Malaysia

Malaysia is not a regional center for money laundering. However, its formal and informal financial sectors are vulnerable to abuse by narcotic traffickers, financiers of terrorism, and criminal elements. Malaysia's relatively lax customs inspection at ports of entry and free trade zones, its uneven enforcement of intellectual property rights, and its offshore financial services center serve to increase its vulnerability.

Since 2000, Malaysia has made significant progress in constructing a comprehensive anti-money laundering regime. Malaysia's National Coordination Committee to Counter Money Laundering (NCC), comprised of members from 13 government agencies, oversaw the drafting of Malaysia's Anti-Money Laundering Act 2001 (AMLA) and coordinates government-wide anti-money laundering efforts.

The AMLA, enacted in January 2002, criminalized money laundering and lifted bank secrecy provisions for criminal investigations involving more than 150 predicate offenses. The law also created a financial intelligence unit (FIU) located in the Central Bank, Bank Negara Malaysia (BNM). The FIU is tasked with receiving and analyzing information, and sharing financial intelligence with the appropriate enforcement agencies for further investigations. The Malaysian FIU works with more than twelve other agencies to identify and investigate suspicious transactions.

The Government of Malaysia (GOM) has a well-developed regulatory framework, including licensing and background checks, to oversee onshore financial institutions. BNM's guidelines require customer identification and verification, financial record keeping, and suspicious activity reporting. These guidelines are intended to require banking institutions to determine the true identities of customers opening accounts and to develop a transaction profile of each customer in order to identify unusual or suspicious transactions. A comprehensive supervisory framework has been implemented to audit financial institutions' compliance with AMLA. Currently, there are 300 examiners who are responsible for money laundering inspections for both onshore and offshore banks

Malaysia has strict "know your customer" rules under the AMLA. Every transaction, regardless of its size, is recorded. Reporting institutions must maintain records for at least six years and report any suspicious transactions to Malaysia's financial intelligence unit, Unit Perisikan Kewangan-Bank Negara Malaysia. Regardless of the transaction size, if the reporting institution deems a transaction suspicious, it must report that transaction to the FIU. Officials indicate that they receive regular reports from institutions, but cannot divulge the volume or frequency of such reports. Reporting individuals and their institutions are protected by statute with respect to their cooperation with law enforcement. While Malaysia's bank secrecy laws prevent general access to financial information, those secrecy provisions are waived in the case of money laundering investigations.

Malaysia has adopted due diligence or banker negligence laws that make individual bankers responsible if their institutions launder money. Both reporting institutions and individuals are required to adopt internal compliance programs to guard against any offense. Under the AMLA, any person or group that engages in, attempts to engage in, or abets the commission of money laundering, would be subject to criminal sanction. All reporting institutions are required to file suspicious transaction reports and are subject to the same review by the FIU and other law enforcement agencies. Reporting institutions include: commercial banks, Islamic banks, money changers, discount houses, insurers, insurance brokers, Islamic insurance and reinsurance (takaful and retakaful) operators, offshore banks, offshore insurers, offshore trusts, the Pilgrim's Fund (to pay for Hajj trips to Mecca), Malaysia's postal service, development banks such as Malaysia's National Savings Bank (Bank Simpanan Nasional), the People's Cooperation Bank (Bank Kerjasama Rakyat Malaysia Berhad), and licensed casinos.

By using a consultative approach, Malaysia's FIU continues to expand the scope of institutions that must report suspicious transactions. This approach encouraged Malaysia's professional societies for lawyers and accountants to add suspicious transaction reporting requirements to their bylaws. Likewise, in consultation with the Security Commission, stockbrokers and brokerage houses are now required to submit suspicious transaction reports. Other designated professions include public notaries and company secretaries. The Government's consultative approach has minimized potential political fallout from the statute's expansion.

Malaysia's Islamic finance sector, accounting for approximately 11 percent of total deposits, is subject to the same strict supervision to combat financial crime as the commercial banks. A combination of legacy exchange controls imposed after the 1997-98 Asian financial crisis and robust regulation and supervision by the Central Bank makes the Islamic financial sector as unattractive to financial criminals as is the conventional financial sector.

In 1998 Malaysia imposed foreign exchange controls that restrict the flow of the local currency, the ringgit, from Malaysia. Onshore banks must record cross-border transfers over RM5,000 (approximately $1,326). Since April 2003, an individual form is completed for each transfer above RM50,000 (approximately $13, 260). Recording is done in a bulk register for transactions between RM5,001 and RM50,000. Banks are obligated to record the amount and purpose of these transactions.

Malaysia's offshore banking center on the island of Labuan, is more vulnerable to money laundering and the financing of terrorism than the rest of the formal financial sector in Malaysia. However, its regulation of the offshore banking sector has improved over the past few years. The Labuan Offshore Financial Services Authority (LOFSA) is under the authority of the Central Bank, Bank Negara. The offshore sector has different regulations for the establishment and operation of offshore businesses. But the same anti-money laundering laws as those governing domestic financial service providers govern the offshore sector. Offshore banks, insurance companies, and trust companies are required to file suspicious transaction reports under the country's anti-money laundering law.

LOFSA licenses offshore banks, banking companies, trusts, and insurance companies, and performs stringent background checks before granting an offshore license. The financial institutions operating in Labuan are generally among the largest international banks and insurers. Nominee (anonymous) directors are not permitted for offshore banks, trusts or insurance companies. Labuan has 5,022 registered offshore companies, money banking companies, trusts, and insurance companies. Offshore companies must be established through a trust company. Trust companies are required by law to establish true beneficial owners and submit suspicious transaction reports as necessary. Conversely, there is no requirement to reveal the true identity of the beneficial owner of international corporations. LOFSA officials may require any organization operating in Labuan to disclose information on its beneficial owner or owners. Bearer instruments are strictly prohibited in Labuan. Over the past few years, LOFSA has injected more formality into the system by working with the FIU to require training on the reporting requirements covered under the AMLA.

Presently, Labuan has 59 offshore banks in operation, along with 112 insurance and insurance-related companies, 68 leasing operations, 37 fund management groups (19 private funds, 3 public funds, and 15 fund management companies), 20 trust companies, and 3 money broking companies. Many of the companies in Labuan are Japanese firms established primarily to service Japanese companies in Malaysia. Malaysia bans offshore casinos and Internet gaming sites.

The Free Zone Act of 1990 is the enabling legislation for free trade zones in Malaysia. The zones are divided into Free Industrial Zones (FIZ), where manufacturing and assembly takes place, and Free Commercial Zones (FCZ), generally for warehousing commercial stock. The Minister of Finance may designate any suitable area as an FIZ or FCZ. Currently there are 13 FIZs and 12 FCZs in Malaysia. The Minister of Finance may appoint any federal, state, or local government agency or entity as an authority to administer, maintain and operate any free trade zone. Legal treatment for such zones is

also different. The time needed to obtain such licenses from the administrative authority for the given free trade zone depends on the type of approval. Clearance time ranges from two to eight weeks. There is no information available suggesting that Malaysia's free industrial and free commercial zones are being used for trade-based money laundering schemes or by the financiers of terrorism. However, the GOM considers these zones as areas outside the country, and they receive lenient tax and customs treatment relative to the rest of the country.

In April 2002, the GOM passed the Mutual Assistance in Criminal Matters Bill and has concluded Mutual Legal Assistance treaties with several regional countries. In 2004, Malaysia made its first money laundering arrest, which ended in a conviction in December 2005. The Government of Malaysia has added five new arrests in 2005, with a total of 188 money laundering charges valued at RM 29.9 million ($7.9 million). Malaysia cooperates with regional, multilateral, and international partners to combat financial crimes and permits foreign countries to check the operations of their banks' branches. The FIU has signed memoranda of understanding (MOUs) with the FIUs of Australia, Indonesia, Thailand, and the Philippines. MOUs with the United States, the United Kingdom, China, Japan, South Korea, the Netherlands, Finland, Albania, and Argentina are reportedly pending.

In March 2006, the GOM expects to enact amendments to five different pieces of legislation that will enable it to accede to the UN Convention on the Suppression of the Financing of Terrorism. Parliament passed amendments to the Anti-Money Laundering Act, the Penal Code, the Subordinate Courts Act, and the Courts of Judicature Act in November 2003. The criminal procedure code is the last major piece of domestic legislation that needs amendment before all of the legislation can be incorporated into domestic law (a select committee has finished its review and plans to submit the final draft early 2006). The amendments to the AMLA, once enacted, will make the financing of terrorism one of the 185 predicate offenses for which money laundering can be charged as a crime. When implemented, the 2003 amendments will increase penalties for terrorist acts, allow for the forfeiture of terrorist-related assets, allow for the prosecution of individuals who provide material support for terrorists, expand the use of wiretaps and other surveillance of terrorist suspects, and permit video testimony in terrorist cases. Malaysia is also a party to the 1988 UN Drug Convention. Malaysia is a party to the UN Convention against Transnational Organized Crime .

The GOM has cooperated closely with U.S. law enforcement in investigating terrorist-related cases since the signing of a joint declaration to combat international terrorism with the United States in May 2002. The GOM currently has the authority to identify and freeze terrorist or terrorist-related assets, and has issued orders to all licensed financial institutions, both onshore and offshore, to freeze the assets of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. The Ministry of Foreign Affairs opened the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) in August 2003, which has hosted a series of counterterrorism courses and seminars, including training on counterterrorism finance.

