence that they are being used in trade-based money laundering schemes or terrorist financing operations. The GOT closely controls access to the free trade zones.

Money laundering takes place in both banks and non-bank financial institutions. Money laundering methods in Turkey include: the cross-border smuggling of currency; bank transfers into and out of the country; and the purchase of high value items such as real estate, gold, and luxury automobiles. It is believed that Turkish-based traffickers transfer money to pay narcotics suppliers in Pakistan and Afghanistan, primarily through Istanbul exchange houses. The exchange houses then wire transfer the funds through Turkish banks to accounts in Dubai and other locations in the United Arab Emirates. The money is then paid, often through alternative remittance systems, to the Pakistani and Afghan traffickers.

Turkey criminalized money laundering in 1996 for a wide range of predicate offenses, including narcotics-related crimes, smuggling of arms and antiquities, terrorism, counterfeiting, and trafficking in human organs and in women. Whoever commits a money laundering offense shall be sentenced to imprisonment from two to five years and is subject to a fine of double the amount of the money laundered and asset forfeiture provisions. The Council of Ministers subsequently passed a set of regulations that require the filing of suspicious transaction reports (STRs), customer identification, and the maintenance of records for five years. These regulations apply to banks and a wide range of non-bank financial institutions, including insurance firms and jewelry dealers.

In 2004, the GOT enacted additional anti-money laundering legislation: a new criminal law and a new criminal procedures law. The new Criminal Law, which will take effect in April 2005, broadly defines money laundering to include all predicate offenses punishable by one year's imprisonment. Previously, Turkey's anti-money laundering law comprised a list of specific predicate offenses. A new

Criminal Procedures Law, which will also come into effect in April 2005, will facilitate asset forfeiture.

In July 2001, the Ministry of Finance issued a banking regulation circular requiring all banks, including the Central Bank, securities companies, and post office banks, to record tax identity information for all customers opening new accounts, applying for checkbooks, or cashing checks. The circular also requires exchange offices to sign contracts with their clients. Additionally, non-interest-utilizing entities such as Islamic financial institutions are required to record tax identity information for all transactions. The Ministry of Finance also issued a circular mandating that a tax identity number be used in all financial transactions as of September 1, 2001. The circular applies to all Turkish banks and to branches of foreign banks operating in Turkey, as well as to other financial entities. The new requirements are intended to increase the Government's ability to track suspicious financial transactions. Turkey does not have secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement officials. According to anti-money laundering law Article 5, public institutions, individuals, and corporate bodies must submit information and documents as well as adequate supporting information upon the request of Turkey's Financial Crimes Investigation Board (MASAK) or other authorities specified in Article 3 of the law. Natural persons and corporate bodies from whom information and documents are requested may not refrain from submitting the requested items by claiming the protection provided by privacy provisions in special laws, provided that the provisions related to the right of defense are reserved.

Generally speaking, Turkey does not have foreign exchange restrictions. However, Turkey does have cross-border currency reporting requirements. Except for payments for imports, invisible transactions and capital exports, banks and special finance institutions must inform authorities, within 30 days, about transfers abroad exceeding $50,000 or its equivalent in foreign currency notes (including transfers from foreign exchange deposits). Travelers may take up to $5,000 or its equivalent in foreign currency notes out of the country.

Since the financial crisis of 2000, the GOT has significantly tightened oversight of the banking system through an independent regulatory authority, the Banking Regulatory and Supervisory Agency (BRSA). BRSA conducts anti-money laundering compliance reviews at banks under authority delegated from MASAK. BRSA's reputation was hurt by its failure to detect a major bank fraud in 2003, but it is working to improve its capabilities in this area.

The 1996 anti-money laundering law establishes MASAK, which is part of the Ministry of Finance. MASAK, which became operational in 1997, serves as Turkey's Financial Intelligence Unit (FIU), receiving, analyzing, and referring STRs for investigation. MASAK has a pivotal role between the financial community, on the one hand, and Turkish law enforcement, investigators, and judiciary, on the other. MASAK itself is not yet functioning at the optimal level of efficiency, and is trying to strengthen its role. It would benefit from additional legal authority, continuity of senior management, training, and computers. Training and equipment needs are being addressed by a European Union accession project, which is expected to end in June 2006. Under current law, MASAK has three functions: regulatory, financial intelligence, and investigative. Under long-pending draft legislation currently under review by relevant GOT agencies, MASAK would cede its investigative function to the public prosecutors, while retaining its regulatory and financial intelligence roles. Passage of the law is expected in early 2005.

The number of STRs being filed is quite low, even taking into consideration the fact that the Turkish economy is cash-based. A possible reason for this is the lack of safe harbor protection for bankers and other filers of STRs. Turkish officials indicated in December 2004 that the GOT has drafted legislation that will provide such protection, but it has not yet been enacted. Another reason is that many bankers do not believe that money laundering occurs through Turkish banks.

Turkey's anti-money laundering regime does not have a strong reputation for enforcement. Since its inception, MASAK has pursued more than 500 money laundering cases, but, as of December 2004, only one had resulted in a conviction-which was later overturned. Factors contributing to this low conviction rate include the fact that Turkey's police, prosecutors, judges, and investigators still need substantial training in dealing with financial crimes, a lack of coordination among law enforcement agencies and a lack of coordination between the courts that prosecute the predicate offenses and the courts that prosecute money laundering cases. Most of the cases involve non-narcotics criminal actions or tax evasion; roughly 30 percent are narcotics related. There were no arrests or prosecutions for money laundering in Turkey in 2004.

Turkey has traditionally taken a strong stance against terrorism, but the GOT still has not explicitly criminalized terrorist financing. The GOT believes that the new draft anti-money laundering law described above and the pending Law to Combat Terrorism should ameliorate the situation, in part by the inclusion of a definition of terrorist financing. In the interim, there are various laws with provisions that can be used to punish the financing of terrorism. In particular, Article 169 of the Turkish Penal Code prohibits assistance in any form to a criminal organization or to any organization which acts to influence public services; media; proceedings of bids, concessions, and licenses; or to gain votes, by using or threatening violence. To commit crimes by implicitly or explicitly intimidating and cowing people is illegal under the provisions of the Law No. 4422 on the Prevention of Benefit-Oriented Criminal Organizations. In February 2002, MASAK issued General Communiqué No. 3, which details a new type of STR to be filed by financial institutions in cases of terrorist financing. The GOT distributes to interested GOT agencies (but not financial institutions) the UNSCR 1267 Sanctions Committee's consolidated list. Financial institutions receive the consolidated list through the Turkish Bankers Association.

Another area of vulnerability in the area of terrorist financing is the GOT's loose supervision of non-profit organizations. The General Director of Foundations (GDF) issues licenses for charities and oversees them. The GDF requires charities to verify and prove their funding sources and to have bylaws. Charities are audited by the GDF and are subject to being shut down if they act outside the bylaws. However, the GOT does not have other oversight mechanisms, such as requiring the publication of annual reports or periodic reporting to competent authorities. In addition, there is no central registry of charities. The GOT has taken no steps to regulate or register alternative remittance systems.

The GOT has the authority to identify and freeze only the assets of individuals and entities on the UNSCR 1267 Sanctions Committee's consolidated list. The Council of Ministers promulgated a decree (2001/2483) on December 22, 2001 to freeze all the funds and financial assets of individuals and organizations included on the UN list. If enacted, the Law on the Fight Against Terrorism would authorize the dissolution of associations, foundations, and unions that are found to have lent support to terror movements. Additionally, their assets would be subject to confiscation. However, the tools currently available under Turkish law for locating, freezing, seizing, and confiscating terrorist assets are cumbersome, limited, and not particularly effective. For example, there is no legal mechanism to freeze the assets of terrorists not on the consolidated list. In the past year, the assets of 241 individuals and organizations have been frozen under the Council of Minister's Decrees on the grounds of being connected to terrorist organizations or terrorist activities. One individual and two organizations were found to have assets in Turkey. All of the funds and assets of these parties have been frozen by relevant GOT authorities.

Turkey also has in place a system for identifying, tracing, freezing, and seizing assets that are not related to terrorism, although Turkish law allows for only criminal forfeiture not for the administrative freezing of assets. The anti-money laundering law, Article 7, provides for the confiscation of all property and assets (including derived income or returns) that are the proceeds of a money laundering predicate offense (soon to be expanded to crimes punishable by one year imprisonment), once the

defendant is convicted. The law allows for the confiscation of the equivalent value of direct proceeds that could not be seized. Instrumentalities of money laundering can be confiscated under the law. In addition to the anti-money laundering law, Article 36 of the Criminal Code provides for post-conviction seizure and confiscation of the proceeds of crimes. The defendant, however, must own the property subject to forfeiture. Legitimate businesses can be seized if used to launder drug money, support terrorist activity, or are otherwise related to other criminal proceeds. Property or its value that is confiscated is transferred to the Treasury.

The government enforces existing drug-related asset seizure and forfeiture laws. MASAK, the Turkish National Police, and the Courts are the government entities responsible for tracing, seizing and freezing assets. According to Article 9 of the anti-money laundering law, the Court of Peace—a minor arbitration court for petty offenses—has the authority to issue an order to freeze funds held in banks and non-bank financial institutions as well as other assets, and to hold the assets in custody during the preliminary investigation. During the trial phase, the presiding court has freezing authority. Public Prosecutors may freeze assets in cases where it is necessary to avoid delay. The Public Prosecutors' Office notifies the Court of Peace about the decision within 24 hours. The Court of Peace has 24 hours to decide whether to approve the action. There is no time limit on freezes. There is no provision in Turkish law for the sharing of seized assets with other countries. The GOT is expected to participate in a meeting in Vienna in January 2005 to prepare a UN model bilateral agreement on the disposal of confiscated proceeds of crime.

The GOT cooperates closely with the United States and with its neighbors in the Southeast Europe Cooperation Initiative (SECI). Turkey and the United States have a Mutual Legal Assistance Treaty (MLAT) and cooperate closely on narcotics and money laundering investigations. However, problems remain in terms of timely information sharing by Turkey with other countries, law enforcement and counterterrorist financing agencies.

Turkey is a member of the Financial Action Task Force (FATF). The MASAK is a member of the Egmont Group. Turkey is a party to the 1988 UN Drug Convention, the UN International Convention for Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Turkey has signed and ratified the COE Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime, and it will come into force on February 1, 2005. Turkey has signed, but not yet ratified, the UN Convention against Corruption. However, implementation efforts on UN anti-financial crime conventions are weak, and Turkey is not believed to be in conformity with the FATF's Special Recommendations on Terrorist Financing. The GOT asserts that legislation being prepared in early 2005 will bring Turkey into conformity with all international counterterrorist financing standards.

The Government of Turkey has publicly declared its commitment to fight money laundering and terrorist financing. However, it needs to strengthen its legislative basis for this by swiftly enacting the draft laws to strengthen MASAK's powers and to criminalize terrorist financing. Turkey should also provide training for its prosecutors, judges, and investigators. Turkey should improve the coordination among the various entities charged with responsibility in its anti-money laundering/counterterrorist financing regime and between the courts, in order to increase successful investigations and convictions for money laundering. Turkey should enact its safe harbor bill to protect the filers of STRs, which may result in increased filings. Turkey should also regulate and investigate alternative remittance networks to thwart misuse by terrorist organizations or their supporters. It should also strengthen its oversight of charities.

Turkmenistan

Turkmenistan is not an important regional financial center; there are only four international banks and a small, underdeveloped financial sector. Foreign companies operate six hotels and casinos in

Turkmenistan. These entities could be vulnerable to financial fraud and used for money laundering. Turkmenistan's national currency, the Turkmen Manat, has an unofficial, but generally accepted, exchange rate that is four times the official rate, creating an environment where money laundering is possible. Turkmenistan has no offshore companies or banks.

The Turkmen Criminal Code of June 12, 1997, Article 242 (Legalization of illegally obtained funds or other property) prohibits money laundering.

Turkmenistan's Law on currency regulations of October 8, 1993, defines general principles for conducting currency operations within the domestic and international accounts of Turkmenistan. It also details authorities and functions of state agencies in currency regulations and management of currency resources, rights and responsibilities of residents and non-residents in regard to ownership, use and handling of hard currency, directions of currency control, and responsibility for violating currency legislation. According to Presidential Decree No. 4715 of June 15, 2000, "Measures to Strengthen Currency Regulations in Turkmenistan," Turkmen ministries, departments, state enterprises and organizations are prohibited from opening bank accounts abroad except as specifically permitted by Turkmen legislation.

Presidential Resolution No. 0210/02-2 of October 17, 1995, gives the Central Bank of Turkmenistan (CBT) authority over all international financial transactions. Under this resolution, any entity making an electronic transfer of funds to an account abroad must provide documentation establishing the source of the money. The CBT regulations also permit an individual to transfer funds abroad of no more than $15,000 every three months. Presidential Decree No. 5976 of November 20, 2002, "Strengthening the Regulations of Turkmen Bank Operations carried out in Foreign Currency," orders Turkmenistan banks to carry out correspondent, deposit, investment and other operations in foreign currency outside Turkmenistan only through open correspondent accounts in the CBT or State Foreign Economic Relations Bank ("Vnesheconombank").

Turkmenistan's tax inspectorate is responsible for uncovering any irregularities. If any irregularities are discovered, the tax inspectorate turns the matter over to Turkmen law enforcement for investigation. To date, no cases have been reported.

The current Law on Free Economic Zones in Turkmenistan adopted in 1993, and amended in 1994, determines the legal regime for conducting business in these zones, guarantees the rights of both foreign and domestic investors, forbids nationalization of enterprises and discrimination against foreign investors, and provides guarantees to foreign investors for exporting production and repatriating after-tax profits. All related enterprises are exempt from taxes on profits for the first three years of profitable operation. All goods and properties must be declared when imported into or exported from free economic zones. There are ten free economic zones in Turkmenistan including: Mary-Bayramali, Okarem-Hazar (Cheleken), Turkmenabat-Seyidi, Baharly-Serdar, Dashoguz Airport, Ashgabat-Anau, Ashgabat-Abadan, Ashgabat International Airport, Serakhs, and Guneshli Turkmenistan near Anau. The first seven zones were created in 1992, and the Serakhs zone was established in 1996. Two more zones, the international airport zone in Ashgabat and the Guneshli Turkmenistan zone near Anau, were created in 1997.

Presidential Decree No. 6097 of January 24, 2003, authorizes the Turkmenistan Supreme Court to open a centralized deposit account at the CBT for receiving payments from illegal enrichment, compensation of material loss or other assets obtained illegally and seized during inspection, investigation, and court trials for all crimes, including: organized crime, drug-trafficking and terrorist financing. The assets will remain in the Supreme Court account until the announcement of the court's final verdict on the case or until another decision is made.

The Turkmenistan Antiterrorism Law of August 15, 2003, authorizes the government to freeze resources and/or other financial assets, deposits, economic resources, and material values of:

individuals who commit or attempt to commit terrorist acts, or contribute to their commitment; organizations directly or indirectly placed under ownership or under control of such individuals; and, individuals and organizations acting on behalf of the above individuals and organizations, including any assets acquired or received through the use of property directly or indirectly belonging to or controlled by such individuals and/or organizations. Turkmen counterterrorism laws require Turkmenistan to cooperate with foreign states and international organizations in terrorism matters and render assistance to other states in criminal investigations and prosecutions of individuals involved in financing or supporting terrorist activities.

The Ministry of Foreign Affairs reports that it distributes information regarding designated individuals and organizations subject to asset forfeiture, provided by the United States, to the Ministry of Finance, the Ministry of National Security, the Ministry of Internal Affairs, and other concerned agencies.

Turkmenistan is a party to the 1988 UN Drug Convention.

The Government of Turkmenistan should enact appropriate legislation and take steps to implement a comprehensive anti-money laundering regime capable of thwarting terrorist financing that conforms to international standards. Turkmenistan should sign and ratify the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Turkmenistan should also consider joining or becoming an observer to the new Eurasian Group on Combating Money Laundering and Financing of Terrorism, a Financial Action Task Force (FATF) Style Regional Body established in October 2004.

Turks and Caicos

The Turks and Caicos Islands (TCI) is a Caribbean overseas territory of the United Kingdom (UK). TCI is comprised of two island groups and forms the southeastern end of the Bahamas archipelago. The U.S. dollar is the currency in use. TCI has a significant offshore center, particularly with regard to insurance and international business companies (IBCs). Its location has made it a transshipment point for narcotics-traffickers. The TCI is vulnerable to money laundering because of a large offshore financial services sector as well as because of bank and corporate secrecy laws and Internet gaming activities. There is no updated information to add for 2004.

As of 2003, the TCI's offshore sector has eight banks (five of which also deal with onshore clientele), approximately 2,500 insurance companies, 1,000 trusts, and 13,000 "exempt companies" that are IBCs, including those formed by the Enron Corporation. The Financial Services Commission (FSC) licenses and supervises banks, trusts, insurance companies, and company managers; it also licenses IBCs and acts as the Company Registry for the TCI. The Financial Services Commission employs a staff of 14 and conducts limited on-site inspections. The FSC became a statutory body under the Financial Services Commission Ordinance 2001 and became operational in March 2002, and now reports directly to the Governor.

The offshore sector offers "shelf company" IBCs, and all IBCs are permitted to issue bearer shares; however, the Companies (Amendment) Ordinance 2001 requires that bearer shares be immobilized by depositing them, along with information on the share owners, with a defined custodian. This applies to all shares issued after enactment and allows for a phase-in period for existing bearer shares of two years. Trust legislation allows establishment of asset protection trusts inoculating assets from civil adjudication by foreign governments; however, the Superintendent of Trustees has investigative powers and may assist overseas regulators.

The 1998 Proceeds of Crime Ordinance criminalizes money laundering related to all crimes and establishes extensive asset forfeiture provisions and "safe harbor" protection for good faith compliance with reporting requirements. The Law also establishes a Money Laundering Reporting Authority (MLRA), chaired by the Attorney General, to receive, analyze, and disseminate financial disclosures

such as suspicious activity reports (SARs). Its members also include the following individuals or their designees: Collector of Customs, the Superintendent of the FSC, the Commissioner of Police, and the Superintendent of the Criminal Investigation Department. The MLRA is authorized to disclose information it receives to domestic law enforcement and foreign governments.

The Proceeds of Crime (Money Laundering) Regulations came into force January 14, 2000. The Money Laundering Regulations place additional requirements on the financial sector such as identification of customers, retention of records for a minimum of five years, training staff on money laundering prevention and detection, and development of internal procedures in order to ensure proper reporting of suspicious transactions. The Money Laundering Regulations apply to banking, insurance, trustees, and mutual funds. Although the customer identification requirements only apply to accounts opened after the Regulations came into force, TCI officials have indicated that banks would be required to conduct due diligence on previously existing accounts by December 2005.

In 1999, the FSC, acting as the secretary for the MLRA, issued non-statutory Guidance Notes to the financial sector, in order to help educate the industry regarding money laundering and the TCI's anti-money laundering requirements. Additionally, it provided practical guidance on recognizing suspicious transactions. The Guidance Notes instruct institutions to send SARs to either the Royal Turks & Caicos Police Force or the FSC. Officials forward all SARS to the Financial Crimes Unit (FCU) of the Royal Turks and Caicos Islands Police Force, which analyzes and investigates financial disclosures. The FCU also acts as TCI's Financial Intelligence Unit (FIU).

As with the other United Kingdom Caribbean overseas territories, the Turks and Caicos underwent an evaluation of its financial regulations in 2000, co-sponsored by the local and British governments. The report noted several deficiencies and the government has moved to address most of them. The report noted the need for improved supervision, which the government acknowledged. An Amendment to the Banking Ordinance was introduced in February 2002 to remedy deficiencies outlined in the report relating to notification of the changes of beneficial owners, and increased access of bank records to the FSC, but the Ordinance has not yet been enacted. No legislation has yet been introduced to remedy the deficiencies noted in the report with respect to the Superintendent's lack of access to the client files of Company Service and Trust providers, nor is there legislation that clarifies how the Internet gaming sector is to be supervised with respect to anti-money laundering compliance.

The TCI cooperates with foreign governments-in particular, the United States and Canada-on law enforcement issues including narcotics-trafficking and money laundering. The FCU also shares information with other law enforcement and regulatory authorities inside and outside of the TCI. The Overseas Regulatory Authority (Assistance) Ordinance 2001, allows the TCI to further assist foreign regulatory agencies. This assistance includes search and seizure powers and the power to compel the production of documents.

The TCI is a member of the Caribbean Financial Action Task Force, and is subject to the 1988 UN Drug Convention. The Mutual Legal Assistance Treaty between the United States and the United Kingdom concerning the Cayman Islands was extended to the TCI in November 1990.

The Government of the Turks and Caicos Islands have put in place a comprehensive system to combat money laundering with the relevant legislative framework and an established FIU. The FSC has made steady progress in developing its regulatory capability and has some experienced senior staff. However, the current regulatory structure is not fully in accordance with international standards. The Turks and Caicos Islands should criminalize the financing of terrorists and terrorism, and enhance its on-site supervision program. Turks and Caicos Islands should expand efforts to cooperate with foreign law enforcement and administrative authorities. Turks and Caicos Islands should provide adequate resources and authorities to provide supervisory oversight of its offshore sector in order to further ensure criminal or terrorist organizations do not abuse the Turks and Caicos Island's financial sector.

Uganda

Uganda is not a regional financial center and is not a major hub for narcotics trafficking or terror finance. Some money laundering occurs in Uganda, It appears that a large percentage of the money laundering occurring in Uganda stems from domestic criminal actions, often related to smuggling counterfeit products, and other financial fraud. Reportedly, large drug-trafficking organizations, organized crime groups, and terror groups have historically not played a leading role in money laundering activities in the country. However, there have been reports during the past year that certain significant figures may be involved in organized international money laundering schemes, possibly related to narcotics trafficking. The Government of Uganda (GOU) does not monitor cross-border financial activities. The GOU has finally begun to draft legislation to confront money laundering on a broad scale.

Money laundering also occurs in the informal financial sectors. Many Ugandans working abroad use alternate, cash-based, informal remittance systems to send money back to their families. Many establishments in Kampala accept U.S. dollars for cash transactions. Under legislation passed in 2004, foreign exchange bureaus are not authorized to transfer money abroad. The GOU has no effective means to prevent money launderers from accessing the many charitable and faith-based organizations that operate in Uganda. Moreover, to date, the GOU has not been able to document the level to which money launderers have used these entities.

Uganda does not have an offshore banking sector. The Special Economic Zones Bill of 2002 authorized the creation of export-processing zones (EPZs) and free trade areas within Uganda, and the GOU recently received a World Bank credit to establish EPZs. However, the GOU has not yet developed either EPZs or free trade areas. In 2001, Uganda criminalized narcotics-related money laundering. In 2003, the Bank of Uganda issued know your customer guidelines for Ugandan commercial banks, though it currently is unwilling to enforce compliance. In December 2003, the Ministry of Finance submitted to Parliament a comprehensive anti-money laundering bill based on the Financial Action Task Force's (FATF's) Forty Recommendations on Money Laundering. This legislation would criminalize money laundering for all serious crimes. However, the legislation did not pass during the past year. Until the draft AML legislation passes, the GOU maintains only limited authority and ability to investigate and prosecute money laundering related violations. To date, the GOU has not prosecuted anyone for narcotics-related or any other crime-related money laundering.

Beginning in 2004, the Bank of Uganda has circulated to financial institutions the list of individuals and entities included on the UNSCR 1267 Sanctions Committee's consolidated list. The Uganda Anti-Terrorism Act (ATA) of 2002, which entered into effect in June 2002, criminalized contributing, soliciting, controlling, or managing funds used to support terrorism or terror organizations. Despite the ATA, GOU authorities believe they have limited powers to freeze or seize terrorist finance-related assets. The draft AML would significantly expand this authority allow the GOU to seize all proceeds of crime.

Uganda is a member of the East and Southern African Anti-Money Laundering Group (ESAAMLG) and served as chair from August 2003 to August 2004. Uganda is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the United Nations Convention against Transnational Organized Crime. At this time, Uganda and the United States do not have formal agreements to facilitate the exchange of information and records in connection with investigations relating to narcotics, terrorism, and other crimes. Nevertheless, Ugandan authorities have cooperated with U.S. law enforcement efforts. In May 2004, at the request of the United States, the GOU detained and deported two U.S. citizens to face money laundering and wire fraud charges in the U.S.

The Government of Uganda should act on the draft legislation pending since December 2003 and enact comprehensive anti-money laundering legislation that meets international standards and

construct a viable anti-money laundering regime capable of thwarting terrorist financing. It should ratify the UN Convention against Transnational Organized Crime.

Ukraine

Ukraine has made rapid progress over the past two years in adopting, enacting and implementing comprehensive anti-money laundering legislation. However, high-level and widespread corruption, organized crime, smuggling, tax evasion, and other economic crimes continue to plague Ukraine's economy. Money laundering in Ukraine is not primarily related to proceeds from narcotics-trafficking, although this activity does generate at least a portion of organized crime income. Illicit proceeds also originate in criminal activities such as fraud, manipulation of the privatization process, fictitious entrepreneurship, smuggling of goods, trafficking in weapons and human beings, and large-scale corruption by government officials and others. Retail outlets that sell luxury goods and other businesses (including casinos and some restaurants) in Kiev and elsewhere are suspected of being fronts for money laundering and/or tax evasion. In June 2004, a federal jury in the United States convicted Ukraine's former Prime Minister, Pavlo Lazarenko, of money laundering, conspiracy to launder money, wire fraud, and transportation of stolen property. Ukraine provided assistance to the United States in connection with this prosecution.

According to Ministry of the Interior reports, banking fraud was the most common economic crime for the period of January through September 2004. The Ministry of Interior registered 39,300 economic crimes, or 6.2 percent more than over the same period of 2003, including 371 cases of money laundering, 3,500 cases of bank fraud, and 1,700 cases of smuggling. The market for smuggled goods remains significant in Ukraine, especially for textiles, automobiles, alcohol, and tobacco products.

Ukraine has created eleven Free Economic Zones (FEZs), and nine Priority Development Territories (PDTs), reportedly covering some 10 percent of Ukrainian territory. In August 2002, the Cabinet of Ministers introduced a moratorium on the establishment of FEZs and PDTs until January 1, 2005. There is a separate law for each FEZ that defines a set of tax exemptions enjoyed by the FEZ. Creation of FEZs was originally intended to enliven business and attract investment to depressed territories, but effectiveness of their operation is disputable. Legislative loopholes permit companies to misuse FEZ status, and to avoid taxes and import duties. The State Department of Financial Monitoring has uniform policy regarding economic entities operating throughout the country and does not envisage any specific provisions on FEZs.

When the Financial Action Task Force (FATF), in September 2001, placed Ukraine on the list of non-cooperative countries and territories in the fight against money laundering (NCCT), it noted that Ukraine lacked (1) a complete set of anti-money laundering (AML) laws, (2) an efficient mandatory system for reporting suspicious transactions to a Financial Intelligence Unit (FIU), (3) adequate customer identification requirements, and (4) adequate resources at present to combat money laundering. Following the FATF action, the U.S. Treasury Department issued an advisory to all U.S. financial institutions instructing them to "give enhanced scrutiny" to all transactions involving Ukraine. At its September 2002 plenary, FATF extended its original October 2002 deadline, by which Ukraine had to enact comprehensive, effective anti-money laundering legislation, or it would face the possibility of a recommendation for countermeasures from the FATF member countries, until December 15, 2002. On November 28, 2002, President Kuchma signed into law Ukrainian Law No. 249-IV, an anti-money laundering package "On Prevention and Counteraction of the Legalization (Laundering) of the Proceeds from Crime" (the Basic AML Law). On December 20, 2002, the FATF determined that Ukraine's new AML statute did not meet international standards and announced a recommendation that FATF members impose countermeasures on Ukraine. Under Section 311 of the USA PATRIOT Act, on December 20, 2002, the United States designated Ukraine as a jurisdiction of primary money laundering concern. In response to the imminent threat of countermeasures, Ukraine

passed further comprehensive legislative amendments in December 2002 and February 2003, in accordance with FATF recommendations. Immediately upon passage of the February amendments, the FATF withdrew its call for members to invoke countermeasures and the United States followed suit on April 17, 2003, by revoking Ukraine's designation under Section 311 of the USA PATRIOT Act as a jurisdiction of primary money laundering concern.

By passing comprehensive anti-money laundering legislation, Ukraine was not only able to avoid the countermeasures threatened by the FATF, but to initiate the process of NCCT de-listing. At the FATF plenary in September 2003, Ukraine was invited to submit an implementation plan, and upon review by the FATF Europe Review Group (ERG), an on-site visit to assess Ukraine's progress in developing its AML regime was conducted on January 19-23, 2004. The positive results of the on-site visit by the FATF evaluation team were reported to the ERG, and Ukraine was accordingly de-listed at the FATF plenary on February 25, 2004. As a condition for de-listing, Ukraine continues to undergo monitoring by the FATF on implementation of its AML regime.

As a member of the Council of Europe, Ukraine has undergone two mutual evaluations by that group's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), in May 2000 and September 2003. Although Ukraine criminalized drug money laundering in 1995, the initial 2000 mutual evaluation report was highly critical of Ukraine. The 2003 evaluation presented quite a different finding, as evaluators noted that a number of the previously noted deficiencies had been remedied, especially with regard to passage of the basic AML law in November 2002.