The GOM has rules regulating charities and other non-profit entities. The Registrar of Societies is the principal government official who supervises and controls charitable organizations, with input from the Inland Revenue Board and occasionally the Companies Commission. The Registrar mandates that every registered society of a charitable nature submits its annual returns, which include financial statements. Should the Registrar find activities he deems suspicious, he may revoke their registration or file a suspicious transaction report. The FIU plans to conduct a review of the non-profit sector with the Registrar and the Companies Commission to ensure that they are well-regulated and following their bylaws. Malaysia's tax law allows contributions to charitable organizations (zakat, as required by Islam) to be deducted from one's total tax liability, encouraging the reporting of such contributions. Islamic zakat contributions can be taken as payroll deductions, another tool to prevent the abuse of charitable giving.

Malaysia has endorsed the Basel Committee's Core Principles for Effective Banking Supervision. Labuan Offshore Financial Services Authority serves as a member of the Offshore Group of Banking Supervisors. Malaysia is a member of the Asia/Pacific Group on Money Laundering. Malaysia's FIU gained membership to the Egmont Group of financial intelligence units in July 2003. Malaysia generally follows international standards related to money laundering, including the FATF Forty Recommendations on Money Laundering and the Nine Special Recommendations on Terrorist Financing. The FIU has provided capacity building and training in anti-money laundering efforts to some of its ASEAN partners, including Cambodia, Laos, and Vietnam. In February 2006, the Asian Development Bank (ADB) will be funding a team from the FIU to run a workshop in Laos for two state-owned banks, and then draft Laos's anti-money laundering compliance procedures by the end of September.

The GOM continues to make a broad, sustained effort to combat money laundering and terrorist financing flows within its borders. To further strengthen its anti-money laundering regime, Malaysia should insist on the identification and registration of the true beneficial owners of the more than 5,000 international business companies of Labuan. The Malaysian parliament is expected to enact terrorist financing legislation in 2006, and on that basis, Malaysia should accede to the UN International Convention for the Suppression of the Financing of Terrorism and to all other terrorist-related UN conventions.

Marshall Islands

The Republic of the Marshall Islands (RMI), a group of atolls located in the North Pacific Ocean, is a sovereign state in free association with the United States. The population of RMI is approximately 60,000. The financial system in RMI has total banking system assets of $95.4 million and total deposits of $53.1 million. The RMI financial sector consists of two commercial banks, one of which is insured by the Federal Deposit Insurance Corporation (FDIC), and a government-owned development bank whose primary function is to perform development lending in government-prioritized sectors; there are also several low-volume insurance agencies that primarily sell policies on behalf of foreign insurance companies. In realization of the country's vulnerability to systemic shock in the financial sector, the government introduced a reform program geared toward enhancing transparency, accountability, and good governance. Among other initiatives, the reform program called for the establishment of the requisite infrastructure for detecting, preventing, and combating money laundering and terrorist financing.

The Marshall Islands has not seen an increase in financial crime in recent years. There have not been any prosecutions for money laundering. However, an evolving trend that poses a challenge to RMI's anti-money laundering/counterterrorist financing effort is the significant outflow of cash, generally attributed to expatriate businesses sending proceeds out of the country. There is currently no requirement to report cross-border currency transfers.

Money laundering has been criminalized and customer identification and suspicious transaction reporting mandated. The Marshall Islands also issued guidance to its financial institutions for the reporting of suspicious transactions. In addition, the RMI drafted anti-money laundering regulations.

In November 2000, the Government of the Marshall Islands (GRMI) approved the establishment of a financial intelligence unit that may exchange information with international law enforcement and regulatory agencies. The Domestic Financial Intelligence Unit (DFIU) is located within the Banking Commission. The DFIU has the power to receive, analyze, and disseminate financial intelligence. In 2003, its processes were streamlined and automated to the fullest extent possible. In December 2005, the DFIU installed a system for banking institutions, under the supervision of the Banking Commission, to electronically submit suspicious activity reports (SAR) and currency transaction

reports (CTRs). The system utilizes Analyst Notebook software that allows the DFIU to review and analyze the data links between related transactions.

In May 2002, the GRMI passed and enacted its Anti-Money Laundering Regulations, 2002. The 2002 regulations provide the standards for reporting and compliance within the financial sector. Components of this legislation include reporting of beneficial ownership, internal training requirements regarding the detection and prevention of money laundering by financial institutions, record keeping, and suspicious and currency transaction reporting. Additionally, the Banking Commission and the Attorney General's office worked with the Federal Deposit Insurance Corporation to develop a set of examination policies and an examination procedures manual. Both sets of documents are being used by examiners from the Banking Commission as guides in the on-site reviews of banks' and financial institutions' compliance with the anti-money laundering regulations. Since the establishment of the statutory and regulatory framework, the Banking Commission has conducted on-site examinations of financial institutions and cash dealers. Money laundering controls extend to all financial institutions, but do not cover professionals, i.e., lawyers and accountants. However, individuals can be held liable for money laundering violations by their institutions.

Under the Banking Amendment, the Proceeds of Crime Act, and the Counter-Terrorism Act, the RMI can freeze, seize, and upon conviction transfer to the general fund, the proceeds of any crime that results in a one-year or greater sentence. Provisions allow for a broad range of forfeiture: any real or personal property owned by the person, any property used in the crime, and any proceeds of the crime. The Mutual Assistance Act allows the transfer to a requesting government of proceeds of such a crime committed in a foreign country. The Counter-Terrorism Act provides for the closing of any businesses involved in exporting or importing terrorist funds or supplies. These laws allow for both civil and criminal forfeiture. Although the laws are designed to meet the GRMI's international obligations, their effectiveness has not been tested, as there has been no terrorist activity in the RMI and therefore no seizures.

Depending on the nature of the offense, the Attorney General or the Banking Commission would be responsible for enforcement and for seizures of assets. Police powers are adequate, but resources are limited. However, the GRMI retains a close relationship to U.S. institutions and could call on them for assistance in cases of concern to the United States. Assets can be frozen "without undue delay."

Since the passage of its anti-money laundering law, and a suite of counterterrorism laws, as well as the subsequent promulgation of implementing regulations, the GRMI has undertaken a number of initiatives to further strengthen its anti-money laundering/counterterrorist financing (AML/CFT) regime. The government and local institutions have received positive reports from the Financial Action Task Force (FATF).

However, a very significant problem has resulted from efforts to comply with AML/CFT requirements. This issue is causing a system-wide disturbance in banking and more specifically in transaction settlement and clearance. The Bank of the Marshall Islands (BOMI), in an effort to assure full compliance, commissioned an internal audit of its procedures and controls in 2003. The results of that audit identified several weaknesses which BOMI has taken steps to correct. However, the existence of the audit, and fears of sanctions under the Bank Secrecy Act and the USA PATRIOT Act, led Citizens Security Bank of Guam to discontinue its "payable through" relationship with BOMI, effective February 15th, 2004. Suspension of "payable through" meant that BOMI checks cannot be used outside the country. This situation has disrupted that status quo in the business community. The second largest population center, Ebeye, has no banking services available for international transactions, as there is no Bank of Guam branch on Ebeye. This remained a serious problem to the RMI in 2005, as there are only two financial institutions in operation. Customers on Majuro have shifted deposits to the Bank of Guam, which closes all avenues for healthy competition on demand

deposit accounts between the two available banks. The RMI has limited possibilities to seek reinstatement of a "payable through" for its local bank.

The RMI offshore financial sector is vulnerable to money laundering. Nonresident corporations (NRCs), the equivalent of international business companies, can be formed. Currently, there are 5,500 registered NRCs, half of which are companies formed for registering ships. NRCs are allowed to offer bearer shares. Corporate officers, directors, and shareholders may be of any nationality and live anywhere. NRCs are not required to disclose the names of officers, directors, and shareholders or beneficial owners, and corporate entities may be listed as officers and shareholders. The corporate registry program, however, does not allow the registering of offshore banks, offshore insurance firms, and other companies which are financial in nature.

Although NRCs must maintain registered offices in the Marshall Islands, corporations can transfer domicile into and out of the Marshall Islands with relative ease. Marketers of offshore services via the Internet promote the Marshall Islands as a favored jurisdiction for establishing NRCs. In addition to NRCs, the Marshall Islands offer nonresident trusts, partnerships, unincorporated associations, and domestic and foreign limited liability companies. Offshore banks and insurance companies are not permitted in the Marshall Islands.

Having established the requisite supervisory processes to ensure compliance with legislative mandates for detection and suppression of money laundering and terrorist financing, the GRMI's main emphasis was on fine-tuning these processes. After undertaking nine on-site examinations of financial institutions, following procedures developed in cooperation with the FDIC, the Banking Commission has now gained a better understanding of the risk profile of these institutions with respect to their exposure to money laundering and terrorist financing. This has proven especially useful in amalgamating some supervisory processes with the routine FIU processes, thereby maximizing benefit for the limited resources available to the GRMI. The Banking Commission had planned that some of the supervisory processes would be incorporated into the required annual audits of banks. This initiative has been fully implemented since 2004. The Banking Commission recruited an Assistant Commissioner who is spearheading this task along with other examination tasks relating to anti-money laundering compliance and prudential banking practices.

The GRMI has enacted a Proceeds of Crime Act, Counter-Terrorism Act, and Foreign Evidence Act. Although the GRMI is not a signatory to the 1988 UN Convention, RMI is a party to all 12 major UN conventions and protocols for terrorism including the UN International Convention for the Suppression of the Financing of Terrorism.