Two subsequent sets of amendments to the Basic AML Law, adopted in December 2002 and February 2003, have further helped bring Ukraine into compliance with internationally-recognized standards, as set forth by the FATF, UN and European Union (EU) conventions and directives on money laundering, and the Basel Committee's "Core Principles for Effective Banking Supervision". Effective September 1, 2001, the Government of Ukraine (GOU) criminalized non-drug money laundering in the Criminal Code of Ukraine. Subsequent amendments adopted in January 2003 include willful blindness provisions and expand the scope of predicate crimes for money laundering to include, with certain exceptions, any action that is punishable under the criminal code by imprisonment of three years. Provisions in the criminal code also address drug-related money laundering offenses and provide for the confiscation of proceeds generated by criminal activities.

The GOU enacted the "Act on Banks and Banking Activities"(Act) of January 2001, which imposes anti-money laundering measures upon banking institutions. The Act prohibits banks from opening accounts for anonymous persons, requires the reporting of large transactions and suspicious transactions to state authorities, and provides for the lifting of bank secrecy pursuant to an order of a court, prosecutor, or specific state body. Further amendments in February 2003 require banks to conduct due diligence to identify beneficial account owners prior to opening an account or conducting certain transactions, and to maintain records on suspicious transactions and the people carrying them out for a period of five years. The AML legislation also mandates the establishment of AML procedures in first-line financial institutions such as banks; stock, securities, and commodity brokers; and insurance companies, among other entities. Subsequent amendments mandate establishment of bank compliance programs and the appointment of bank compliance officers who may be subject to criminal liability for non-compliance. They also require employees of entities that carry out financial transactions to report transactions suspected for money laundering or terrorism finance. The AML legislation includes a "safe harbor" provision that protects reporting institutions from liability for cooperating with law enforcement agencies. In June 2004, the National Bank of Ukraine (NBU) drafted amendments to the Act, strengthening anti-money laundering requirements for banks. In particular, it mandates that the AML compliance officer also be a bank director, forbids banks to have correspondent accounts with shell banks, and authorizes the NBU to obtain information from other state authorities and legal persons in order to determine the business reputation and financial

circumstances of prospective bank owners and directors. Travelers must declare cross-border transportation of cash sums exceeding $1000.

In August 2001, "The Law on Financial Services and State Regulation of the Market of Financial Services" (August 2001 Law) was signed. The August 2001 Law establishes regulatory controls over non-bank financial institutions that manage insurance, pension accounts, financial loans, or "any other financial services involving savings and money from individuals." Specifically, it imposes record keeping requirements on covered entities and identifies the responsibilities of regulatory agencies. The August 2001 Law creates the State Commission on Regulation of Financial Services Markets, which, together with the NBU and the State Commission on Securities and the Stock Exchange, has the primary responsibility for regulating financial services markets. Amendments introduced in February 2003 set forth additional requirements similar to those prescribed for banks for all non-bank financial institutions. Additionally, in August 2003, the State Commission established a State Register of financial institutions; as of December 2004, it contains information on over 1200 non-bank financial institutions.

Significantly, amendments to Article 11 of the August 2001 Law reduce the monetary threshold over which transactions and operations are subject to compulsory financial monitoring, from Ukrainian hryvnias (UAH) 300,000 (approximately $57,750) for cashless payments and UAH 100,000 (approximately $19,250) for payments in cash to one single amount for both, UAH 80,000 (approximately $15,400). The compulsory transaction-reporting threshold applies only if the transaction also meets one or more suspicious activity indicators as set forth in the law. Any transaction that is suspected of being connected to terrorist activity is to be reported to the appropriate authorities immediately.

In November 2004, the GOU approved and sent to Parliament for review a draft law "On Amending Some Legislative Acts of Ukraine on Prevention to Legalization (Laundering) of the Proceeds from Crime and Terrorist Financing." The draft law, which proposes amendments to several pieces of existing legislation, is designed to bring Ukraine into compliance with the revised FATF Forty Recommendations, the Special Recommendations on Terrorist Financing, and the UN International Convention for the Suppression of the Financing of Terrorism. Proposed amendments to the Basic AML Law include expanding the list of covered entities to include financial intermediaries, such as real estate dealers, lawyers, notaries, advocates, public accountants, auditors, dealers in precious metals and stones, and others. These amendments also would widen the list of supervisory and regulatory financial monitoring authorities over such entities; in particular, designating the Ministry of Finance as responsible for gambling institutions, legal persons that organize any lotteries, dealers in precious metals and precious stones, public accountants and auditors; the State Committee on Land Resources for real estate dealers (realtors); the Ministry of Justice for notaries, lawyers, businesses providing incorporation and registration services for enterprises as well as management services of enterprises and property; and the Ministry of Transport and Communications for postal operators.

Additional proposed amendments to the Basic AML law include provisions to allow financial intermediaries to suspend suspected money laundering or terrorist finance related financial transactions for two working days and to require them to notify the Financial Intelligence Unit (FIU)-the entity to be designated as the authority for combating terrorist financing in Ukraine-of the suspension within one day. The FIU is authorized to suspend the transaction for an additional five working days. Customer due diligence (CDD) requirements for financial intermediaries would also be expanded to bring them into conformity with the revised FATF recommendations on customer identification and establishment of beneficial ownership. The Code of Ukraine on Administrative Offenses also would be supplemented to provide new supervisory and regulatory bodies with the authority to impose administrative fines on financial intermediaries for non-compliance with AML requirements. Notably, the draft law also amends the Ukrainian Criminal Code, criminalizing terrorist financing as a separate crime, and lowering the threshold of predicate offenses for money laundering

from three to two years. Although the first reading in Parliament did not secure enough votes for adoption of the draft law, it is currently under review and will most likely undergo a second vote in 2005.

On December 10, 2001, the Ukrainian Presidential Decree "On Measures to Counteract Legalization (Laundering) of Proceeds from Crimes" mandated the creation of the State Department of Financial Monitoring (FMD) by January 1, 2002, to function as Ukraine's FIU. The FMD became operational on June 12, 2003. Under the terms of this decree, the FMD is an independent authority, administratively subordinated to the Ministry of Finance, and is the sole agency authorized to receive and analyze financial information from first line financial institutions. Ukraine's basic AML law establishes a two-tiered system of financial monitoring and combating of criminal proceeds, including terrorist financing: entities of initial financial monitoring, or those legal entities that carry out financial transactions; and entities of state financial monitoring, or those regulating entities charged with regulation and supervision of the activities of the service providers. The overall regulatory authority in the system is vested in the FMD. The FMD is an administrative agency with no investigative or arrest authority. It is authorized to collect and analyze suspicious transactions, including those related to terrorist financing, and to transfer financial intelligence information to competent law enforcement authorities for investigation. By presidential decree on September 28, 2004, the FMD was elevated to a Central Executive agency with special status. The change, which takes effect on January 1, 2005, subordinates the new agency, known as the Financial Monitoring Committee (FMC), directly to the Cabinet of Ministers. Beginning January 2005, the FMD plans to open territorial offices in each of Ukraine's 27 administrative regions. Due to the change in status of the FIU and also to the creation of the territorial offices, the FIU staff size has correspondingly been increased from 100 to 338 persons.

In 2003, the FMD received 220,427 suspicious transaction reports (STRs), the bulk of which have been reported by banks. Approximately ten percent of these were identified by the FMD for "active research" and 3,211 were sent to competent law enforcement agencies as part of 18 case referrals. In 2004, the FMD received 725,959 STRs, 96.6 percent filed by banks. Of the 3.4 percent of STRs filed by non-banking financial intermediaries, the insurance sector comprised over 67 percent of the reporting. The FMD referred 164 cases comprising 20,929 STR filings to law enforcement authorities for the calendar year, seven of which were linked to terrorist financing.

From June 12, 2003, the date the FMD became operational, through December 31, 2004, FMD has referred a total of 182 cases to law enforcement agencies, 44 of which were sent to the General Prosecutor's Office (GPO), 42 to the Ministry of Interior, 50 to the Security Service of Ukraine, and 46 to the State Tax Administration of Ukraine. As a result of subsequent investigation, law enforcement agencies initiated 32 criminal cases based upon 67 original case referrals. Eleven of these cases were initiated based on suspicion of money laundering, with predicate offenses ranging from fraud, fictitious entrepreneurship, unlawful activity with payment cards, forgery, and abuse of power or official position. Three criminal cases have been passed to the courts and others are currently under investigation. Additionally, during the first eight months of 2004, the State Security Service filed 71 criminal cases on money laundering charges. The Ministry of Interior reported that over 10 months of 2004 it detected 398 crimes connected to money laundering. Eighty-three of them were committed by criminal groups involved in laundering proceeds from trafficking in drugs or arms, smuggling and tax evasion.

Ukraine is in the initial stages of drafting a law that may permit asset forfeiture. Ukraine has yet to establish a system and a legal basis for freezing and seizing assets derived from serious crimes. In response to earlier criticisms by the FATF regarding lack of coordination and information-sharing among agencies, the Cabinet of Ministers issued Decree No. 1896 on December 10, 2003, establishing a Single State Informational System (SSIS) of Prevention and Counteraction of Money Laundering and Terrorism Financing. This is a functioning system that electronically unites databases of 17 ministries and agencies through a central server located at the FIU and sub-servers at each of the

participating state agencies, thereby allowing the FIU electronic access to virtually all information housed in the databases of the other agencies. In order to foster better interagency cooperation, on September 22, 2004, the Cabinet of Ministers adopted a resolution establishing a Governmental Coordination Council On Functioning of a Single State Informational System. The Council will be comprised of high-level governmental officials in the Cabinet of Ministers, Ministries of Economy, Finance and Interior, Customs Office, and other agencies, including the FIU, and will address organizational issues of SSIS functioning and expansion.

Amendments to criminalize terrorist financing and to vest the Security Service of Ukraine with authority to investigate terrorist financing have been proposed as part of the draft law submitted to Parliament in November 2004. The GOU has cooperated with U.S. Government efforts to track and freeze the financial assets of terrorists and terrorist organizations. The NBU, State Tax Administration, Ministry of Finance, and State Security Service are fully aware of U.S. Executive Order (E.O.) 13224 and subsequent updates and addenda to the lists of terrorists and terrorist organizations. All agencies have tracked data that was provided and have exchanged information. The NBU has issued orders to banks to freeze accounts of individuals or organizations listed in the E.O. Ukraine plans to sign a U.S.-Ukraine agreement on mutual admission and actions on a list of persons/entities related to terrorist activities.

The GOU has also taken steps to implement UN Security Council resolutions relevant to fighting terrorism. The Cabinet of Ministers, on December 22, 1999, issued a resolution ordering agencies and banks to freeze assets and funds of the entities and individuals on the UNSCR 1267 Sanctions Committee's consolidated list. A Cabinet of Ministers resolution instructed the NBU to order all banks to comply with UNSCR 1333. In response to these measures, the NBU sent letters to regional departments and commercial banks to execute all applicable provisions of UNSCRs 1267 and 1333. The FMD acknowledges the existence and use of alternative remittance systems such as hawala. FMD personnel have attended seminars and exchanged information about such systems. The FMD and security agencies monitor charitable organizations and other non-profit entities that might be used to finance terrorism.

Ukraine will host the development of a prototype system for enhancing international data exchange and case collaboration (INDECCS). It is expected that the prototype will be completed in the spring of 2005 for presentation and review by international AML/CTF organizations. If successful, the new system promises to dramatically enhance the speed and quality of international information exchange, and will introduce new real time collaboration capabilities among and between participating countries.

FMD also has authority to conclude interagency agreements, and can exchange intelligence on financial transactions with a money laundering or terrorist financing nexus with other FIUs. In June 2004, FMD joined the Egmont Group. As of December 2004, 19 memoranda of understanding were concluded between the FMD and the FIUs of Russia, the Slovak Republic, Estonia, Italy, Spain, Belgium, the Czech Republic, Colombia, Georgia, France, Serbia, Macedonia, Slovenia, Poland, Romania, Portugal, Cyprus, Brazil, and Panama. However, as a member of Egmont, Ukraine may also exchange information with any other FIU whose legislation similarly allows information exchange without a memorandum of understanding in place. Under this framework, the FMD regularly exchanges information with the United States and other Egmont members, and has reported a 50 percent increase in information exchange with foreign FIUs since its accession to the Egmont Group.

The U.S.-Ukraine Treaty on Mutual Legal Assistance in Criminal Matters was signed in 1998, and entered into force in February 2001. A bilateral Convention for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with respect to Taxes on Income and Capital, which provides for the exchange of information in administrative, civil and criminal matters, is also in force. The GOU has also participated in GUUAM (Georgia, Ukraine, Uzbekistan, Azerbaijan and Moldova) for the

development of a joint law enforcement center that would cover asset seizure issues on a regional basis.

Ukraine ratified the UN Convention against Transnational Organized Crime in May 2004. Ukraine is a party to the 1988 UN Drug Convention as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. In March 2002, the European Convention on the Suppression of Terrorism was signed. Ukraine ratified the UN International Convention for the Suppression of the Financing of Terrorism in September 2002. Ukraine also became a signatory to the UN Convention against Corruption.

The Government of Ukraine has demonstrated considerable political will to combat money laundering by strengthening, clarifying, and implementing its newly adopted laws. As evidenced by the positive steps taken by its FIU, the NBU, and other actors in the financial and legal sectors, Ukraine has clearly shown its ability to implement a comprehensive anti-money laundering regime. Ukraine should criminalize the financing and support of terrorists and terrorism. Ukraine should adopt an asset forfeiture regime. Ukraine should continue to enhance and implement its newly adopted anti-money laundering regime, and should enact its pending legislation to expand coverage of its anti-money laundering laws to financial intermediaries. Law enforcement agencies should give higher priority to investigating money laundering cases. Both law enforcement officers and the judiciary lack a fundamental understanding of the nature of money laundering as a criminal offense. Both should be provided training in the theoretical and practical aspects of investigation and prosecution of money laundering.

United Arab Emirates

The United Arab Emirates (UAE) is an important financial center for the Gulf region. The UAE is still a largely cash-based society. However, the financial sector is modern and progressive. Dubai, in particular, is a major international banking center. There is also a growing offshore sector. The UAE's robust economic development, political stability, and liberal business environment have attracted a massive influx of people and capital. Because of the UAE's geographic location and role as the primary transportation and trading hub for the Gulf States, East Africa, and South Asia, and with its expanding trade ties with the countries of the former Soviet Union, the UAE has the potential to be a major center for money laundering. The large number of resident expatriates from the above regions, many of whom are engaged in legitimate trade with their homelands, or send remittances there, exacerbates that potential. Approximately 80 percent of the UAE population is comprised of non-nationals. The laundering of proceeds from the illegal narcotics trade is known to occur in UAE, and given the country's close proximity to Afghanistan, where most of the world's opium is produced, such narcotics-trafficking is a likely source. In addition, the potential exploitation of the UAE financial system by foreign terrorist groups is a serious concern.

Following the September 11 terrorist attacks in the United States, and amid revelations that terrorists had moved funds through the UAE, the Emirates' authorities acted swiftly to address potential vulnerabilities and, in close concert with the United States, to freeze the funds of groups with terrorist links, including the Al-Barakat organization, which was headquartered in Dubai. Both federal and Emirate-level officials have gone on record as recognizing the threat money laundering activities in the UAE pose to the nation's security. They have taken significant steps in 2004 to better monitor cash flows through the UAE financial system and to cooperate with international efforts to combat terrorist financing, including the passage of a law that specifically criminalizes terrorist financing.

Law No. 4 of 2002 criminalizes all forms of money laundering activities. The law calls for stringent reporting requirements for wire transfers exceeding $545 and currency importation/exportation limits set roughly at $11,700. The law imposes stiff criminal penalties (up to seven years in prison and a fine of up to 300,000 dirhams ($81,700), as well as seizure of assets if found guilty) for money laundering.

It also provides safe harbor provisions for those who report such crimes. Banks and other financial institutions (exchange houses, investment companies, and brokerage houses) are supervised by the Central Bank (CB) and are required to follow strict "know your customer" guidelines; all financial transactions over $54,000, regardless of their nature, must be reported to the CB. Financial institutions also are required to maintain records on transactions for five years.

In July 2000, the UAE established the National Anti-Money Laundering Committee (NAMLC), under the Chairmanship of the Central Bank's Governor, with representatives from the Ministries of Interior, Justice, Finance, and Economy; the National Customs Board; the Secretary General of the Municipalities; the Federation of the Chambers of Commerce; and five major banks and money exchange houses (as observers). It has overall responsibility for coordinating anti-money laundering policy.

The supervision of the UAE banking and financial sector falls under the authority of the CB. The CB issues instructions and recommendations as it deems appropriate and is permitted to take any necessary measure to ensure the integrity of the UAE's financial system. The CB issues licenses to financial institutions under its supervision and may impose administrative sanctions for compliance violations. The CB has issued a number of circulars requiring customer identification and providing for a basic suspicious transaction-reporting obligation. When suspicious activity is reported from a financial institution, the Central Bank is able to freeze suspect funds, make appropriate inquiries, and coordinate with law enforcement officials.

In an effort to consolidate and expand anti-money laundering requirements for the financial sector, the CB issued Circular 24/2000 in November 2000 to all banks, money exchanges, finance companies, and other financial institutions operating in the UAE. This circular delineates the procedures to be followed for the identification of natural and juridical persons, the types of documents to be presented, and rules on what customer records must be maintained on file at the institution. Other provisions of Circular 24/2000 call for customer records to be maintained for a minimum of five years, and further require that they be periodically updated as long as the account is open.

On July 29, 2004, the UAE strengthened its legal authority to combat terrorism and terrorist financing, by passing Federal Law Number 1 of 2004 on Combating Terror Crimes (Law No. 1/2004). The law sets stiff penalties for the crimes covered, including life imprisonment and the death penalty. It also provides for asset seizure or forfeiture. Under the law, founders of terrorist organizations face up to life imprisonment. The law also penalizes the illegal manufacture, import, or transport of "non-conventional weapons" or their components, with the intent to use them in a terrorist activity.

Law No. 1/2004 specifically criminalizes the funding of terrorist activities or terrorist organizations. Article 12 provides that raising or transferring money with the "aim or with the knowledge" that some or all of this money will be used to fund terrorist acts is punishable by "life or temporary imprisonment," whether or not these acts occur. Law No. 1/2004 grants the Attorney General (or his deputies) the authority to order the review of information related to the accounts, assets, deposits, transfer, or property movements on which the Attorney General has "sufficient evidence to believe" are related to the funding or committing of a terror activity stated in the law. The law also provides for asset seizure and confiscation. Article 31 gives the Attorney General the authority to seize or freeze assets until the investigation is completed. Article 32 confirms the Central Bank's authority to freeze accounts for up to seven days if it suspects that the funds will be used to fund or commit any of the crimes listed in the law. The law also allows the right of appeal to "the competent court" of any asset freeze under the law. The court will rule on the complaint within 14 days of receiving the complaint.

Law No. 1/2004 also sets up a "National Anti-Terror Committee" with representatives from the Ministries of Foreign Affairs, Interior, Justice, and Defense, the Central Bank, the State Security Department, and the Federal Customs Authority. The Committee serves as a UAE interagency liaison,

implements UN Security Council Resolutions on terrorism, and shares information with its foreign counterparts as well as with the United Nations (UN).

Law 4/2002 provided for the establishment of the Anti-Money Laundering and Suspicious Case Unit (AMLSCU), which acts as the Financial Intelligence Unit (FIU) and is housed within the CB. Financial institutions under the supervision of the CB are required to report suspicious transactions to the AMLSCU, which is charged with examining them and coordinating the release of information with law enforcement and judicial authorities. It has the authority to request information from foreign regulatory authorities in carrying out its preliminary investigation of suspicious transaction reports. The AMLSCU—a member of the Egmont Group since June 2002—exchanges information with foreign FIUs on a reciprocal basis, and has provided information relating to investigations carried out by the United States and other countries. In June 2004, the AMLSCU hosted a joint training session in Abu Dhabi for the nations of South Asia that are taking steps toward setting up their anti-money laundering regimes, including FIUs. The seminar focused on building an effective anti-money laundering regime, information technology issues, bilateral cooperation and mutual assistance, regulatory issues, hawala, international initiatives, and basic intelligence analysis.

From December 2000 to November 30, 2004, the AMLSCU received 2259 reports of suspicious transactions; of that number, 2148 were investigated by either the AMLSCU, the Central Bank, or law enforcement officials. In 27 cases, the Central Bank issued freeze orders and referred the cases to the Public Prosecutor; 12 of those cases are currently in the process of prosecution for money laundering, and 9 are in the process of judgment for money laundering and confiscation of proceeds.

Some money laundering in the UAE occurs in the formal banking system, including the numerous money exchange houses, but it is more prevalent in the informal and largely undocumented hawala remittance system. The fact that hawala is an undocumented and nontransparent system, and is highly resilient in response to enforcement and regulatory efforts, makes it difficult to control and an attractive mechanism for terrorist and criminal exploitation. The UAE has begun to make progress in confronting its vulnerability to the unregulated use of hawala. New regulations to improve oversight of the hawala system were implemented in 2002, when the CB required hawala brokers to register, submit the names and addresses of senders and beneficiaries, and to file suspicious transaction reports. As of January 2005, the number of applicants to obtain a hawala dar (hawala brokers) certificate reached 151, of which 128 were issued and the remaining 23 are in the process of fulfilling the requirements. There is no accurate estimate of the total number of UAE-based hawala brokers.

The UAE hosted its second International Conference on Hawala in April 2004, which was attended by approximately 350 participants. Delegates included government officials, executives of supervisory institutions, banking experts, and law enforcement officials from the United States, Latin America, Asia, and Europe. The conference statement recognized the key role that hawala and other informal funds transfer systems play in facilitating remittances, particularly those of migrant workers, although such systems can be abused for illegal activities. The conference reaffirmed the "The Abu Dhabi Declaration on Hawala," which calls for the establishment of a sound mechanism to regulate hawala.

The new attention on hawala is encouraging more people in the country to use regulated exchange houses. Representatives of money exchange business noted that their sector could transfer money anywhere, even to a private residence, for a fee competitive with hawala, persuading many to use the formal, and more secure, banking network.

In January 2002, the UAE CB published a declaration requirement for cash imported into the country above $10,900. The regulations provide customs services with the authority to seize undeclared cash; however, strict enforcement is still lacking. The UAE National Anti-Money Laundering Committee held its Second Annual Conference in December 2004 under the title "Customs Inspectors and the Implementation of the Cash Declaration Regulation" to look at ongoing implementation efforts.

The UAE Government (UAEG) also has admitted the need to better regulate "near-cash" items such as gold, jewelry, and gemstones, especially in the burgeoning markets in Dubai. The UAE has participated in the Kimberley Process Certification Scheme for Rough Diamonds (KPCS) since November 2002 and began certifying rough diamonds exported from the UAE on January 1, 2003. In 2004, the UAE was the first KPCS participant country to volunteer for a "peer review visit" on internal control mechanisms.

The Dubai Metals and Commodities Center (DMCC) is the quasi-governmental organization charged with issuing KP certificates in the UAE, and employs four individuals full-time to administer the KP program. Prior to January 1, 2003, the DMCC circulated a sample UAE certificate to all KP member states and embarked on a public relations campaign to educate the estimated 50 diamond traders operating in Dubai concerning the new KP requirements. UAE customs officials may delay or even confiscate diamonds entering the UAE from a KP member country without the proper certificate.

The Securities and Commodities Authority (SCA) supervises the country's two stock markets. In February 2004, it sent out anti-money laundering guidelines to brokers and the markets, instructing them to verify client information when opening accounts and created a reporting requirement for cash transactions above $10,900. The SCA also instructed the markets and brokers to file suspicious transaction reports for initial analysis before forwarding them to the AMLSCU for further action. The instructions also provide for a five-year record keeping requirement.

Dubai's booming property market might also be susceptible to money laundering abuse. In 2002, Dubai permitted three companies to sell "freehold" properties to non-citizens. Several other emirates (though not Abu Dhabi) have announced their intention to follow suit. The intense interest in these properties, and rumors of cash purchases, sparked concerns about the potential for money laundering. As a result, developers have stopped accepting cash purchases, alleviating some of the concerns about possible money laundering activities in this sector of the economy.

The UAEG monitors registered charities in the country and requires them to keep records of donations and beneficiaries. The Ministry of Labor and Social Affairs (MLSA) regulates charitable organizations in the UAE. The CB prohibits banks from opening accounts for charities, unless they are registered with the MLSA. The UAEG is much more sensitive since September 11 to the oversight of charities and the accounting of transfers aboard. In 2002, the UAEG mandated that all licensed charities interested in transferring funds overseas must do so via one of three umbrella organizations: the Red Crescent Authority, the Zayed Charitable Foundation, or the Muhammad Bin Rashid Charitable Trust. These three quasi-governmental bodies are in a position to ensure that overseas financial transfers go to legitimate parties. As an additional step, the UAEG has contacted the governments in numerous aid receiving countries to compile a list of recognized acceptable recipients for UAE charitable assistance.

The UAE is noted for its growing number of free trade zones (FTZs). Every emirate except Abu Dhabi has at least one functioning FTZ. There are over a hundred multinational companies located in the FTZs with thousands of individual trading companies. The FTZs permit 100 percent foreign ownership, no import duties, full repatriation of capital and profits, no taxation, and easily obtainable licenses. Companies located in the free trade zones are treated as being offshore or outside the UAE for legal purposes. However, UAE law prohibits the establishments of shell companies and trusts, and does not permit non-residents to open bank accounts in the UAE.

In March 2004, the UAEG passed Federal Law No. 8 Regarding the Financial Free Zones (Law No. 8/2004). The new law exempts FFZs and their activities from UAE federal civil and commercial laws, but subjects them and their operations to federal criminal laws including the Anti-Money Laundering Law No. 4/2002 and the Anti-Terror Law No. 1/2004. The new law and a subsequent federal decree also allowed for the establishment, in September 2004, of the UAE's first financial free zone (FFZ), known as the Dubai International Financial Center (DIFC). Sheikh Mohammed bin Rashid Al-

Maktoum, Crown Prince of Dubai and UAE Defense Minister, is the President of the DIFC, which is currently the only FFZ operating in the UAE.

With regard to banking activities in the FFZs, Law No. 8/2004 limits licenses to branches of companies, joint companies, and wholly owned subsidiaries, provided that they "enjoy a strong financial position and systems and controls, and are managed by persons with expertise and knowledge of such activity." The law prohibits companies licensed in the free zone from dealing in UAE currency (dirham) or taking "deposits from the state's markets." It further stipulates that the licensing standards of companies "shall not be less than those applicable in the state." The Law empowers the Emirates Stocks and Commodities Authority to approve the listing of any company listed on any UAE stock market in the free zone and the licensing of any UAE licensed broker. The law limits any insurance activity in the UAE carried out by a free zone company, to reinsurance. It further gives competent authorities in the Federal Government the power to inspect financial free zones and submit their findings to the UAE cabinet.

DIFC regulations provide for an independent regulatory body, the Dubai Financial Services Authority (DFSA), which reports to the office of Dubai Crown Prince and an independent Commercial Court. Observers called the independence of the DFSA into question in the summer of 2004, even prior to the inauguration of the DIFC, with the high profile firing of the chief regulator and the head of the regulatory council (the supervisory authority). Subsequent to the firing, Dubai passed laws which appear to give the DFSA more regulatory independence from the DIFC, although these laws have not yet been tested. The DFSA, whose regulatory regime is generally modeled after the United Kingdom system, is the only authority responsible for licensing firms providing financial services in the DIFC. There are currently two banks and three other financial firms operating in the DIFC. The DFSA's rules prohibit offshore casinos or Internet gaming sites' operating in the UAE. The DFSA requires firms to send suspicious transaction reports to the AMLSCU (along with a copy to the DFSA). Although firms operating in the DIFC are subject to Law No 4/2002, the DFSA has also issued its own anti-money laundering regulations and supervisory regime, creating some ambiguity as to the authority of the CB and AMLSCU within the DIFC.

The UAE is a party to the 1988 UN Drug Convention. It signed the UN Convention against Transnational Organized Crime in 2002, but has not yet ratified it. It has yet to sign the UN International Convention for the Suppression of the Financing of Terrorism. It has entered into a series of bilateral agreements on mutual legal assistance. The CB has circulated to all financial institutions under its supervision the UNSCR 1267 Sanctions Committee's consolidated list. To date, the CB has frozen a total of $3.13 million in 18 bank accounts in the UAE since September 11, 2001. The UAEG has also frozen other financial assets under Law 4/2002. Additionally, the AMLSCU has provided international organizations and its counterpart FIUs information on cases related to terrorist financing and anti-money laundering. In April 2004, the CB Governor announced that the CB had frozen all accounts related to a company suspected of trying to smuggle nuclear materials.

The UAE was very active in supporting the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004; the UAE was one of the original charter signatories. MENAFATF is a FATF-style regional body. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors.

The United Arab Emirates Government has begun constructing a far-reaching anti-money laundering program. The United Arab Emirates has sought to crack down on potential vulnerabilities in the financial markets and is cooperating in the international effort to prevent money laundering, particularly by terrorists. There has been a substantial improvement on behalf of the AMLSCU in the area of information sharing with other countries. However, there remain areas requiring further action. The Central Bank and AMLSCU should clarify and assert their jurisdiction in enforcing federal laws

with respect to the DFIC. Law enforcement and customs officials should begin to take the initiative to recognize money laundering activity and proactively develop cases without waiting for referrals from the AMLSCU. United Arab Emirates officials should give greater scrutiny to trade-based money laundering in all of its forms. The Central Bank should be more diligent in its efforts to encourage hawala dealers to participate in the registration program. The AMLSCU should take a more active role in participating in international anti-money laundering gatherings and increasing its ties with other FIUs. The United Arab Emirates should ratify both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism.