The Marshall Islands is a member of the Asia/Pacific Group on Money Laundering. The DFIU became a member of the Egmont Group in June 2002. RMI is also a founding member of the recently established Association Financial Supervisors of Pacific Islands Countries, a group of regulators from the Pacific Islands Forum countries that will be representing the region in the Basel group.

The GRMI has stabilized its key defenses against money laundering and terrorist financing, and has commenced work aimed at aligning its anti-money laundering system with the revised 40 plus 9 Recommendations of the Financial Action Task Force on Money Laundering. The Republic of the Marshall Islands should become a party 1988 UN Drug Convention. Additionally, the GRMI should require the identification of the beneficial owners of Non-resident Corporations.

Mexico

The illicit drug trade continues to be the principal source of funds laundered through the Mexican financial system. Mexico is a major drug producing and drug-transit country. Mexico also serves as one of the major conduits for proceeds from illegal drug sales leaving the United States. Other crimes, including corruption, kidnapping, firearms trafficking, and immigrant trafficking are also major

sources of illegal proceeds. The smuggling of bulk shipments of U.S. currency into Mexico and the movement of the cash back into the United States via couriers, armored vehicles, and wire transfers, remain favored methods for laundering drug proceeds. Mexico's financial institutions are vulnerable to currency transactions involving international narcotics trafficking proceeds that include significant amounts of U.S. currency or currency derived from illegal drug sales in the United States.

Currently, there are 29 commercial banks and 71 foreign financial representative offices operating in Mexico, with seven commercial banks representing 89 percent of total assets in the banking sector. Commercial banks, foreign exchange companies, and general commercial establishments are allowed to offer money exchange services. Mexico has 87 insurance companies, 13 bonding institutions, 178 credit unions, and 24 money exchange houses. The size of the underground economy is unknown, although it is estimated to account for anywhere between 20 and 40 percent of the gross domestic product in Mexico. However, the informal economy is considered to be much less of a problem overall than that of the narcotics-driven segments of the economy. Beginning in 2005, permits were issued for casinos to operate in Mexico. Gambling is also legally allowed through national lotteries, horse races, and sport pools. Casinos and offshore banks are currently not subject to anti-money laundering reporting requirements.

Since 2000, Mexicans have received an estimated $52 billion in remittances, and conservative estimates indicate that this amount will increase to over $80 billion by the end of 2006. Remittances from the United States to Mexico reached a record high $20 billion in 2005. Although non-bank companies continue to dominate the market for remittances, many U.S. banks have teamed up with their Mexican counterparts to develop systems to simplify and expedite the transfer of money. These measures include wider acceptance by U.S. banks of the matricula consular, an identification card issued by Mexican consular offices to Mexican citizens residing in the United States that has been criticized, based on security issues. In some cases, neither the sender nor the recipient of a remittance is required to open a bank account in the United States or Mexico, but must simply provide the matricula consular as identification and pay a flat fee. Although these systems have been designed to make the transfer of money faster and less expensive for the customers, the rapid movement of such vast sums of money by persons of questionable identity leaves the new money transfer systems open to potential money laundering and exploitation by organized crime groups.

According to U.S. law enforcement officials, Mexico remains one of the most challenging money laundering jurisdictions for the United States, especially with regard to the investigation of money laundering activities involving the cross-border smuggling of bulk currency from drug transactions. While Mexico has taken a number of steps to improve its anti-money laundering system, significant amounts of narcotics-related proceeds are still smuggled across the border. In addition, such proceeds can still be introduced into the financial system through Mexican banks or casas de cambio, or repatriated across the border without record of the true owner of the funds. Corruption is also a concern. In recent years, various Mexican officials, including former officials from the Mexico City government, have come under investigation for alleged money-laundering activities.

In 2005, U.S. authorities observed a significant increase in the number of complex money-laundering investigations by the Financial Crimes Unit of the Office of the Deputy Attorney General Against Organized Crimes (SIEDO), including cases coordinated with U.S. officials. The U.S. Treasury Department's Office of Foreign Asset Control (OFAC) announced in January 2005 the designation of 39 "Tier II" targets involved in significant narcotics trafficking. Some of these designations centered on foreign exchange centers, which fall under the supervision of the Secretariat of Finance and Public Credit (Hacienda). The designation of these companies, which are associated with the previously designated Arellano Felix drug trafficking organization, under the Foreign Narcotics Kingpin Designation Act, resulted from cooperation among OFAC, other U.S. government entities and SIEDO. These designations allowed U.S. and Mexican authorities to seek the freezing of assets of Mexican drug cartels, hindering their ability to take advantage of the U.S. and Mexican financial systems.

The Government of Mexico (GOM) continues efforts to implement an anti-money laundering program according to international standards such as those of the Financial Action Task Force (FATF), which Mexico joined in June 2000. Money laundering related to all serious crimes was criminalized in 1996 under Article 400 bis of the Federal Penal Code, and is punishable by imprisonment of five to fifteen years and a fine. Penalties are increased when a government official in charge of the prevention, investigation, or prosecution of money laundering commits the offense.

In 1997, the GOM established a financial intelligence unit (FIU) under the Hacienda. Previously known as the Dirección General Adjunta de Investigación de Operaciones (DGAIO), the FIU was renamed the Unidad de Inteligencia Financiera (UIF) in 2004 with the consolidation of all of the Hacienda offices responsible for investigating financial crimes into the UIF. The UIF is responsible for receiving, analyzing and disseminating financial reports from a wide range of obligated entities. The UIF also reviews all crimes linked to Mexico's financial system and examines the financial activities of public officials. The UIF's personnel number approximately 70—mostly forensic accountants, lawyers, and analysts. Its director reports to the Minister of Finance.

Regulations have been implemented for banks and other financial institutions (mutual savings companies, insurance companies, financial advisers, stock markets, and credit institutions), as well as exchange houses, and money remittance businesses to know and identify customers and maintain records of transactions. These entities must report suspicious transactions, transactions over $10,000, and transactions involving employees of financial institutions who engage in unusual activity to the UIF. Financial institutions with a reporting obligation now require occasional customers performing transactions equivalent to or exceeding $3,000 in value to be identified, so the transactions can be aggregated daily to prevent circumvention of the requirements to file cash transaction reports (CTR) and suspicious transaction reports (STR). Financial institutions also have implemented programs for screening new employees and verifying the character and qualifications of their board members and high-ranking officers. Real estate brokerages, attorney, notaries, accountants and dealers in precious metals and stones are required under a November 2005 provision of the tax law to report all transactions exceeding $10,000 to the UIF, via the Tax Administration Service. In 2005, the FIU received approximately 4,800,000 CTRs and 57,700 STRs from obligated entities.

In December 2000, Mexico amended its Customs Law to reduce the threshold for reporting inbound cross-border transportation of currency or monetary instruments from $20,000 to $10,000. At the same time, it established a requirement for the reporting of outbound cross-border transportation of currency or monetary instruments of $10,000 or more. These reports are also received by the UIF. Efforts are ongoing to compare the declarations filed in Mexico with those filed in the U.S. to determine compliance with this reporting requirement. However, Mexico's reporting requirements include a wider range of monetary instruments (e.g. bank drafts) than those of the United States.

Following the analysis of CTRs and STRs, the UIF sends reports that are deemed to require further investigation, and have been approved by Hacienda's legal counsel, to the Office of the Attorney General (PGR). As of November, the UIF had sent 56 cases to the PGR in 2005. The PGR's special financial crimes unit is part of SIEDO, which works closely with the UIF in carrying out money laundering investigations. The PGR and SHCP instituted and strengthened coordination between the two ministries with the signing of memoranda of understanding (MOUs) in June 2004 and October 2005. In addition to working with SIEDO, UIF personnel have initiated working-level relationships with other federal law enforcement entities, including the Federal Investigative Agency (AFI), in order to support the investigations of criminal activities with ties to money laundering. The UIF is also negotiating MOUs with the Ministry of the Economy and the Ministry for Immigration that would allow the UIF access to their databases.

In September 2003, Mexico underwent its second mutual evaluation by the FATF, and the findings of the evaluation team were accepted at the FATF plenary meetings in June 2004. The evaluation team

found that the GOM had made progress since the first mutual evaluation by removing specific exemptions to customer identification obligations, implementing on-line reporting forms and a new automated transmission process for reporting transactions to the UIF, and slightly reducing the delay in reporting transactions overall. The GOM also developed an overall anti-money laundering strategy and plan.

However, the FATF evaluation team also identified a number of deficiencies in the system. Mexico does not have a separate offense of terrorist financing. Bank and trust secrecy were considered impediments to many aspects of Mexico's anti-money laundering/counterterrorist financing system, particularly for law enforcement and prosecutorial and judicial authorities during investigations and prosecutions. As a result of these deficiencies, the GOM must update the FATF on its progress, which it did at the June and October 2005 plenary meetings of the FATF. While Mexico has not yet criminalized terrorist financing, it has made improvements to its bank secrecy laws. Amendments to the Banking Law that were approved in April 2005 now allow specific government entities, such as the PGR and the state attorney generals, to receive records directly from banks without prior approval from the National Banking and Securities Commission (CNBV). Previously, all requests to lift bank secrecy had to be approved by the CNBV. Financial institutions must respond to these requests within three days.