United Kingdom

The United Kingdom (UK) plays a leading role in European and world finance and remains attractive to money launderers because of the size, sophistication, and reputation of its financial markets. Although drugs are still a major source of illegal proceeds for money laundering, the proceeds of other offenses, such as financial fraud and the smuggling of people and goods, have become increasingly important. The past few years have witnessed the movement of cash placement away from High Street banks and mainstream financial institutions. Criminals continue to use bureaux de change, cash smuggling into and out of the UK, gatekeepers (including solicitors and accountants), and the purchase of high-value assets as disguises for illegally obtained money, and credit/debit card fraud has been on the increase since 2002.

The UK has implemented the provisions of the European Union's two Directives on the prevention of the use of the financial system for the purpose of money laundering and the Financial Actiona Task Force (FATF) Forty Recommendations on Money Laundering. Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from other serious crimes is criminalized by subsequent legislation. Banks and non-bank financial institutions in the UK must report suspicious transactions.

In November 2001, money laundering regulations were extended to money service bureaus (e.g., bureaux de change, money transmission companies). As of January 1, 2004, more business sectors are subject to formal suspicious transaction reporting (STR) requirements, including attorneys, solicitors, accountants, real estate agents, and dealers in high-value goods such as cars and jewelry. Sectors of the betting and gaming industry that are not currently regulated are being encouraged to establish their own codes of practice, including a requirement to disclose suspicious transactions.

The Proceeds of Crime Act 2002 was enacted on July 24, 2002, and entered into force on January 1, 2003. The final regulations took effect on March 1, 2004. The Act creates, for the regulated sector, a new criminal offense of failing to disclose suspicious transactions in respect to all crime, not just narcotics- or terrorism-related crimes, as was the case previously. Along with the Act came an expansion of investigative powers relative to large movements of cash in the UK. In light of this, Her Majesty's (HM) Customs has increased its national priorities to include investigating the movement of cash through money exchange houses and identifying unlicensed money remitters. A total of $159.6 million (£84 million) has been seized under the Act to date.

The UK's banking sector provides accounts to residents and nonresidents, who can open accounts through private banking activities and various intermediaries that often advertise on the Internet and also offer various offshore services. Private banking constitutes a significant portion of the British banking industry. Both resident and nonresident accounts are subject to the same reporting and record keeping requirements. Individuals typically open nonresident accounts for a tax advantage or for investment purposes.

Bank supervision falls under the Financial Services Authority (FSA). The FSA's primary responsibilities relate to the safety and soundness of the institutions under its jurisdiction. The FSA also plays an important role in the fight against money laundering through its continued involvement in the authorization of banks, and investigations of money laundering activities involving banks. The FSA regulated approximately 10,500 institutions and approved of 160,000 individuals in key positions (compliance officers, etc.) during the first half of 2003. From October of 2003, the FSA increased its regulatory role to include mortgage and general insurance agencies, totaling over 30,000 institutions. The FSA administers a civil-fines regime and has prosecutorial powers. The FSA has the power to make regulatory rules with respect to money laundering, and to enforce those rules with a range of disciplinary measures (including fines) if the institutions fail to comply.

In December 2003, the FSA fined Abbey National, the UK's sixth largest bank, $4.37 million (£2.3 million), for "extremely serious failings" in its anti-money laundering procedures during the period 2001-2003. According to the FSA, Abbey National was cited for failure to report suspicious banking transactions in a timely manner, as well as failure to carry out proper identity checks on new customers.

STRs are filed with the Financial Intelligence Division (FID), formerly the Economic Crime Bureau, of the National Criminal Intelligence Service (NCIS), which serves as the UK's Financial Intelligence Unit (FIU). The FID analyzes reports, develops intelligence, and passes information to police forces and HM Customs and Excise for investigation. The FID received approximately 32,000 STRs in 2001, 65,000 in 2002, and 100,000 in 2003.

The Proceeds of Crime Act 2002 enhances the efficiency of the forfeiture process and increases the recovered amount of illegally obtained assets. The Act consolidates existing laws on forfeiture and money laundering into a single piece of legislation, and, perhaps most importantly, creates a civil asset forfeiture system for the proceeds of unlawful conduct. It also creates the Assets Recovery Agency (ARA), to enhance the financial investigators' power to request information from any bank about whether it holds an account for a particular person. The Act provides for confiscation orders, and for restraint orders to prohibit dealing with property. It also allows for the recovery of property that is, or represents, property obtained through unlawful conduct, or that is intended to be used in unlawful conduct. Furthermore, the Act shifts the burden of proof to the holder of the assets to prove that the assets were acquired through lawful means. In the absence of such proof, assets may be forfeited, even without a criminal conviction. The Act gives standing to overseas requests and orders concerning property believed to be the proceeds of criminal conduct. The Act also provides the ARA with a national standard for training investigators, and gives greater powers of seizure at a lower standard of proof.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual, without a license from the Treasury, to make any funds for financial or related services available, directly or indirectly, to, or for the benefit of, a person who commits, attempts to commit, facilitates, or participates in the commission of acts of terrorism. The Order also makes it an offense for a bank or building society to fail to disclose to the Treasury a suspicion that a customer or entity, with whom the institution has had dealings since October 10, 2001, is attempting to participate in acts of terrorism. The Anti-Terrorism, Crime, and Security Act 2001 provides for the freezing of assets. In 2004, the UK issued 20 terrorist asset freeze orders on 34 individuals and 13 organizations.

As a direct result of the events of September 11, 2001, the FID established a separate Terrorist Finance Team (TFT) to maximize the effect of reports from the regulated sector. The TFT chairs a law enforcement group to provide outreach to the financial industry concerning requirements and typologies. The operational unit that responds to the work and intelligence development of the TFT has seen a threefold increase in staffing levels directly due to the increase in the workload. The Metropolitan Police responded to the growing emphasis on terrorist financing by expanding the focus

and strength of its specialist financial unit dedicated to this area of investigations. This unit is now called the National Terrorist Financing Investigative Unit (NTFIU).

Charitable organizations and foundations are subject to supervision by the UK Charities Commission. Such entities must be licensed and are subject to reporting and record keeping requirements. The Commission has investigative and administrative sanctioning authority, up to and including the authority to remove management, appoint trustees and place organizations into receivership.

The UK cooperates with foreign law enforcement agencies investigating narcotics-related financial crimes. The UK is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The UK has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The UK is a member of the FATF and the European Union. The NCIS is an active member of the Egmont Group and has information sharing arrangements in place with the FIUs of the United States, Belgium, France, and Australia. The Mutual Legal Assistance Treaty (MLAT) between the UK and the United States has been in force since 1996. The United States and UK recently negotiated an asset sharing agreement that is awaiting signature by the appropriate parties. The UK also has an MLAT with the Bahamas. Additionally, there is a memorandum of understanding between the U.S. Customs Service and HM Customs and Excise.

The Government of the United Kingdom should provide adequate oversight of its gaming sector. The United Kingdom should continue the strong enforcement of its comprehensive anti-money laundering/counterterrorist financing program and its active participation in international organizations to combat the domestic and global threat of money laundering and the support and financing of terrorists and their organizations.

Uruguay

In the past, Uruguay's strict bank secrecy laws, liberal currency exchange and capital mobility regulations, and overall economic stability made it a regional financial center vulnerable to money laundering. However, its extent and exact nature have always been relatively unknown. In 2002, banking scandals and mismanagement, along with massive withdrawals of Argentine deposits, led to a near collapse of the Uruguayan banking system, significantly weakening Uruguay's role as a regional financial center. This crisis likely diminished the attractiveness of Uruguayan financial institutions for money launderers in the medium term.

Uruguay has been a member of the Financial Action Task Force for South America (GAFISUD) since the organization was created in December 2000. In 2003, Uruguayan President Batlle's Deputy Chief of Staff served as the Task Force' s President, and in December, 2004, Alejandro Montesdeoca Broquetas, Uruguay's delegate to GAFISUD was selected to serve as the organization's new Executive Director Secretariat. GAFISUD's mutual evaluation in 2003 noted that Uruguay's anti-money laundering regime met international standards. GAFISUD also recognized Uruguay's efforts to train public and private sector players in money laundering-related issues.

While Uruguay's past role as a financial center put it at risk of becoming a money laundering center, the 2003 report of the OAS' Inter-American Drug Abuse Control Commission (CICAD) noted that there had been no arrests or prosecutions for money laundering in the previous three years. There were no arrests or prosecutions in 2004.

Over the last five years, the GOU has instituted several legislative and regulatory reforms in its anti-money laundering regime. In May 2001, Law 17,343 extended the predicate offenses for money laundering beyond narcotics- trafficking and corruption to include: terrorism; smuggling (value over $20,000); illegal trafficking in weapons, explosives and ammunition; trafficking in human organs, tissues and medications; trafficking in human beings; extortion; kidnapping; bribery; trafficking in

nuclear and toxic substances; and illegal trafficking in animals or antiques. The courts have the power to seize and confiscate property, products or financial instruments linked to money laundering activities. Legally, money laundering is considered a crime separate from underlying crimes such as narcotics-trafficking, administrative corruption, terrorism and smuggling, which are formally listed in the statutes.

In December 2003, the Uruguayan Chamber of Deputies approved a bill designed to limit bank secrecy and confidentiality. The bill is intended to increase credit transparency by eliminating bank secrecy for information pertaining to personal loans, financial credits, mortgages, or similar obligations. As of the end of 2004, however, the bill was still pending in commission in the Senate and had not been approved into law.

In its 2003 mutual evaluation report, GAFISUD made several suggestions to expand the scope of Uruguayan money laundering legislation as it relates to gambling, real estate, certain professions (primarily in the legal and financial services sectors), and the smuggling of cash and securities. GAFISUD also suggested that the Government of Uruguay (GOU) improve its investigative and administrative capabilities.

In September 2004, the Uruguayan Congress approved Law 17,835, which significantly strengthened the GOU's money laundering regime. The law incorporated all of GAFISUD's recommendations that had to be legislated, while other recommendations were met over the past two years through administrative regulations. The 2004 law expands the realm of entities subject to the filing of suspicious activities reports (SARs) and makes reporting of such activities a legal obligation. It specifically confers to the Central Bank's Financial Information and Analysis Unit (UIAF) the role of receiving and analyzing SARs, and the authority to request additional related information. The law also includes specific provisions related to the financing of terrorism and to the freezing of assets linked to terrorist organizations, as well as to undercover operations and controlled deliveries.

Central Bank regulations require all banks, currency exchange houses, stockbrokers and insurance companies to implement anti-money laundering policies, such as thoroughly identifying customers, recording transactions over $10,000 in internal databases, and reporting suspicious transactions to the UIAF. The 2004 law now makes this a legal obligation, extended to all financial intermediaries, as well as casinos, art dealers, real estate and fiduciary companies. Additionally, the law extends the reporting requirement to all persons coming in or out of Uruguay with over $10,000 in cash or monetary instruments. Regulations for the 2004 law are being issued by the Central Bank for all entities it supervises, and by the Executive for all other reporting entities, such as casinos, real estate companies and art dealers.

Three government bodies are involved in combating money laundering. The President's Deputy Chief of Staff heads the National Drug Council, which is the senior authority directing anti-money laundering policy. The Center for Training on Money Laundering serves as a forum for discussion and policy advice based on public and private sector input. Created in 2000, the UIAF acts as a financial intelligence unit receiving, analyzing, and remitting suspicious transaction reports to judicial authorities. Central Bank Circular 1722, which created the UIAF, provides for responding to requests for international cooperation. In November 2004, Resolution 2002-2072 of the Central Bank Board of Directors raised the UIAF to the level of a directorate reporting directly to the Board.

The Ministry of Finance and Economics, the Ministry of the Interior (via the police force), and the Ministry of Defense (via the Naval Prefecture) also participate in anti-money laundering efforts. The financial private sector, most of which is foreign owned, has developed self-regulatory measures against money laundering such as the Codes of Conduct approved by the Association of Banks and the Chamber of Financial Entities (1997), the Association of Exchange Houses (2001), and the Securities Market (2002).

Despite the power of the courts to confiscate property linked to money laundering, real estate ownership is not publicly registered in the name of the titleholder, which complicates efforts to track money laundering in this sector, especially in the partially foreign-owned tourist industry. The UIAF can have access to the name of titleholders at any time, however, and so can other government agencies through a judicial order. The GOU is planning to establish a computerized system that will facilitate the UIAF's access to titleholders' names.

Offshore banks are subject to the same laws and regulations as local banks, with the GOU requiring them to be licensed through a formal process that includes a background investigation. There are six offshore banks and 21 representatives of foreign banks. There are no records of the number of Uruguayan offshore firms or shell companies. Offshore trusts are not allowed. Bearer shares may not be used in banks and institutions under the authority of the Central Bank, and any share transactions must be authorized by the Central Bank.

Safeguarding the financial sector from money laundering is a priority for the GOU, and Uruguay remains active in international anti-money laundering efforts. It is a party to the 1988 UN Drug Convention, and participates in GAFISUD and the OAS Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering. The USG and the GOU are parties to extradition and mutual legal assistance treaties that entered into force in 1984 and 1994, respectively. Uruguay has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. In 2003 Uruguay ratified the UN International Convention for the Suppression of the Financing of Terrorism. The GOU is taking steps to comply with the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing. Some of these recommendations, such as the criminalization of

terrorism financing and provisions for the freezing of terrorist assets, were met by the 2004 money laundering law.

Effective implementation and enforcement of its anti-money laundering legislation should be a priority for the Government of Uruguay and should enact legislation that requires the identification and registration of the titleholders of real estate- a sector that is particularly vulnerable to money laundering. Uruguay should ratify the UN Convention against Transnational Organized Crime.

Uzbekistan

Uzbekistan is not considered an important regional financial center and does not have a well-developed financial system. Reportedly, legitimate business owners, ordinary citizens, and foreign residents generally attempt to avoid using the Uzbek banking system for transactions, except when absolutely required, because of the onerous nature of the Government of Uzbekistan's (GOU) financial control system and the fear of GOU seizure of one's assets. As a result, Uzbek citizens have functioning bank accounts only if they are required to do so by law. They deposit only funds they are required to deposit and often resort to subterfuge to avoid depositing currency. The Central Bank of Uzbekistan (CBU) asserts that deposits from individuals have been increasing over the past two years.

Narcotics proceeds are controlled by local and regional drug-trafficking organizations and organized crime. Foreign and domestic proceeds from criminal activity in Uzbekistan are held either in cash, high-value transferable assets, such as gold or automobiles, or in foreign bank accounts. The GOU could not provide information on whether financial crimes have been increasing. There is a significant black market for smuggled goods in Uzbekistan. Since the GOU imposed a very restrictive trade and import regime in the summer of 2002, smuggling of consumer goods, already a considerable problem, increased dramatically. Many Uzbek citizens continue to make a living by illegally shuttle-trading goods from neighboring countries, Iran, the Middle East, India, Korea, Europe, and the U.S. The black market for smuggled goods does not appear to be significantly funded by narcotics proceeds.

However, drug dealers may be exchanging their drug money in a fashion that allows the black market business people to access drug dollars. It is possible that this unofficial, basically unmonitored cash-based market may create the potential for small-scale terrorist or drug-related laundering activity. The funds generated by the smuggling and corruption are not laundered through the banking system. There appears to be virtually no money laundering through formal financial institutions in Uzbekistan because of the extremely high degree of supervision and control over all bank accounts in the country exercised by the CBU, the Ministry of Finance and the state-owned and controlled banks. Although Uzbek financial institutions do not engage in illegal transactions in U.S. currency, illegal unofficial exchange houses, where the majority of cash-only money laundering takes place, deal in local soum and U.S. dollars. Moreover, drug dealers and others can transport their criminal proceeds in cash across Uzbekistan's borders for deposit in the banking systems of other countries, such as Kazakhstan, Russia or the United Arab Emirates.

Money laundering of the proceeds from drug-trafficking and other criminal activities is a criminal offense. With regard to drugs, Article 41 of the Law on Narcotic Drugs and Psychotropic substances (1999) stipulates that any institution may be closed for performing a financial transaction for the purpose of legalizing (laundering) proceeds derived from illicit narcotics-trafficking. Penalties for money laundering are from ten to fifteen years imprisonment, under Article 243 of the Criminal Code. This article defines the act of money laundering to include as punishable acts the transfer; conversion; exchange; or concealment of origin, true nature, source, location, disposition, movement and rights with respect to the assets derived from criminal activity. There has not yet been a complete assessment of the implementation and use of this legislation.

The CBU and the National Security Service (NSS) closely monitor all banking transactions to ensure that money laundering does not occur in the banking system. Though not legislatively mandated, banks are required to know, record and report the identity of customers engaging in significant transactions, including the recording of large currency transactions at thresholds appropriate to Uzbekistan's economic situation. All transactions involving sums greater than $1000 in salary expenses for legal entities and $500 in salaries for individuals must be tracked and reported to the authorities. The CBU unofficially requires commercial banks to report on private transfers to foreign banks exceeding $10,000. Depending on the type and amount of the transaction, banks are required to maintain records for time deposits for a minimum of three years, possibly not sufficient time to reconstruct significant transactions. The law protects reporting individuals with respect to their cooperation with law enforcement entities. However, reportedly, the GOU has not adopted "banker negligence" laws that make individual bankers responsible if their institutions launder money.

Parliament passed a new law in August 2004 to combat money laundering and terrorist financing. This law, scheduled to take effect in January 2006, requires certain entities to report cash transactions above $26,000 (approximately) as well as suspicious transactions. In addition, this law also covers some non-banking financial institutions, such as investment foundations, depositaries and other types of investment institutions; stock exchanges; insurers; organizations which render leasing and other financial services; organizations of postal service; pawnshops; lotteries; and notary offices. It does not include intermediaries such as lawyers, accountants, or broker/dealers. Casinos are illegal.

The law on banks and bank activity (1996), article 38, stipulates conditions under which banking information can be released to law enforcement, investigative and tax authorities, prosecutor's office and courts. Different conditions for disclosure apply to different types of clients—individuals and institutions. In September 2003, Uzbekistan enacted a bank secrecy law that prevents the disclosure of client and ownership information for domestic and offshore financial services companies to bank supervisors and law enforcement authorities. In all cases, private bank information can be disclosed to prosecution and investigation authorities, provided there is a criminal investigation underway. The information can be provided to the courts on the basis of a written request in relation to cases currently

under consideration. Protected banking information also can be disclosed to tax authorities in cases involving the taxation of a bank's client.

Existing controls on transportation of currency across borders, would, in theory, facilitate detection of the international transportation of illegal source currency. When entering/exiting the country, foreigners and Uzbek citizens are required to report all currency they are carrying. Residents and non-residents may bring the equivalent of $10,000 into the country tax-free. Amounts in excess of this limit are assessed a one-percent duty. Non-residents may take out as much currency as they brought in, however, residents are limited to the equivalent of $2000. Residents wishing to take out higher amounts must obtain authorization to do so; amounts over $2000 must be approved by an authorized commercial bank and amounts over $5000 must be approved by the CBU.

International business companies are permitted to have offices in Uzbekistan and are subject to the same, if not stricter, regulations as domestic businesses. Offshore banks are not present in Uzbekistan and other forms of exempt or shell companies are not officially present.

In accordance with Uzbekistan's Code of Criminal Procedure, investigation of money laundering offenses falls under the jurisdiction of the Ministry of Internal Affairs (MVD). The Department of Investigation of Economic Crimes within the Ministry conducts investigations of all types of economic offenses. A specialized structure within the NSS and the Department on Combating Economic Crimes and Corruption in the Office of the Prosecutor General also are authorized to conduct investigations of money laundering offenses. There are no known arrests or prosecutions for money laundering or terrorist financing since January 1, 2002, except for one case following the suicide bombings of Spring 2004. Unofficial information from numerous law enforcement officials indicates that there have been few, if any, prosecutions for money laundering under article 243 of the Criminal Code since its enactment in 2001. The GOU appears to lack a sufficient number of experienced and knowledgeable agents to investigate money laundering.

Article 155 of Uzbekistan's Criminal Code and the law "On Fighting Terrorism" criminalize terrorist financing. The latter law names the NSS, the MVD, the Committee On The Protection Of State Borders, the State Customs Committee, the Ministry of Defense, and the Ministry for Emergency Situations as responsible for implementing the counterterrorist legislation. The law names the NSS as the coordinator for government agencies fighting terrorism.

The GOU has the authority to identify, freeze, and seize terrorist assets. Uzbekistan has circulated to its financial institutions the names of individuals and entities included on the UN 1267 Sanction Committee's consolidated list. In addition, the GOU has circulated the lists of individuals and entities included in the U.S. executive order to the CBU, which has, in turn, forwarded these lists to all banks operating in Uzbekistan. According to the CBU, no assets have been frozen.

Other than a plan to step up enforcement of currency regulations, the GOU has taken no steps to regulate or deter alternative remittance systems such as hawala, black market exchanges, trade-based money laundering, or the misuse of gold, precious metals and gems. We are not aware of any legislative initiatives under consideration. Although currency convertibility has been officially announced, in many regions of the country there is a strong black market for foreign exchange that accounts for a significant amount of informal economic activity.

The GOU closely monitors the activities of charitable and non-profit entities, such as NGOs, that can be used for the financing of terrorism. In February 2004, the Cabinet of Ministers issued Decree # 56 to allow the Government to vet grants to local NGOs from foreign sources, ostensibly to fight money laundering and terrorist financing. Given the degree of supervision of charities and other non-profits, and the level of threat Uzbekistan itself faces from the Islamic Movement of Uzbekistan (IMU), a designated terrorist organization, it is extremely unlikely that the NSS would knowingly allow any funds to be funneled to terrorists through Uzbekistan-based charitable organizations or NGOS.

Uzbekistan has established systems for identifying, tracing, freezing, seizing, and forfeiting proceeds of both narcotics-related and money laundering-related crimes. Major points in current laws include the ability to seize items used in the commission of crimes such as conveyances used to transport narcotics, farm facilities (except land) where illicit crops are grown or which are used to support terrorist activity, legitimate businesses if related to criminal proceeds and bank accounts. The banking community, which is entirely state-controlled and with few exceptions, state-owned, cooperates with efforts to trace funds and seize bank accounts. Uzbek law does not allow for civil asset forfeiture, but the Criminal Procedure Code provides for "civil" proceedings within the criminal case to decide forfeiture issues. As a practical matter, these proceedings are conducted as part of the criminal case. No new legislation or changes in current law are under active consideration by the GOU regarding seizure or forfeiture of assets. The obstacles to enacting such laws are largely rooted in the widespread corruption that exists within the country.

In 2000, Uzbekistan set up a fund to direct confiscated assets to law enforcement activities. In accordance with the regulation the assets derived from the sale of confiscated proceeds and instruments of drug-related offenses were transferred to this fund to support entities of the NSS, the MVD, the State Customs Committee, and the Border Guard Committee, all of which are directly involved in combating illicit drug-trafficking. According to the GOU, a total of 115 million soum (approximately $115,000) has been deposited into this fund since its inception, which includes about 40 million soum ($40,000) during 2004. Roughly $80,000 has been turned over to Uzbek law enforcement agencies. In 2004, however, the Cabinet of Ministers issued an order to close the Special Fund as of November 1, 2004. Under the new procedure, each agency will manage the assets it seizes. There is also a specialized fund within the MVD set up to reward those officers who directly participate in or contribute to law enforcement efforts leading to the confiscation of property. This fund has generated 20 percent of its assets from the sale of property confiscated from persons who have committed offenses such as the organization of criminal associations, bribery and racketeering. The GOU enthusiastically enforces existing drug-related asset seizure and forfeiture laws. The GOU has not been forthcoming with information regarding the total dollar value of assets seized from crimes. Reportedly, existing legislation does not permit sharing of seized narcotics assets with other governments.

Uzbekistan's government agencies are extremely cooperative and positive to efforts by the U.S. and other countries to trace or seize assets. GOU agencies make use of tips from other countries' enforcement officials regarding the flow of drug-derived assets or of assets intended to support terrorism.

The GOU has repeatedly emphasized the importance of international cooperation in the fight against drugs and transnational organized crime and has made efforts to integrate the country in the system of international cooperation. Uzbekistan has entered into agreements with Uzbek supervisors to facilitate the exchange of supervisory information including on-site examinations of banks and trust companies operating in the country. Uzbekistan has entered into bilateral agreements for the cooperation or exchange of information on drug related issues with the U.S., Germany, Italy, Latvia, Bulgaria, Poland, China, Iran, Pakistan, the CIS, and all the countries in Central Asia. It has multilateral agreements in the framework of the CIS, under the Shanghai Cooperation Organization and under memoranda of understanding. An "Agreement on Narcotics Control and Law Enforcement Assistance" was signed with the United States on August 14, 2001, with two supplemental agreements that came into force in 2004.

Uzbekistan does not have a Mutual Legal Assistance Treaty with the United States. However, Uzbekistan has reached informal agreement with us on mechanisms for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious crime investigations. When requested, Uzbekistan has cooperated with appropriate

law enforcement agencies of the USG and other governments investigating financial crimes and several important terrorist-related cases.

The GOU is an active party to the relevant agreements concluded under the CIS, CAEC, ECO, Shanghai Cooperation Organization and the "Six Plus Two" Group. The GOU has also participated in GUUAM (Georgia, Ukraine, Uzbekistan, Azerbaijan and Moldova) for the development of a joint law enforcement center that would cover asset seizure issues on a regional basis. Uzbekistan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism and to the UN Convention against Transnational Organized Crime.

A lack of trained personnel, resources, and modern equipment hinder Uzbekistan's efforts to fight money laundering and terrorist financing. The Government of Uzbekistan should continue to refine its pertinent legislation to bring it up to international standards. Uzbekistan also should establish supervisory oversight of intermediaries, such as accountants and attorneys, and expand the cross-border currency reporting rules to cover the transfer of monetary instruments, gold, gems and precious metals. Access to financial institution records should be given to appropriate regulatory and law enforcement agencies so that they can properly conduct compliance examinations and investigations. Uzbekistan should establish a Financial Intelligence Unit to receive and analyze the suspicious transaction reports it proposed to require.

Vanuatu

Vanuatu's offshore sector is vulnerable to money laundering, as Vanuatu has historically maintained strict secrecy provisions that have the effect of preventing law enforcement agencies from identifying the beneficial owners of offshore entities registered in the sector. Due to allegations of money laundering, and in response to pressure from the Financial Action Task Force (FATF), a few United States-based banks announced in December 1999 that they would no longer process U.S. dollar transactions to or from Vanuatu. The Government of Vanuatu (GOV) responded to these concerns by introducing reforms designed to strengthen domestic and offshore financial regulation.

Vanuatu's financial sector includes five licensed banks (that carry on domestic and offshore business) and 60 credit unions, regulated by the Reserve Bank of Vanuatu. The Financial Services Commission (FSC) regulates the offshore sector that includes 9 banks and approximately 2,500 "international companies" (i.e., international business companies or IBCs), as well as offshore trusts and captive insurance companies. IBCs may be registered using bearer shares, shielding the identity and assets of beneficial owners of these entities. Secrecy provisions protect all information regarding IBCs and provide penal sanctions for unauthorized disclosure of information. These secrecy provisions, along with the ease and low cost of incorporation, make IBCs ideal mechanisms for money laundering and other financial crimes.

As of January 1, 2003, according to the Australian High Commission in Port Vila, the Reserve Bank of Vanuatu regulates nine offshore banks registered in Vanuatu that were formerly regulated by the FSC. This requirement was one of many recommendations of the 2002 International Monetary Fund Module II Assessment Report (IMFR) that found Vanuatu's onshore and offshore sectors to be " noncompliant" with many international standards.

The Financial Transaction Reporting Act (FTRA) of 2000 established Vanuatu's Financial Intelligence Unit (FIU) within the State Law Office. The one-person FIU receives suspicious transaction reports (STRs) filed by banks and distributes them to the Public Prosecutor's Office, the Reserve Bank of Vanuatu, the Vanuatu Police Force, the Vanuatu Financial Services Commission, and law enforcement agencies or supervisory bodies outside Vanuatu. The FIU also issues guidelines to, and provides training programs for, financial institutions regarding record keeping for transactions and reporting obligations.

The Act also regulates how such information can be shared with law enforcement agencies investigating financial crimes. Financial institutions within Vanuatu must establish and maintain internal procedures to combat financial crime. Every financial institution is required to keep records of all transactions. Five key pieces of information are required to be kept for every financial transaction: the nature of the transaction, the amount of the transaction, the currency in which it was denominated, the date the transaction was conducted, and the parties to the transaction

The IMFR noted several weaknesses in Vanuatu's anti-money laundering regime. Consequently, the Government of Vanuatu (GOV) has prepared a policy paper currently being considered by the Council of Ministers. FRTA amendments are expected to be passed in parliament some time this year—the next ordinary session is scheduled to sit in March. The amendments to the FTRA, if enacted, would require mandatory customer identification requirements; broaden the range of covered institutions required to file STRs to include auditors, trust companies, and company service providers; and provide safe harbor for both individuals and institutions required to file STRs. The proposed amendments would override any inconsistent banking or other secrecy provisions and clarify the FIU's investigative powers.