In November 2003, the Senate passed a bill amending the Federal Penal Code that would link terrorist financing to money laundering. However, little progress was made with regard to the passage of this bill by the Congress. In 2005, the draft legislation was re-submitted as two separate draft laws: one to criminalize the financing of terrorism and one to address outstanding international cooperation issues. This legislation, once passed, is intended to bring Mexico into compliance with international standards. The proposed amendments would also create two new crimes: conspiracy to launder assets and international terrorism (when committed in Mexico to inflict damage on a foreign state). The draft legislation is currently under consideration in the Senate.

Although Mexico does not have a specific crime criminalizing the financing of terrorism because terrorism is declared to be a serious crime, money laundering associated with terrorism is punishable under the existing Penal Code. The GOM has responded to U.S. Government (USG) efforts to identify and block terrorist-related funds, and, although no assets were frozen, it continues to monitor suspicious financial transactions.

Although the United States and Mexico both have forfeiture laws and provisions for seizing assets abroad derived from criminal activity, USG requests to Mexico for the seizure, forfeiture, and repatriation of criminal assets have not met with success, as Mexican authorities have difficulties with assets seized for forfeiture in Mexico if these assets are not clearly linked to narcotics. Most assets seized during law enforcement operations go to the Service for the Management and Transfer of Assets (SAE), a semi-autonomous branch of the Hacienda established in late 2002. Although Mexican officials have made significant progress in modernizing their approach to asset seizure, actual asset forfeiture remains a challenge. In two significant U.S. cases involving fraud, authorities seized real property and money generated from the crime. Although authorities gained forfeiture of the property in the United States, counterparts in Mexico did not carry out such orders in Mexico, nor have they returned related assets to the United States for forfeiture.

Mexico has developed a broad network of bilateral agreements with the United States, and regularly meets in bilateral law enforcement working groups with the United States. The U.S.-Mexico Mutual Legal Assistance Treaty entered into force in 1991. The GOM and the USG continue to implement other bilateral treaties and agreements for cooperation in law enforcement issues, including the Financial Information Exchange Agreement (FIEA) and the memorandum of understanding (MOU) for the exchange of information on the Cross-border Movement of Currency and Monetary Instruments. In February 2005, the UIF and the U.S. financial intelligence unit, FinCEN, signed an

MOU further detailing the procedures for information exchange. The U.S. Customs Service and Mexico City entrepreneurs have established a Business Anti-Smuggling Coalition, including a financial BASC chapter created to deter money laundering, which remained active in 2005.

In addition to its membership in the FATF, Mexico participates in the Caribbean Financial Action Task Force as a cooperating and supporting nation and in the South American Financial Action Task Force as an observer member. Mexico is a member of the Egmont Group and the OAS/CICAD Experts Group to Control Money Laundering. The GOM is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the UN International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention Against Terrorism. The UIF has signed memoranda of understanding for the exchange of information with the FIUs of Argentina, Bolivia, Brazil Colombia, Chile, Dominican Republic, El Salvador, Guatemala, Honduras, Paraguay, Peru and Ukraine, in addition to the MOU with the United States.

The Government of Mexico should fully implement and improve the mechanisms for asset forfeiture and money laundering cooperation with the United States, and should increase efforts to control the bulk smuggling of currency across its borders. Mexico should also closely monitor remittance systems for possible exploitation by criminal or terrorist groups. Mexico should enact its proposed legislation to criminalize the financing and support of terrorists and terrorist organizations. Furthermore, despite the preventive mechanisms that have been put in place, improved cooperation among law enforcement authorities and a strong public campaign against corruption, Mexico continues to face challenges in prosecuting and convicting money launderers, and should continue to focus its efforts on improving its ability to do so.

Monaco

The second-smallest country in Europe, the Principality of Monaco is known for its tradition of bank secrecy, network of casinos, and favorable tax regime. The principality does not face the ordinary forms of organized crime, and the crime that does exist does not seem to generate significant illegal proceeds (save for fraud and offenses under the "Law on Checks"); rather, money laundering offenses relate mainly to offenses committed abroad. Russian organized crime and the Italian Mafia reportedly have laundered money in Monaco. Monaco remains on an OECD list of so-called "non-cooperative" countries in terms of provision of tax information.

Monaco has a population of approximately 32,000, of which only 7,000 are Monegasque nationals. Monaco's approximately 60 banks and financial institutions hold more than 300,000 accounts and manage total assets of about 70 billion euros ($82.5 billion). Approximately 85 percent of the banking customers are nonresident. In 2002, the financial sector represented over 17 percent of Monaco's economic activity. Monaco's non-banking financial institutions include insurance companies, portfolio management companies, and trusts created through notaries, of which there are three, all nominated by the Prince. The real estate sector is another important area because of the high prices for land throughout the principality. There are four casinos run by the Société des Bains de Mer, in which the state holds a majority interest.

Monaco's banking sector is linked to the French banking sector through the Franco-Monegasque Exchange Control Convention signed in 1945 and supplemented periodically, most recently in 2001. Through this convention, Monaco operates under the banking legislation and regulations issued by the French Banking and Financial Regulations Committee, including Article 57 of France's 1984 law regarding banking secrecy. Most of Monaco's banking sector is concentrated in portfolio management and private banking. The subsidiaries of foreign banks operating in Monaco can withhold customer information from the parent bank.

Although the French Banking Commission is the supervisor for Monegasque institutions, Monaco shoulders the responsibility for legislating and enforcing measures to counter money laundering and terrorism financing. The Finance Counselor (within the Government Council) is responsible for anti-money laundering implementation and policy.

Money laundering in Monaco is a criminal offense. It is criminalized by Act 1.162 of July 7, 1993, "On the Participation of Financial Institutions in the Fight against Money Laundering," and Section 218-3 of the Criminal Code, amended by Act 1.253 of July 12, 2002, "Relating to the Participation of Financial Undertakings in Countering Money Laundering and the Financing of Terrorism." Section 218-3 of the Criminal Code is being reviewed in order to expand the list of predicate offenses.

Banks, insurance companies, and stockbrokers are required to report suspicious transactions and to disclose the identities of those involved. Casino operators must alert the government of suspicious gambling payments possibly derived from drug-trafficking or organized crime. The law imposes a five-to-ten-year jail sentence for anyone convicted of using illicit funds to purchase property, which is itself subject to confiscation.

The 2002 amendments to Act 1.162 expanded the scope of money laundering requirements to include corporate service providers, portfolio managers, certain trustees (those subject to Law 214), and institutions within the offshore sector. New procedural requirements have also been put into place, such as internal compliance, client identification, and records maintenance. Meetings are held with compliance officers so that implementation issues and concerns may be aired and addressed.

Offshore companies are subject to the same due diligence and suspicious reporting obligations as banking institutions, and Monegasque authorities conduct on-site audits. The 2002 legislation strengthened the "know your client" obligations for casinos and obliges companies responsible for the management and administration of foreign entities not only to report suspicions to Monaco's financial intelligence unit (FIU), but also to set up internal anti-laundering and counterterrorist financing procedures, the enforcement of which is monitored by the FIU.

Banking laws do not allow anonymous accounts, but Monaco does permit the existence of alias accounts, which allow the account's owner to use a pseudonym in lieu of his or her real name. Cashiers do not know the client, but the bank knows the identity of the customer and retains client identification information.

Prior approval is required to engage in any economic activity in Monaco, regardless of its nature. The Monegasque authorities issue approvals of the type of business to be engaged in, and the location for a given length of time. Of particular importance is the fact that this government approval is personal and may not be assigned. Changes in any of the above terms require the issuance of a new approval.

Monaco established its FIU, the Service d'Information et de Controle sur les Circuits Financiers (SICCFIN), to collect information on suspected money launderers. SICCFIN receives suspicious transaction reports, analyzes them, and forwards them to the prosecutor when they relate to drug-trafficking, organized crime, terrorism, terrorist organizations, or the funding thereof. SICCFIN also is responsible for supervising the implementation of anti-money laundering legislation. SICCFIN has provided training to intermediaries, most recently to lawyers and notaries. Under Law 1.162, Article 4, SICCFIN may suspend a transaction for up to twelve hours and advise the judicial authorities to investigate.

In November 2001, Monaco and France reached an agreement on initiatives to counter money laundering in the principality. The French Finance Ministry stated that SICCFIN had doubled the number of its staff, and that there had been a "noteworthy" increase in the number of suspicious activity reports being filed. The 2002 amendments to the money laundering legislation increased SICCFIN's investigatory powers. In 2002, SICCFIN received 275 disclosures, 33 of which were passed to the public prosecutor for further investigation. In 2003, SICCFIN received 254 disclosures,

19 of which were referred to the public prosecutors. In 2004, SICCFIN had received an additional 341 disclosures, of which 18 were passed to the public prosecutor for further investigation. In 2004 SICCFIN received 55 requests for financial information from other FIUs.

Investigation and prosecution are handled by the two-officer Money Laundering Unit (Unite de Lutte au Blanchiment) within the police. The Organized Crime Group (Groupe de Repression du Banditisme) may also handle cases. Depending on the number and types of cases, there are seven police officers equipped to deal with money laundering. Monaco has had three convictions for money laundering and one acquittal.

Monaco's legislation allows for the confiscation of property of illegal origin as well as a percentage of illegally acquired and legitimate property that has been co-mingled. A court order is required for confiscation. In the case of money laundering, confiscation of property is restricted to the offenses listed in the Criminal Code. On the basis of letters rogatory, over 11.7 million euros ($13.8 million) have been seized. Monaco has extradited criminals, mainly to Russia.

In July and August 2002, Monaco passed Act 1.253 and promulgated two Sovereign Orders intended to implement United Nations Security Council Resolution 1373 by outlawing terrorism and its financing. Monaco is a party to the UN International Convention for the Suppression of the Financing of Terrorism; in April and August 2002, Monaco promulgated Sovereign Orders to import into domestic law the international obligations it accepted when it ratified that convention.

The Securities Regulatory Commissions of Monaco and France signed a memorandum of understanding on March 8, 2002, on the sharing of information between the two bodies. The agreement was a step in Monaco's efforts to conform to standards proscribed by the International Organization of Securities Commissions, whose mission is to establish international standards to promote the integrity of securities markets. The Government of Monaco sees the MOU as an important tool in combating financial crimes, particularly money laundering.

In 2004 SICCFIN signed information exchange agreements with counterparts in Malta, Poland, Andorra, Mauritius, Slovakia, Canada, and Peru. In previous years it had signed such agreements with Slovenia, Italy, Ireland, Lebanon, Switzerland, Liechtenstein, Panama, Luxembourg, France, Spain, Belgium, Portugal, and the United Kingdom. SICCFIN is a member of the Egmont Group.

Monaco was admitted to the Council of Europe on October 4, 2004. Well before that date, in 2002, SICCFIN approached the Council of Europe's MONEYVAL Committee and requested full participation in that Committee, including having an evaluation conducted on its anti-money laundering regime. In October 2002, the evaluation was performed; the evaluators acknowledged the extensive and thorough regime that has been developed.

Monaco is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime In May 2002, Monaco acceded to the Council of Europe Convention on the Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

The Government of Monaco should amend the Criminal Code to include an "all-crimes" approach, rather than the current list of predicate offenses. Monaco should also amend its legislation to implement full corporate criminal liability. Monaco should continue to enhance its anti-money laundering and confiscation regimes.

Morocco

Morocco is not a regional financial center, and the extent of the money laundering problem in the country is not known. Morocco remains an important producer and exporter of cannabis, with estimated revenues of $13 billion annually, according to a joint study released in May 2005 by the United Nations Office on Drugs and Crime (UNODC) and Morocco's Agency for the Promotion and

the Economic and Social Development of the Northern Prefectures and Provinces of the Kingdom. Some of these proceeds may be laundered in Morocco and abroad. There is no indication that international or domestic terrorist networks have engaged in widespread use of the narcotics trade to finance terrorist organizations and operations in Morocco.

Morocco has a significant informal economic sector, including remittances from abroad and cash-based transactions. There are unverified reports of trade-based money laundering, including bulk cash smuggling, under-and over-invoicing, and the purchase of smuggled goods. Banking officials have indicated that the country's system of unregulated money exchanges provides opportunities for potential launderers. Morocco has a free trade zone in Tangier, with customs exemptions for goods manufactured in the zone for export abroad. There have been no reports of trade-based money laundering schemes or terrorist financing activities using the Tangier free zone or the zone's offshore banks, which are regulated by an interagency commission chaired by the Ministry of Finance. A Free Trade Agreement with the United States will go into effect in 2006.

There were no reported arrests or prosecutions for money laundering or terrorist financing in Morocco in 2005. Morocco has a relatively effective system for disseminating U.S. Government (USG) and United Nations Security Council Resolution (UNSCR) terrorist freeze lists to the financial sector and law enforcement. Morocco has provided detailed and timely reports requested by the UNSCR 1267 Sanctions Committee. A handful of small value accounts have been administratively frozen based on the U.S. list of Specially Designated Global Terrorists, designated pursuant to E.O. Executive Order 13224.

The Moroccan financial sector is modeled after the French system and consists of 16 banks, five government-owned specialized financial institutions, approximately 30 credit agencies, and 12 leasing companies. The monetary authorities in Morocco are the Ministry of Finance and the Central Bank, Bank Al Maghrib (CBM), which monitors and regulates the banking system. A separate Foreign Exchange Office regulates international transactions. Morocco has used administrative instruments and procedures to freeze suspect accounts.

The CBM issued Memorandum No. 36 in December 2003, in advance of the passage of still pending anti-money laundering legislation, instructing banks and other financial institutions to conduct their own internal analysis/investigations. It also mandates "know your customer" procedures, reporting of suspicious transactions and the retention of suspicious activity reports. Morocco also has in effect: legislation prohibiting anonymous bank accounts; foreign currency controls that require declarations to be filed when transporting currency across the border (although these are not strictly enforced); and internal bank controls designed to counter money laundering and other illegal/suspicious activities.

In June 2003, Morocco adopted a comprehensive counterterrorism bill that provided the legal basis for the lifting of bank secrecy to obtain information on suspected terrorists, freeze suspect accounts and prosecute terrorist finance-related crimes. The law also provides for the seizing and confiscation of terrorist assets and for international cooperation with regard to foreign requests for freezing assets of a suspected terrorist entity. This law was designed to bring Morocco into compliance with UNSCR 1373 requirements for the criminalization of the financing of terrorism.

As of December 2005, Morocco has enacted two banking/financial sector reform bills that will further strengthen Morocco's anti-money laundering system. A specific anti-money laundering (AML) bill is in the process of being presented to Parliament for passage. The proposed law reportedly includes, among other provisions, a suspicious transaction reporting scheme and the creation of a Financial Intelligence Unit (FIU). All three bills are based on the Financial Action Task Force (FATF) Forty Recommendations and Egmont Group guidelines and will help bring Morocco's financial sector in line with international standards.

Together, the three bills will enhance the supervisory and enforcement authority of the Central Bank and outline investigative and prosecutorial procedures. The Central Bank has already mandated "know your customer" requirements and the reporting of suspicious transactions by financial institutions. All money transfer activities that take place outside the realm of the official Moroccan banking system-as set by the CBM guidelines-are deemed illegal. The bills also expand the CBM's regulatory authority over non-banking financial transactions. Other significant provisions include: the lifting of bank secrecy during investigations, as well as legal liability protection of bankers and investigators for cooperation during investigations.

Morocco is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of Financing of Terrorism, and the UN Convention against Transnational Organized Crime; in fact, Morocco has ratified or acceded to 11 of the 12 UN and international conventions and treaties related to counterterrorism. Morocco 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.

Morocco should strengthen its AML capacity by moving expeditiously to pass the anti-money laundering bill. Upon passage of the AML legislation, and as part of a comprehensive anti-money laundering program, Morocco should establish a centralized Financial Intelligence Unit (FIU) that will receive and analyze suspicious transaction reports and disseminate them to appropriate law enforcement agencies for investigation.

Mozambique

Mozambique is not a regional financial center. Although there have not been prosecutions, money laundering is believed to be fairly common and is linked principally to customs fraud and narcotics trafficking. Authorities believe the proceeds from these illicit activities have helped finance the recent spate of large-and small-scale commercial real estate developments, particularly in the capital. Multi-million dollar construction projects are allegedly financed with cash, and branch businesses owned by these same developers reputedly conceal illicit proceeds gained by selling imported goods on which no duties have been paid, and by trafficking illegal drugs from South Asia and South America. Most narcotics are destined for South African and European markets; Mozambique is not a significant consumption destination and is rarely a transshipment point to the United States. Local organized crime controls narcotics trafficking operations in the country, with significant involvement by Pakistani and Indian immigrants. While money laundering in the banking sector is considered to be a serious problem, foreign currency exchange houses, cash couriers, and the hawala remittance system also play a significant role in financial crimes and money laundering. Despite these problems, or perhaps because of them, there are no documented links between Mozambique-based drug traffickers, money launderers and the financing of terrorists.

The financial sector in general is not believed to be experiencing any increase in crimes such as money laundering, but a formal assessment of criminal trends is difficult due to a dearth of reporting, investigations or prosecutions. There were no money laundering arrests in 2005, nor any prosecutions. Black markets for smuggled goods and financial services are widespread, dwarfing the formal retail and banking sectors in most parts of the country. The presence of these markets makes it difficult to determine when and where laundering of illicit proceeds from customs fraud and narcotics trafficking—as well as bribes and kickbacks, skimmed money from contracts, undeclared income, and theft—are occurring. Much of the laundering is believed to be happening behind the scenes at foreign currency exchange houses. The government has banned the opening of any new exchange houses, and government officials have publicly discussed the need for more intense scrutiny on those currently in operation. While no evidence has been uncovered through formal investigations, it is widely believed

that corrupt officials are directly involved with customs fraud, narcotics trafficking and the laundering of profits.

Money laundering has long been a criminal offense in Mozambique, but the crime had not been narrowly defined until enactment of the 2002 Anti-Money Laundering Act. The Act contains specific provisions related to narcotics trafficking, in addition to a wider range of offenses considered predicates for money laundering. While the initial set of implementing regulations for the anti-money laundering law were only issued in September 2004, by year's end, all regulations and amendments had been passed, including provisions for the creation of the country's first financial intelligence unit (FIU). The World Bank and International Monetary Fund have worked with the government to help establish the framework for the FIU, which is to begin operating formally in 2006. The FIU will be housed in the prime minister's office, and participating members of the FIU will represent the Central Bank, Ministry of Justice, Ministry of the Interior, Ministry of Finance, and the Office of the Attorney General. The new FIU will reportedly have regulatory and investigative duties, and can, through the Attorney General's office, refer cases for criminal prosecution.