Regulatory agencies in Vanuatu have instituted stricter procedures for issuance of offshore banking licenses under the International Banking Act no 4 of 2002 and continue to review the status of previously issued licenses. All financial institutions, both domestic and offshore, are required to report suspicious transactions and to maintain records of all transactions for six years, including the identities of the parties involved.

The Serious Offenses (Confiscation of Proceeds) Act 1989 criminalized the laundering of proceeds from all serious crimes and provided for seizure of criminal assets and confiscation after a conviction. The Proceeds of Crime Act (2002) retains the criminalization of the laundering of proceeds from all serious crimes, criminalizes the financing of terrorism, and includes full forfeiture, and restraining, monitoring, and production powers regarding assets.

Vanuatu passed the Mutual Assistance in Criminal Matters Act in December 2002 for the purpose of facilitating the provision of international assistance in criminal matters for the taking of evidence, search and seizure proceedings, forfeiture or confiscation of property, and restraints on dealings in property that may be subject to forfeiture or seizure. The Attorney General possesses the authority to grant requests for assistance, and may require government agencies to assist in the collection of information pursuant to the request. The Extradition Act of 2002 includes money laundering within the scope of extraditable offenses.

The amended International Banking Act has now placed Vanuatu's international and offshore banks under the supervision of the Reserve Bank of Vanuatu. Section 5(5) of the Act states that if existing licensees wish to carry on international banking business after December 31, 2003, the licensee should have submitted an application to the Reserve Bank of Vanuatu under Section 6 of the Act for a license to carry on international banking business. If an unregistered licensee continues to conduct international banking business after December 31, 2003, it will be in contravention of Section 4 of the Act, and, if found guilty, the licensee will be subject to a fine or imprisonment. Under Section 19 of the Act, the Reserve Bank can conduct investigations where it suspects that an unlicensed person or entity is carrying on international banking business.

One of the most significant requirements of the amended legislation is the banning of "shell" banks. As of January 1, 2004, all offshore banks registered in Vanuatu must have a physical presence in Vanuatu, and management, directors, and employees must be in residence. At the September 2003 plenary session of the Asia/Pacific Group on Money Laundering (APG), Vanuatu noted its intention to draft new legislation regarding trust companies and company service providers. The new legislation will cover disclosure of information with other regulatory authorities, capital and solvency

requirements, and "fit and proper" requirements. Additionally, Vanuatu is drafting legislation to comply with standards set by the International Associations of Insurance Supervisors.

The E-Business Act No. 25 of 2000 and the Interactive Gaming Act No. 16 of 2000 regulate e-commerce. Section 5 of the E-Business legislation permits the establishment of a Vanuatu-based website where business can be conducted without residency, directors, shareholders, or a registered office. Reportedly, the E-Business Act requires online operations to maintain stringent customer identification and record keeping requirements, as well as reporting suspicious transactions. The Financial Transaction Reporting Act of 2000 applies to e-commerce or businesses by defining any company listed under the Vanuatu Interactive Gaming Act 2000 as a financial institution.

In April 2002, the Organization for Economic Cooperation and Development (OECD) launched an initiative to address harmful tax practices worldwide. Vanuatu was one of seven countries listed as an "uncooperative tax haven." In January 2004, the OECD revealed that it has removed Vanuatu from its list of "uncooperative tax havens," following Vanuatu's earlier announcement that it will implement measures under the Harmful Tax Initiative. The OECD stated in a news release that it welcomes the commitment that Vanuatu has made to improve the transparency of its tax and regulatory systems, and to establish, by December 2005, effective exchange of information for tax matters with OECD countries. This move by OECD has made Vanuatu the first country to secure removal from the list of uncooperative tax havens.

In addition to the Asia Pacific Group, Vanuatu is a member of the Offshore Group of Banking Supervisors, the Commonwealth Secretariat, and the Pacific Island Forum. Its Financial Intelligence Unit became a member of the Egmont Group in June 2002. However, Vanuatu has yet to sign either the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, or the 1988 UN Drug Convention

The Government of Vanuatu should immobilize bearer shares and require complete identification of the beneficial ownership of international business companies (IBCs). It should implement all the provisions of its Proceeds of Crime Act and enact all additional legislation that is necessary to bring both its onshore and offshore financial sectors into compliance with international standards. Vanuatu should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention.

Venezuela

Venezuela is not a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking sector, which consists of 52 banks, primarily serves the domestic market. Venezuela is a major drug-transit country. Proximity to drug producing countries, weaknesses in its anti-money laundering system, and corruption continue to make Venezuela particularly vulnerable to money laundering. The main source of money laundering in Venezuela stems from proceeds generated by Colombia's cocaine and heroin trafficking organizations. Trade-based money laundering, such as the Black Market Peso Exchange, through which money launderers furnish narcotics-generated dollars in the United States to commercial smugglers, travel agents, investors, and others in exchange for Colombian pesos, remains a prominent method for laundering narcotics proceeds. It is suspected that many of these black market traders ship their wares through Venezuela's Margarita Island free trade zone. Reportedly, some money is also laundered through the real estate market in Margarita Island.

The 1993 Organic Drug Law provides the only legal mechanism for the investigation and prosecution of money laundering crimes. Under this law, a direct connection between the illegal drugs and the proceeds must be proven to establish a money laundering offense. The Government of Venezuela

(GOV) freezes assets of individuals charged in international drug trade or money laundering cases directly related to narcotics-trafficking. If a conviction is obtained, the frozen assets are turned over to the Ministry of Finance for use in drug demand reduction programs. After the introduction of a new Code of Criminal Procedure in 1999, responsibility for initiating these actions shifted from judges to prosecutors. Due to prosecutors' unfamiliarity with the accusatory judicial system, as well as their having to assume the burden of tens of thousands of backlogged cases, the number of cases resulting in seizure of trafficker assets has decreased.

To expand the predicate offenses for money laundering beyond activities involving the illicit drug trade, the GOV introduced the Organic Law against Organized Crime bill in 2002. Under this bill, money laundering is made a separate, autonomous offense, with no drug nexus required, and those who cannot establish the legitimacy of possessed or transferred funds, and who have awareness of the illegitimate origins of those funds, would be guilty of money laundering. The bill broadens asset forfeiture and sharing provisions, adds conspiracy as a criminal offense, strengthens due diligence requirements, establishes the Financial Intelligence Unit (FIU) as a fully autonomous unit, and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques such as the use of undercover agents. Although 97 of its 150 articles were approved in 2002, not a single additional article was passed in 2003 or 2004. The bill remains in its final reading at the National Assembly. If the Organized Crime bill is ultimately enacted, the GOV would meet the requirements of the 1998 Vienna Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime, all of which have been ratified by the GOV.

Under Resolution 333-97 of 1997, entitled "Standards for the Prevention, Control, and Prosecution of Money Laundering," the Superintendence of Banks and Other Financial Institutions (SUDEBAN) have implemented controls to prevent and investigate money laundering. These include stricter customer identification requirements, and the reporting of both currency transactions over a designated threshold and suspicious transactions. These controls apply to all banks (commercial, investment, mortgage, private), savings and loan institutions, financial rental agencies, currency exchange houses, money remitters, money market funds, capitalization companies, and frontier foreign currency dealers. The institutions are also required to file suspicious and cash transaction reports with Venezuela's FIU, the Unidad Nacional de Inteligencia Financiera (UNIF), which was created under the SUDEBAN in July 1997 and began operations in June 1998. In 2004, the UNIF was expanded to include two new divisions: one for research and development, and another for strategic analysis. Three different officials held the position of director of the UNIF in 2004.

The UNIF receives suspicious transaction reports (STRs) and reports of currency transactions exceeding 4.5 million bolívares (approximately $2,350) from institutions regulated by SUDEBAN, the Office of the Insurance Examiner, the National Securities and Exchange Commission, the Bureau of Registration and Notaries, the Central Bank of Venezuela, and the Bank Deposits and Protection Guarantee Fund. Some institutions regulated by SUDEBAN, such as tax collection entities and public service payroll agencies, are exempt from the reporting requirement. SUDEBAN also allows certain customers of financial institutions-those who demonstrate "habituality" in the types and amounts of transactions they conduct-to be excluded from currency transaction reports filed with the UNIF. A system has been developed for electronic receipt of currency transaction reports (CTRs), but STRs must be filed in paper format. The UNIF received 965 STRs in 2003, although that amount is expected to decrease in 2004.

In addition to STRs and CTRs, the UNIF also receives reports on the transfer of foreign currency exceeding $10,000, the sale and purchase of foreign currency exceeding $10,000, and summaries of cash transactions by states that exceed 4.5 million bolívares. The UNIF does not, however, receive reports on the transportation of currency or monetary instruments into or out of Venezuela. The Venezuelan Association of Currency Exchange Houses (AVCC), which counts all but one of the

country's money exchange companies among its membership, voluntarily complies with the same reporting standards as those required of banks, including the filing of CTRs and STRs and "know your customer" policies. Each currency exchange house in the country has and employs systems to electronically transmit transaction reports to SUDEBAN and the Public Ministry. However, inadequate foreign exchange controls by the GOV's Commission for Administrative Control of Currency Exchange (CADIVI) present new opportunities to circumvent regulations applicable in the banking and financial institution sectors. Procedures to limit the potential for laundering funds through the stock market are also thought to be inadequate.

The UNIF analyzes STRs and other reports, and refers those deemed appropriate for further investigation to the Public Ministry (the Office of the Attorney General). Approximately 30 percent of the STRs received by the UNIF are sent to the Public Ministry for further investigation. The Public Ministry subsequently opens and oversees the criminal investigation. The Venezuelan constitution guarantees the right to bank privacy and confidentiality, but in cases under investigation by the UNIF, SUDEBAN or the Public Ministry, or by order of a Judge of Control, bank secrecy may be waived. Comprehensive financial and law enforcement information is available to the UNIF under existing legislation. When the Organized Crime bill is passed, the UNIF will become a fully autonomous unit, rather than being part of SUDEBAN. There is some concern among GOV officials about moving the UNIF out of SUDEBAN, as approximately 90 percent of the STRs received are filed by banks.

Venezuela is one of the few countries in Latin America that does not have restrictive bank secrecy laws. Although the Venezuelan constitution guarantees the right to privacy and confidentiality, investigations by the UNIF, SUDEBAN or the Public Ministry are not hindered by bank secrecy provisions. However, due to the lack of a legal basis to employ modern investigative techniques, with appropriate legal safeguards, Venezuelan law enforcement authorities find it difficult if not impossible to investigate and prosecute sophisticated criminal organizations and complex crimes such as money laundering. No law enforcement offices have dedicated specific resources to investigating and prosecuting money laundering. There is no special prosecutorial unit for the prosecution of money laundering cases under the Public Ministry, which is the only entity legally capable of initiating money laundering investigations. Currently only the drug prosecutors receive STRs from the UNIF and conduct money laundering investigations, although STRs may then be shared with other prosecutors as deemed necessary. There are only 20 drug prosecutors for all of Venezuela, most of whom lack the technical financial experience to successfully prosecute money laundering investigations, and there are no financial analysts or forensic accountants dedicated to assisting them with the preparation of their cases. Indeed, there have only been three money laundering convictions in Venezuela since 1993, and all of them were narcotics-related. No money laundering cases were tried in 2004. Venezuela has limited mechanisms for freezing assets tied to illicit activities. The assets must be linked to a crime such as narcotics trafficking—or money laundering directly related to narcotic trafficking—and must pass through a lengthy judicial process.

Current Venezuelan law does not specifically criminalize terrorism, although it is addressed as a matter of public order under a 1936 law. The Organized Crime Bill, when passed, would rectify this by defining terrorist activities and establishing punishments of up to 20 years in prison. The bill's expanded definition of money laundering would also make it possible to prosecute those engaged in terrorism financing, and to freeze and seize their assets. However, the bill does not establish terrorist financing as an autonomous crime.

The UNIF has been a member of the Egmont Group since 1999 and has signed bilateral information exchange agreements with counterparts worldwide. Venezuela participates in the Organization of American States Inter-American Commission on Drug Abuse Control (OAS/CICAD) Experts Group to Control Money Laundering and is a member of the Caribbean Financial Action Task Force (CFATF). Although Venezuela is a member of GAFISUD, the South American Financial Task Force, the GOV has not participated in any GAFISUD meetings or other initiatives since it first became a

member in July 2003. Venezuela also participates in a multilateral initiative with the governments of the United States, Colombia, Panama, and Aruba designed to address the problem of trade-based money laundering through the Black Market Peso Exchange. Venezuela is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. The GOV has signed, but not yet ratified, the UN Convention against Corruption. In January 2004, the GOV deposited its instrument of ratification for the OAS Inter-American Convention Against Terrorism. The GOV continues to share money laundering information with U.S. law enforcement authorities under the 1990 Agreement Regarding Cooperation in the Prevention and Control of Money Laundering Arising from Illicit Trafficking in Narcotics Drugs and Psychotropic Substances, which entered into force on January 1, 1991. The information shared has supported U.S. domestic operations, resulting in the seizure of significant amounts of money and several arrests in the United States. Venezuela has a Mutual Legal Assistance Treaty (MLAT) with the United States.

The Government of Venezuela should take steps to move forward with the passage of the Organic Law Against Organized Crime, which has been under consideration by Congress for nearly three years. The passage of this bill will provide law enforcement and judicial authorities the much-needed tools for the effective investigation and prosecution of money laundering derived from all serious crimes, broaden asset forfeiture and sharing provisions, strengthen due diligence requirements, and expand the mandate of the Financial Intelligence Unit, the Unidad Nacional de Inteligencia Finaciera (UNIF). Venezuela should also expand and strengthen the capabilities of the Public Ministry to successfully investigate and prosecute crimes related to money laundering, and provide further training to financial regulators, investigators, prosecutors and judges. Venezuela should create and enact legislation to criminalize the financing of terrorism, as well as institute measures to expedite the freezing of terrorist assets. The passage of the Organic Law Against Organized Crime and legislation criminalizing the financing of terrorism would bring Venezuela into compliance with international standards for combating financial crimes.

Vietnam

The “drug economy” exists in Vietnam’s informal financial system. Vietnam is a major drug producing and drug-transit country. Vietnam is not an important regional or offshore financial center. The Vietnamese banking sector is underdeveloped and the Government of Vietnam (GVN) controls the flow of all U.S. dollars in official channels. Vietnamese officials assert that their strict banking regulations prevent money laundering and terrorist financing. However, the issue is difficult to monitor since there are no laws in effect at this time to support international money laundering investigations, resulting in a lack of legal and policy-driven authority for Vietnamese law enforcement officials to cooperate bilaterally. Vietnam has a large “shadow economy” in which U.S. dollars and gold are the preferred currency. Due to the limited size of Vietnam’s banking system and currency exchange controls, even legitimate businesses carry on transactions in this “shadow economy.” In addition, Vietnamese regularly transfer money though gold shops and other informal mechanisms to remit or receive funds from overseas. Officially, expatriate remittances account for $3 billion and unofficially the number may be more than double that amount.