According to the 2002 law, banks and exchange houses must immediately record and report to the Attorney General's office any cash transaction valued at 441 times the monthly minimum wage, or about $23,000 at current exchange rates. In addition, exchange houses are required to turn in records of all transactions on a daily basis. All credit card transaction attempts over $5,000 must also be reported and can only be processed with approval from the Central Bank. Banks and exchange houses are required to keep transaction records for 15 years (Article 15 of 2002 law). Financial institutions are required to report any suspicious transactions immediately to the Attorney General's office (Article 16). The Attorney General, in turn, is required to determine within 48 hours whether to permit the transaction (Article 19).

The 2002 law includes due diligence provisions that make both respective bankers and banks responsible if financial institutions launder money (Article 27). Money laundering controls apply to all formal non-banking financial institutions, including exchange houses, brokerages houses, casinos and insurance companies. Individuals who report suspicious transactions in good faith receive protection under the 2002 law (Article 21). Bank secrecy laws exist in Mozambique but do not apply in the case of suspected money laundering (Article 17).

The 1996 Money Exchange Act requires any individual carrying more than $5,000 across the border to file a report with Customs. Taking more than 500,000 meticais (about $20) out of the country is prohibited. Cash couriers must comply with these cross-border currency requirements, but it is believed that there is an increasing trend of couriers transporting large amounts of cash outside the country via airline flights.

Mozambique has not explicitly criminalized the financing of terrorism. Its 1991 Crimes against the Security of State Act criminalizes terrorism, but financing is not addressed. The 2002 anti-money laundering law does list terrorism finance as a serious crime subject to the scope of the law, but elaborates no further (Article 4). The same law codifies Mozambique's long-held authority to identify, freeze, seize and/or forfeit the assets of those charged with financial crimes, including terrorist financing (Articles 5 and 6). Financial institutions do not have direct access to the names of persons or entities included on the UN 1267 Sanctions Committee's consolidated list or the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224; these lists are distributed only to the Central Bank, the Attorney General, the Ministry of Finance, and the Ministry of Foreign Affairs. Authorities in these institutions have not positively identified any of the persons or entities on these lists as operating in Mozambique, and therefore no assets have been identified, frozen, or seized.

Mozambique is not considered an offshore financial center. Many local businessmen use offshore banking in nearby countries, such as Mauritius. There are no free trade zones in Mozambique.

Authorities acknowledge that alternative remittance systems are common in Mozambique, many of which operate in exchange houses that, on paper, are heavily regulated but in fact can easily avoid reporting requirements. The hawala system of remittance, for example, is believed to be widely used within the South Asian community. There are no serious legislative, judicial, or regulatory measures being considered to address this problem. Charitable institutions must receive approval by the Ministry of Justice (MOJ) before receiving a charter, and are subject to investigation by the MOJ thereafter. However, there have been no public reports of the MOJ seriously investigating any charities.

Mozambique is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Mozambique is a signatory to the UN Convention against Transnational Organized Crime. It is also a founding member of a FATF-style regional body, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). Mozambique has entered a series of formal agreements with neighboring countries to share financial information required by law enforcement bodies. Cooperation with the United States on these matters has taken place on an informal basis.

The 2002 Anti-Money Laundering Act contains provisions authorizing the seizure and forfeiture of assets, including those of legitimate businesses used to launder money. In such a case, the Central Bank would be responsible for the initial tracing of assets and the Attorney General would be responsible for freezing and confiscating assets. The Attorney General also has authority to auction confiscated assets and to distribute proceeds to a range of parties. Despite this legal framework, the institutions authorized to implement the law do not have an established system for identifying and freezing narcotics-related assets, and no assets have been seized to date under the 2002 Anti-Money Laundering Act.

The law allows for both civil and criminal forfeiture. An example of civil forfeiture would be the seizure of cash in excess of the $5,000 limit from an individual who tried, secretly, to carry this amount across the border. The seized funds would be sent by Customs to the Central Bank. Appeals then could be made directly to the Bank. Private financial institutions are more closely regulated by criminal forfeiture acts, but are also subject to civil suits. Financial institutions also have the right to file a civil suit against the government for loss of business in cases of unreasonable suspension, a provision that will likely discourage enforcement of the law.

The Government of Mozambique should clarify that the financing of terrorism is specifically criminalized, either by its 1991 or 2002 legislation, or else it should do so in a new instrument. It should ensure that the financial intelligence unit to be established in 2006 operates in accordance with international standards. It should deposit the instrument of ratification for the UN Convention against Transnational Organized Crime. It must also address some additional and serious obstacles to enforcement of its laws, such as resource constraints affecting the Attorney General's office and the Criminal Investigative Police, significant corruption, and intimidating tactics on the part of organized crime. It should improve interagency coordination, and provide intensive training in forensic audit, analytical, and investigation practices to members of the financial intelligence unit. These practical measures will be necessary to enforce any laws.

The Netherlands

The Netherlands is a major financial center and as such is an attractive target for the laundering of funds generated from a variety of illicit activities. Activities involving money laundering are often related to the sale of heroin, cocaine, cannabis, or synthetic and designer drugs (such as ecstasy). As a major financial center, several Dutch financial institutions engage in international business transactions involving large amounts of United States currency. There are, however, no indications that significant amounts of U.S. dollar transactions conducted by financial institutions in the Netherlands stem from illicit activity. Activities involving financial fraud are believed to generate a

considerable portion of domestic money laundering. Much of the money laundered in the Netherlands is likely owned by major drug cartels and other international criminal organizations. There are no indications of syndicate-type structures in organized crime or money laundering, and there is virtually no black market for smuggled goods in the Netherlands. Although under the Schengen Accord there are no formal controls on the borders with Germany and Belgium, the Dutch authorities run special operations in the border areas to keep smuggling to a minimum. The Netherlands is not an offshore financial center nor are there any free trade zones in the Netherlands.

In 1994, the Government of the Netherlands (GON) criminalized money laundering related to all crimes. In December 2001, legislation was enacted making facilitating, encouraging, or engaging in money laundering a separate criminal offense, easing the public prosecutor's burden of proof regarding the criminal origins of proceeds. Under the law, the public prosecutor needs only to prove that the proceeds "apparently" originated from a crime; self-laundering is also covered. In two cases in 2004 and 2005, the Dutch Supreme Court confirmed the wide application of the money laundering offenses by stating that the public prosecutor does not need to prove the exact origin of laundered proceeds and that the general criminal origin as well as the knowledge of the perpetrator may be deducted from objective circumstances.

The Netherlands has an "all offenses" regime for predicate offenses of money laundering. The penalty for "deliberate acts" of money laundering is a maximum of four years' imprisonment and a maximum fine of 45,000 euros (approximately $53,800), while "liable acts" of money laundering (of people who do not know first-hand of the criminal nature of the origin of the money, but should have reason to suspect it) are subject to a maximum imprisonment of one year and a fine no greater than 45,000 euros (approximately $53,800). Habitual money laundering may be punished with a maximum imprisonment of six years and a maximum fine of 45,000 euros (approximately $53,800), and those convicted may also have their professional licenses revoked. In addition to criminal prosecution for money laundering offenses, money laundering suspects can also be charged with participation in a criminal organization (Article 140 of the Penal Code), violations of the financial regulatory acts, violations of the Sanctions Act, or noncompliance with the obligation to declare unusual transactions according to the Economic Offenses Act.

The Netherlands has comprehensive anti-money laundering legislation. The Services Identification Act and the Disclosure Act set forth identification and reporting requirements. All financial institutions in the Netherlands, including banks, bureaux de change, casinos, life insurance companies, securities firms, stock brokers, and credit card companies, are required to report cash transactions over 15,000 euros (approximately $18,800), as well as any less substantial transaction that appears unusual, a broader standard than "suspicious" transactions, to the Office for Disclosure of Unusual Transactions (MOT), the Netherlands' financial intelligence unit (FIU). In December 2001, the reporting requirements were expanded to include trust companies, financing companies, and commercial dealers of high-value goods. In June 2003, notaries, lawyers, real estate agents/intermediaries, accountants, business economic consultants, independent legal advisers, trust companies and other providers of trust related services, and tax advisors were added. Reporting entities that fail to file reports with the MOT may be fined 11,250 euros (approximately $13,500), or be imprisoned up to two years. Under the Services Identification Act, all those that are subject to reporting obligations must identify their clients, including the identity of ultimate beneficial owners, either at the time of the transaction or prior to the transaction, before providing financial services.

In 2004, an evaluation of the anti-money laundering reporting system, commissioned by the Minister of Justice, was published. In response to the report the GON enacted a number of measures to enhance the effectiveness of the existing system. In November 2005, the Board of Procurators General issued a National Directive on money laundering crime that included an obligation to conduct a financial investigation in every serious crime case, guidelines for determining when to prosecute for money laundering and technical explanations of money laundering offenses, case law, and the use of financial

intelligence. A new set of indicators, which determine when an unusual transaction must be filed, also entered into force in November 2005. These new indicators represent a partial shift from a rule-based to a risk-based system and are aimed at reducing the administrative costs of reporting unusual transactions for the reporting institutions without limiting the preventive nature of the reporting system. The Dutch parliament has also approved amendments that expand supervision authority and introduces punitive damages, to the Services Identification Act and Disclosure Act, scheduled to take effect in 2006.