There has been an increase in financial crimes, including but not limited to money laundering, as a result of the developing economy. Some of the transactions in both the formal and alternative remittance systems result from the proceeds of illegal narcotics sales, although the black market for smuggled goods is reportedly not significantly funded by the drug trade.

Vietnam has three free trade zones known as export processing zones (EPZ). Companies operating in EPZs manufacture goods for export and enjoy customs benefits (e.g., duty free for imported

materials). A foreign invested enterprise must have a license to operate in the EPZ. The investment license often stipulates what activities the company can do or what products they can manufacture.

Vietnam does not yet have a separate law on money laundering or terrorist financing. It is working on anti-money laundering legislation, in the form of a Decree that is expected to be issued in the first quarter of 2005. The Decree is expected to cover all serious crimes without specific reference to such offenses covered in the Penal Code. However, a Decree cannot create offenses. In addition, Article 251 of the Amended Penal Code criminalizes money laundering. The Counter-Narcotics Law, which took effect June 1, 2001, makes two narrow references to money laundering in relation to drug offenses: it prohibits the "legalizing" (i.e. laundering) of monies and/or property acquired by committing drug offenses (article 3.5); and it gives the Ministry of Public Security's specialized counternarcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. However, the implementing regulations have not yet been promulgated. The State Bank of Vietnam, which has the lead on countering terrorist financing, can also request the disclosure of information when it believes that a transaction might fall within this category. Furthermore, the State Bank requires banks to report suspicious transactions of any kind.

Under existing Vietnamese legislation, there are provisions for seizing of assets linked to drug trafficking. In the course of its drug investigations, MPS has seized vehicles, property and cash; though the seizures typically are directly linked to the drug crime and the final confiscation requires a court finding. Reportedly, MPS can notify a bank that an account is "seized" and that is sufficient to have the account frozen.

The Asian Development Bank is working with the GVN on draft banking legislation. The GVN is also working with international financial institutions to increase its banking supervision capabilities. Currently banks are required to maintain records from seven to up to 20 years. Banks are responsible for client confidentiality but are also required to provide information to law enforcement authorities for investigation purposes. Banks are responsible for checking all identification and relevant papers presented for opening accounts and implementing transactions. Foreign currency (including notes, coins and traveler's checks) in excess of $3,000, cash exceeding Vietnamese Dong (VND) 5,000,000 and gold of more than 300 grams must be declared at customs upon arrival and departure. There is no limitation on either the export or import of U.S. dollars or other foreign currency provided that all currency in excess of $3,000 (or its equivalent in other foreign currencies) or in excess of VND 5,000,000 in cash is declared upon arrival and departure, and supported by appropriate documentation. If excess cash is not declared, it is confiscated at the port of entry/exit and the passenger may be fined.

The GVN is a party to the 1988 UN Drug Convention and the 1999 International Convention for the Suppression of the Financing of Terrorism. It has signed but not yet ratified the UN Convention against Transnational Organized Crime. The GVN and the USG signed a Letter Of Agreement on Counternarcotics Cooperation in December 2003, to establish and to support projects designed to combat the production and trafficking of illicit narcotics and other forms of transnational criminal activities. The GVN has circulated to its financial institutions the lists of individuals and entities that have been included on the UNSCR 1267 sanctions committee's consolidated list as being linked to Usama Bin Ladin, members of the al-Qaida organization or the Taliban, and has reported that no names or assets have been identified. Vietnamese legal provisions on counterterrorism financing are covered in various legal documents such as the Law on Credit Organizations, the Penal Code (Article 84 and Article 20. paragraph 2) and others.

The Government of Vietnam should promulgate all necessary regulations to fully implement the Counter-Narcotics Law of 2001. While it should proceed with the planned anti-money laundering decree, Vietnam should also amend its Criminal Code to create expanded terrorism offenses, as a Decree cannot create offenses. Vietnam should establish a separate legal document governing the prevention and suppression of terrorism financing. Vietnam should ratify the UN Convention against

Transnational Organized Crime. Vietnam should enforce cross border currency controls and regulate the use of gold as an alternative remittance system. Vietnam should provide implementing regulations for international cooperation regarding both drug crimes and financial crimes and improve its informal cooperation and should become a member of the Asia/Pacific Group on Money Laundering (APG).

Yemen

The Yemeni financial system is not yet well developed. Thus, the extent of money laundering is not known. The prevalence of alternative remittance systems, such as hawala, makes financial institutions vulnerable to money laundering, although they are technically subject to limited monitoring by the Central Bank of Yemen (CBY). The banking sector is relatively small with 17 commercial banks, including four Islamic banks. The CBY supervises the banks. Local banks account for approximately 62 percent of the total banking activities, while foreign banks cover the other 38 percent.

Yemen's parliament passed a comprehensive anti-money laundering legislation (Law 35) in April 2003. The legislation criminalizes money laundering for a wide range of crimes, including narcotics offenses, kidnapping, embezzlement, bribery, fraud, tax evasion, illegal arms trading, and monetary theft, and imposes penalties of three to five years of imprisonment. Yemen has no specific legislation relating to terrorist financing. But terrorism is covered in various pieces of legislation that treat terrorism and its financing as serious crimes.

Law 35 requires banks, financial institutions, and precious commodity dealers to verify the identity of persons and entities that open accounts (or in the case of the dealers for those who execute a commercial transaction), to keep records of transactions for up to ten years, and to report suspicious transactions. In addition, the law requires that reports be submitted to an information-gathering unit within the CBY. The unit acts as the Financial Intelligence Unit (FIU), which in turn reports to the Anti-Money Laundering Committee (AMLC). The AMLC is composed of representatives from the Ministries of Finance, Foreign Affairs, Justice, Interior, and Industry and Trade, the Central Accounting Office, the General Union of Chambers of Commerce and Industry, the CBY, and the Association of Banks. The AMLC is authorized to issue regulations and guidelines and provide training workshops related to combating money laundering efforts.

In addition, Law 35 grants the AMLC the right to exchange information with foreign entities. The head of the AMLC is empowered by law to ask local judicial authorities to enforce foreign court verdicts based on reciprocity. Also, the law permits the extradition of non-Yemeni criminals in accordance with international treaties or bilateral agreements.

Prior to passage of the anti-money laundering law, the CBY issued Circular 22008 in April 2002, instructing banks and financial institutions that they must verify the legality of all proceeds deposited in or passing through the Yemeni banking system. The circular stipulates that financial institutions must positively identify the place of residence of all persons and businesses that establish relationships with them. The circular also requires that banks verify the identity of persons or entities that wish to transfer more than $10,000, when they have no accounts at the banks in question. The same provision applies to beneficiaries of such transfers. Banks must also take every precaution when transactions appear suspicious, and report such activities to the CBY. The circular was distributed to the banks along with a copy of the Basel Committee's "Customer Due Diligence for Banks," concerning "know your customer" procedures and "Core Principles for Effective Banking Supervision". The CBY issued Circular No. 4 on December 9, 2003, ordering banks to set up intelligence gathering units specializing in investigating and monitoring suspicious funds and transactions in their regulatory structures.

In 2003, U.S. Department of Homeland Security/Immigration and Customs Enforcement (DHS/ICE) agents in New York conducted an investigation of a company suspected of being involved in the smuggling and distribution of pseudoephedrine. The investigation disclosed that employees at the

business were sending a large number of negotiable checks to Yemen's capital city of Sanaa. Analysis of the documents seized as a result of search warrants and bank records revealed that the suspects had also wire transferred money to an individual with suspected ties to the al-Qaida organization. ICE agents also initiated an investigation pursuant to an outbound seizure of suspected hawala-generated funds seized en route to Yemen, concealed in jars of honey. The investigation disclosed that the courier and the reputed owner/broker of the funds were actively involved in a hawala network.

In response to the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and Yemen's Council of Ministers' directives, CBY issued two circulars (75304 and 75305) to all banks operating in Yemen, directing them to freeze accounts of 144 persons, companies, and organizations, and to report any finding to CBY. As a result, one account was immediately frozen. In September 2003, the CBY issued Circular No. 75304 containing a consolidated list of all persons and entities belonging to al-Qaida (182) and the Taliban (153). The Yemeni Government did not issue the circular again in 2004. Since the February 2004 addition of Sheikh Abdul Majid Zindani to the UNSCR 1267 Sanctions Committee's consolidated list, the Yemeni government has made no known attempt to enforce the sanctions and freeze his assets.

A law was passed in 2001 governing charitable organizations. This law entrusts the Ministry of Labor and Social Affairs with overseeing their activities. The law also imposes penalties of fines and/or imprisonment on any society or its members convicted of carrying out activities or spending funds for other than the stated purpose for which the society in question was established. The CBY Circular No. 33989 of June 1, 2002, and Circular No. 91737 of November 24, 2004, ordered banks to abide by the enhanced controls regulating the opening and management of the accounts of charities. This was in addition to keeping these accounts under continuous supervision in coordination with the Ministry of Labor and Social Affairs.

During 2004 the FIU and the CBY have been very active in enlightening the public and the financial sector, including money services businesses and money laundering reporting officers, about the proper ways and means of detecting and reporting suspicious financial transactions. They have done so through public forums and workshops. In addition, the AMLC has prepared an anti-money laundering procedural directory that will be distributed to all public and private financial institutions. The directory explains how to monitor and report suspected money laundering cases.

Yemen is one of the original signatories of the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENAFATF). The MENAFATF is a FATF-styled regional body that promotes best practices to combat money laundering and terrorist financing in the region. It was inaugurated in November 2004 in Bahrain by 14 Arab countries. Yemen is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Yemen is a party to the Arab Convention for the Suppression of Terrorism.

The Government of Yemen is making progress in enforcing its domestic anti-money laundering program. The passage of the 2003 anti-money laundering legislation represents a significant first step in meeting international standards. However, development of the FIU and international cooperation with criminal investigations are still in the initial development stages. The Central Bank of Yemen is still organizing its enforcement mechanism. Its effectiveness will demonstrate the authorities' commitment to ending money laundering. Yemen should also examine the prevalence of alternative remittance systems such as hawala and trade-based money laundering. As a next step, Yemen should enact specific legislation with respect to terrorist financing and forfeiture of the assets of those suspected of terrorism. It should ratify the UN Convention against Transnational Organized Crime. It should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Zambia

Zambia is not a major financial center. To the extent that money laundering is a concern in Zambia, reports indicate that proceeds of narcotics transactions and money derived from public corruption are the major sources of laundered money. Law enforcement officials also indicate that bulk cash smuggling is a concern.

The Prohibition and Prevention of Money Laundering Act of 2001 makes money laundering a criminal offense, stiffens penalties for financial crimes, requires financial institutions to report suspicious transactions to regulators and retain transaction records for a period of ten years, allows seizure of assets related to money laundering, and increases the investigative and prosecutorial powers of the Drug Enforcement Commission (DEC). It also establishes an Anti-Money Laundering Authority that is chaired by the attorney general and includes the heads of Zambia's principal law enforcement agencies, Revenue Authority, and Central Bank. The DEC has the responsibility for investigating money laundering offenses. When regulatory agencies have reason to suspect money laundering, they must report this to the DEC, which acts as the enforcement arm of the anti-money laundering authority, and make relevant records available to investigators. The law authorizes investigators to seize property when they have reasonable grounds to believe that it is derived from money laundering. Following a conviction under the anti-money laundering law, the court may order the forfeiture to the state of property seized during an investigation.

The anti-money laundering law does not contain specific provisions on the financing of terrorism; the Government of the Republic of Zambia (GRZ) does have the authority to order financial institutions to freeze assets, but this can be difficult if there is no evidence of a domestic crime. Zambia lacks comprehensive and reliable mechanisms for freezing the assets of terrorist organizations.

In 2003, the GRZ established an anti-money laundering unit under the DEC. The main purpose of the unit is to lead efforts within the GRZ to counter money laundering and enforce the Prevention of Money Laundering Act. In the same year, three officers of a commercial bank were tried and convicted for money laundering offenses. In 2004, the DEC conducted numerous investigations of money laundering, resulting in several arrests under the 2001 anti-money laundering statute. Trials in these cases are pending. The penalty for money laundering is imprisonment for a term not exceeding ten years and/or a fine.

In 2003, Zambia signed the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) memorandum of understanding. In 2004, Zambia's Central Bank was an active participant in ESAAMLG activities. Zambia is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime. Zambia is a party to the 1988 UN Drug Convention.

The Government of Zambia should establish a fully operational financial intelligence unit in accordance with international standards. Zambia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Zambia should also criminalize terrorist financing and implement counterterrorist financing regulations that comport with the FATF recommendations, including the Special Recommendations on Terrorist Financing

Zimbabwe

Zimbabwe is not a regional financial center and is not considered to be at significant risk for money laundering. However, it faces a serious problem with official corruption, which generates substantial funds that need to be concealed.

Narcotics-related money laundering was previously criminalized in Zimbabwe's Anti-Money Laundering Act. In 2004, the Government of Zimbabwe passed the Anti-Money Laundering and Proceeds of Crime Act. The new Act applies the anti-money laundering law to all serious offenses. It requires banks to maintain records sufficient to reconstruct individual transactions for at least six years. The 2004 Act mandates a prison sentence of up to five years for a money laundering conviction. The 2004 Act also addresses terrorist financing and authorizes the tracking and seizing of assets. Given the Government's history of using the legal system selectively and aggressively to target political opponents, the new Act has raised human rights concerns, although its use to date has not been associated with any reported due process abuses nor provoked any serious public opposition. However, the Government also has yet to make much use of the new law.

Over the past year, the Government has arrested many prominent Zimbabweans for activities it calls "financial crimes." Most of these "crimes" involve violations of currency restrictions that criminalize the externalization of foreign exchange activities conducted by many Zimbabwean businesses with substantial volumes of imports or exports (i.e., transferring assets offshore). To date, the Anti-Money Laundering Act has not been employed in the selective prosecution of individuals for such "crimes."

When requested, the banking community has generally cooperated with the Government in the enforcement of other laws involving tracking of assets, such as laws restricting the externalization of foreign currency. The banking community and Central Bank also have cooperated with the U.S. in global efforts to identify individuals and organizations associated with terrorist financing.

Zimbabwe is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the United Nations Convention against Transnational Organized Crime. Zimbabwe has yet to sign the UN International Convention for the Suppression of the Financing of Terrorism. Zimbabwe joined the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body, in August 2003. However, Zimbabwe has yet to sign the ESAAMLG Memorandum of Understanding (MOU).

The Government of Zimbabwe should become a party to both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. It should sign the MOU for the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) and participate actively in that body.