Financial institutions are also required by law to maintain records necessary to reconstruct financial transactions for at least seven years. The requirements also have been applicable to the Central Bank of the Netherlands (to the extent that it provides covered services) since 1998. There are no secrecy laws or fiscal regulations that prohibit Dutch banks from disclosing client and owner information to bank supervisors, law enforcement officials, or tax authorities. Financial institutions and all other institutions under the reporting and identification acts, and their employees, are specifically protected by law from criminal or civil liability related to cooperation with law enforcement or bank supervisory authorities. Furthermore, current legislation requires Customs authorities to report unusual transactions to the MOT; however, the Netherlands does not currently have a currency declaration requirement for incoming travelers. Under the 2004 Dutch European Union (EU) Presidency, the EU reached agreement on a cash courier regulation, which implements the Financial Action Task Force (FATF) Special Recommendation Nine on terrorist financing. The implementation is expected to occur in the Netherlands in 2007.

The Money Transfer and Exchange Offices Act, which was passed in June 2001, requires money transfer offices, as well as exchange offices, to obtain a permit to operate, and subjects them to supervision by the Central Bank. Every money transfer client has to be identified.

The Central Bank of the Netherlands, which merged with the Pension and Insurance Chamber in April 2004, and the Financial Markets Authority, as the supervisors of the Dutch financial sector, regularly exchange information nationally and internationally. Sharing of information by Dutch supervisors does not require formal agreements or memoranda of understanding (MOUs).

The MOT, which was established in 1994, reviews and analyzes the unusual transactions and cash transactions filed by banks and financial institutions. The MOT receives over 98 percent of unusual transaction reports electronically through its secure website. It forwards suspicious transaction reports with preliminary investigative information to the Police Investigation Service and to the Office for Operational Support of the National Public Prosecutor for MOT cases (BLOM). In 2006, the MOT and the BLOM will merge and both entities will be integrated within the National Police (KLPD). This new FIU structure (MOT/BLOM) will provide an administrative function that will receive, analyze, and disseminate unusual currency transaction reports. It will also provide a police function that will serve as a point of contact for law enforcement. Foreign FIUs will be able to turn to this new organization with requests for financial and law enforcement information. Over the last five years, the MOT and the BLOM have cooperated closely in responding to international requests for information, so this merger will not change the nature of the Dutch reporting system.

In 2003, the MOT received 177,157 unusual transaction reports, totaling over 1.5 billion euros (approximately $1.7 billion) and forwarded 37,748 to the BLOM and other police services as suspicious transactions for further investigation. In 2004, the MOT received 174,835 reports, totaling over 3 billion euros (approximately $3.6 billion), and forwarded 41,003 to the BLOM and other police services. The average amount reported was 79,000 euros (approximately $94,500) in 2004, an increase from the 41,000 euros (approximately $49,000) average reported in 2003. Reportedly, this significant increase was due to a few large transactions.

In order to facilitate the forwarding of suspicious transactions, the MOT and BLOM created an electronic network called Intranet Suspicious Transactions (IST). Also, a secure website for the actual

reporting of unusual transactions by financial institutions was developed, thus completing the electronic infrastructure. Furthermore, fully automatic matches of data with the police databases are included with the unusual transaction reports forwarded to the BLOM. Since the money laundering detection system also covers areas outside the financial sector, the system is used for detecting and tracing terrorist financing activity.

On January 1, 2003, the MOT and BLOM formed a special unit (the MBA-unit) to work together to analyze data generated from the IST. Once the data is analyzed by the MBA-unit, it forwards reports to the police. In 2004, the MBA-unit sent 200 reports to the police for further investigations.

In 2004, BLOM opened 712 investigations, which involved 15,203 transactions. BLOM conducted 80 Hit-And-Run Money Laundering (HARM) team actions, including eight involving exchange transactions, 60 involving the physical presence of large amounts of cross border cash money, and six cases involving withdrawals, deposits, wire transfers or offers of bank checks. Of the 80 HARM actions, 58 were the result of BLOM's own investigations. With regard to the cross-border movement of cash, the royal constabulary apprehended 60 outgoing cash couriers at Amsterdam Schiphol Airport and confiscated nearly 10 million euros (approximately $12 million) in cash. In 2004, the office of the public prosecutor issued summons for money laundering offenses in 244 cases, resulting in 138 convictions with 87 cases still pending.

The Public Prosecutor HARM team was established in 2001. Both the MOT and BLOM are internationally recognized institutions that play a major role in the Dutch anti-money laundering regime. BLOM provides the anti-money laundering division of Europol with suspicious transaction reports, and Europol applies the same analysis tools as BLOM.

The Netherlands has enacted legislation governing asset forfeitures. The 1992 Asset Seizure and Confiscation Act enable the authorities to confiscate assets that are illicitly obtained or otherwise connected to criminal acts. The legislation was amended in 2003 to improve and strengthen the options for identifying, freezing, and seizing criminal assets. The police and several special investigation services are responsible for enforcement in this area. These entities have adequate powers and resources to trace and seize assets. Asset seizure has been integrated into all law enforcement investigations into serious crime.

The system is principally value-based, though property-based orders can also be made. Any tangible assets, such as real estate or other conveyances that were purchased directly with the proceeds of a crime tracked to illegal activities, may be seized. Property subject to confiscation as an instrumentality may consist of both moveable property and claims. Assets can be seized as a value-based confiscation. Asset seizure and confiscation legislation also provides for the seizure of additional assets controlled by drug trafficker. Legislation defines property for the purpose of confiscation as "any object and any property right." Proceeds from narcotics asset seizures and forfeitures are deposited in the general fund of the Ministry of Finance. Dutch authorities have not identified any significant legal loopholes that allow drug traffickers to shield assets.

In order to promote the confiscation of criminal assets, special court procedures have been created, enabling law enforcement to continue financial investigations in order to prepare confiscation after the underlying crimes have been successfully adjudicated. All police services investigating in the field of organized crime rely on the real time assistance of financial detectives and accountants, as well as on the assistance of the Proceeds of Crime Office (BOOM), a special bureau advising the Office of the Public Prosecutor in international and complex seizure and confiscation cases. To further international cooperation in this area, the Camden Asset Recovery Network (CARIN) was set up in The Hague in September 2004. BOOM played a leading role in the establishment of this informal international network of asset recovery specialists, whose aim is the exchange of information and expertise in the area of asset recovery.

Statistics provided by the Office of the Public Prosecutor show that the amount of assets seized in 2004 amounted to 11 million euros (approximately $13 million), compared to 10 million euros (approximately $11 million) in 2003. (These figures do not include tax-related confiscations. Dutch Tax Authorities can tax any income, whether legal or illegal.) The United States and the Netherlands have an agreement on asset sharing dating back to 1994. The Netherlands also has a treaty on asset sharing with the United Kingdom, as well as an agreement with Luxembourg.

In June 2004, the Minister of Justice sent an evaluation study to the Parliament on specific problems encountered with asset forfeiture in large, complex cases. In response to this report, the GON announced several measures to improve the effectiveness of asset seizure enforcement, including steps to increase expertise in the financial and economic field, assign extra public prosecutors to improve the coordination and handling of large, complex cases, and establish a specific asset forfeiture fund. The Office of the Public Prosecutor has designed a new centralized approach for large confiscation cases and a more flexible approach for handling smaller cases. Both will take effect in 2006. These measures should significantly increase BOOM's capacity to handle asset forfeiture cases.

Terrorist financing is a crime in the Netherlands. The "Sanction Provision for the Duty to Report on Terrorism" was passed in 1977 and amended in June 2002, to implement European Union (EU) Regulation 2580/2001 and UNSCR 1373. This ministerial decree provides authority to the Netherlands to identify, freeze, and seize terrorist finance assets. The decree also requires financial institutions to report to the MOT all transactions (actually carried out or intended) that involve persons, groups, and entities that have been linked, either domestically or internationally, with terrorism. Any terrorist crime will automatically qualify as a predicate offense under the Netherlands "all offenses" regime for predicate offenses of money laundering. Involvement in financial transactions with suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list or designated by the EU has been made a criminal offense. The Dutch Finance Ministry, in close coordination with the Foreign Affairs Ministry, distributes lists of designated entities to financial institutions and relevant government bodies (including local tax authorities). Freezing of assets is an administrative procedure. The Netherlands has frozen more terrorist-related assets than any other EU member state.

The Act on Terrorist Offenses took effect on August 10, 2004. The Act introduces Article 140A of the Criminal Code, which criminalizes participation in an organization when the intent is to commit acts of terrorism, and defines participation as membership or providing provision of monetary or other material support. Article 140A carries a maximum penalty of fifteen years' imprisonment for participation in and life imprisonment for leadership of a terrorist organization. The GON is considering new legislation that would expand, among other things, investigative powers and the use of coercive measures in antiterrorist inquiries.

Unusual transaction reports by the financial sector act as the first step against the abuse of religious organizations, foundations and charitable institutions for terrorist financing. No individual or legal entity (churches or religious institutions included) is exempt from the obligation of identification when using the financial system. Financial institutions must also inquire about the identity of the ultimate beneficial owners. Thus, a paper trail is maintained throughout the payment chain. A second step is provided by Dutch civil law, which requires registration of all active foundations in the registers of the Chambers of Commerce. Each foundation's formal statutes (creation of the foundation must be certified by a notary of law) must be submitted to the Chambers. Charitable institutions also register with, and report to, the tax authorities in order to qualify for favorable tax treatment. Approximately 15,000 organizations (and their managements) are registered in this way. The organizations have to file their statutes, showing their purpose and mode of operations, and submit annual reports. Samples are taken for auditing. Finally, many Dutch charities are registered with or monitored by private "watchdog" organizations or self-regulatory bodies, the most important of which is the Central Bureau for Fund Raising. In April 2005, the GON approved a plan to replace the current initial screening of

founders of private and public-limited partnerships and foundations with an ongoing screening system. The new system will be introduced in the course of 2007 to improve Dutch efforts to fight fraud, money laundering, and terrorist financing.

Data about informal hawala banking as a potential money laundering/terrorist financing source is still scarce. Initial research by the Dutch police and Internal Revenue Service and Economic Control Service (FIOD/ECD) indicates that the number of *hawala*-type banks in the Netherlands is rising. The Dutch Government plans to implement improved procedures for tracing and prosecuting informal (unlicensed) or hawala-type banking, with the Dutch Central Bank, FIOD/ECD, the Financial Expertise Center, and the Police playing a coordinating and central role. The Dutch Finance Ministry plans to participate in a World Bank-initiated international survey on money flows by immigrants to their native countries, with a focus on relations between the Netherlands and Suriname. The Dutch Central Bank will also initiate a study into the number of informal banking institutions in the Netherlands. In Amsterdam, a special police unit has been investigating underground bankers. These investigations have resulted in the disruption of three major underground banking schemes.

Reportedly, the Netherlands is in full compliance with all FATF Recommendations, with respect to both legislation and enforcement. The Netherlands also complies with the Council Directive 2001/97/EC on prevention of the use of the financial system for money laundering (2nd EU Money Laundering Directive), and in some areas is ahead of the EU legislation (such as full money laundering controls on money remitters, including licensing and identification of customers). In December 2004, the Dutch EU Presidency reached political agreement within the EU on the Third Money Laundering Directive, which was subsequently adopted by the EU in 2005 with full implementation by EU Member States by 2007. The Dutch have already implemented some obligations resulting from this directive, such as effective supervision of currency exchange offices and trust companies.

In December 2003, the International Monetary Fund (IMF) conducted an assessment of the Dutch anti-money laundering and counterterrorist financing system. The Report on the Observance of Standards and Codes (ROSC), released in September 2004, indicates that the Netherlands has a sound anti-money laundering and counterterrorist financing framework. In 2005, the Second Round of the Council of Europe's Group of States Against Corruption (GRECO) evaluation of the Netherlands resulted in positive conclusions regarding Dutch seizure and confiscation legislation.

The MOT supervised the PHARE Project for the European Union (March 2002-December 2003). The PHARE Project was the European Commission's Anti-Money Laundering Project for Economic Reconstruction Assistance to Estonia, Latvia, Lithuania, Poland, the Czech Republic, Slovakia, Hungary, Slovenia, Romania, Bulgaria, Cyprus, and Malta. The purpose of the project was to provide support to Central and Eastern European countries in the development and/or improvement of anti-money laundering regulations. For this purpose, the MOT established a project team and a consortium of international experts. Although the PHARE project concluded in December 2003, the MOT has moved forward with the development of the FIU.NET Project, (an electronic exchange of current information between European FIUs by means of a secure intranet).

The United States enjoys good cooperation with the Netherlands in fighting international crime, including money laundering. In September 2004, the United States and the Netherlands signed two agreements in the area of mutual legal assistance and extradition, stemming from the agreements that were concluded in 2003 between the EU and the United States. One of the amendments to the existing bilateral agreement is the exchange of information on bank accounts. The MOT has established close links with the U.S Treasury's FinCEN and is also involved in efforts to expand international cooperation between disclosure offices.

The Netherlands is a member of the Financial Action Task Force. The GON participates in the Caribbean Financial Action Task Force as a Cooperating and Supporting Nation. The MOT is a

member of the Egmont Group. The MOT has concluded formal information sharing memoranda of understanding (MOUs) with Belgium, Aruba and the Netherlands Antilles. The Netherlands is a party to the 1988 UN Drug Convention and the 1990 Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. The Dutch participate in the Basel Committee, and have endorsed the Committee's "Core Principles for Effective Banking Supervision." The Netherlands is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

The Netherlands should continue the strong enforcement of its anti-money laundering program and its leadership in the international arena.

Netherlands Antilles

The Netherlands Antilles, which has autonomous control over its internal affairs, is a part of the Kingdom of the Netherlands. The Netherlands Antilles is comprised of Curacao, Bonaire, the Dutch part of Sint Maarten/St. Martin, Saba, and Sint Eustatius. The Government of the Netherlands Antilles (GONA) is located in Willemstad, the capital of Curacao, which is also the financial center of the five islands. Narcotics trafficking and a lack of border control between Sint Maarten and St. Martin create opportunities for money launderers in the Netherlands Antilles. Of note is the surge over the past few years of remittance transfers from the Netherlands.

The Netherlands Antilles has a significant offshore financial sector with 23 international banks and approximately 207 trust companies providing financial and administrative services to their international clientele, including approximately 15,571 offshore companies, mutual funds, and international finance companies. The islands also have eight local credit institutions, five savings and credit funds, thirteen foreign credit institutions, seven local commercial banks, four foreign commercial banks, two savings banks, seventeen credit unions, 18 consolidated international banks and 19 non-consolidated international banks. There are 31 institutional investors that may carry out insurance business, 19 captive insurance companies, six professional reinsurance companies, 27 pension funds and one other fund.

On February 1st, 2001, the GONA approved the proposed amendments to the free zone law allowing e-commerce activities into these areas (National Ordinance Economic Zone no.18, 2001). As of this date, it is no longer necessary for goods to be physically present within the zone as was required under the former free zone law. Furthermore, the name "Free Zone" was changed to "Economic Zone" (E-Zone). Seven areas within the Netherlands Antilles qualify as e-zones of which five are designated for e-commerce. The remaining two e-zones, which are located at the airport and the harbor, are designated for goods. These zones are minimally regulated; however, administrators and businesses in the zones have indicated an interest in receiving guidance on detecting unusual transactions.

The Central Bank supervises all banking and credit institutions, including banks for local and international business, specialized credit institutions, savings banks, credit unions, savings and credit funds, and pension funds. However, authorities in other countries supervise some mutual funds. The laws and regulations on bank supervision state that international banks must have a physical presence on the island and hold records there. All life insurance and general insurance companies need to apply for a license from the Central Bank. In early 2003, legislation was introduced to transfer supervision of the trust sector to the Central Bank. International corporations may be registered using bearer shares. The practice of the financial sector in the Netherlands Antilles is for either the bank or the company service providers to maintain copies of bearer share certificates for international corporations, which include information on the beneficial owner(s). There is a proposal to require that the name of the ultimate beneficial owner of the bearer share be recorded in a registry and made accessible to law enforcement officials upon a treaty-based request for the information.

Money laundering is a crime. Legislation in 1993 and subsequent interpretations regarding the "underlying crime" establish that prosecutors do not need to prove that a suspected money launderer also committed an underlying crime in order to obtain a money laundering conviction. Thus, it is sufficient to establish that the money launderer knew, or should have known, of the money's illegal origin.

In recent years, the GONA has taken steps to strengthen its anti-money laundering regime by expanding suspicious activity reporting requirements to gem and real estate dealers, introducing indicators for the reporting of unusual transactions for the gaming industry, issuing guidelines to the banking sector on detecting and deterring money laundering, and modifying existing money laundering legislation that penalizes currency and securities transactions, by including the use of valuable goods. The 2002 National Ordinance on the Supervision of Fiduciary Business institutes a Supervisory Board that oversees the international financial sector. At the same time, GONA subjected the members of this sector to know-your-customer rules. A GONA interagency anti-money laundering working group cooperates with its Kingdom counterparts.

Suspicious transactions are by law reported to the financial intelligence unit, the Netherlands Antilles Reporting Center, MOT NA. The GONA is amending the national ordinance regarding the MOT NA which should go into effect in 2006. The objective is to add new non-financial reporters, such as lawyers, accountants, notaries, jewelers, and real estate agents. The GONA hopes to have in place all relevant laws and agreements prior to the IMF audit in 2007. On June 1, 2003, the Central Bank issued new consolidated reporting guidelines, replacing those of 1996. These guidelines are more closely focused on banks, insurance companies, pension funds, money transfer services, and financial administrators and now specifically include counterterrorism detectors. The Central Bank also established a Financial Integrity Unit to monitor corporate governance and market behavior. Entities under supervision must submit an annual statement of compliance.

Onshore banks are increasingly using their discretionary authority to protect themselves against money laundering. The largest commercial bank lowered its limits on money grams to $2,000. Banks are reluctant to do business with the Internet gaming providers, provoking complaints from that sector. In 2003 Curacao was reported to have six sports booking sites and 100 Internet casinos. The Meldpunt Ongebruikelijke Transacties (MOT NA), the Netherlands Antilles's financial intelligence unit (FIU) has issued a manual for casinos on how to file reports and has started to install software in casinos that will allow reports to be submitted electronically.

The current staff of eight at the MOT NA continues to work to enhance the effectiveness and efficiency of its reporting system. Significant progress has been made in automating suspicious activity reporting; in 2003 reporting institutions sent 99.2 percent of their reports to the MOT NA electronically. Most of the matches with external databases are done electronically. The MOT NA transmits information electronically to the police. On October 18, 2002, the GONA published new indicators for the reporting of unusual transactions with regard to terrorism financing. The new indicators require that unusual transactions reported to the police or judicial authorities in connection with money laundering or the financing of terrorism must also be reported to the MOT NA. This requirement also extends to unusual transactions relating to credit cards, money transfers, and game of chance transactions.

In May 2002 cross-border currency reporting legislation came into force. The law specifies reporting procedures for an individual bringing in or taking out more than NAF 20,000 (approximately $11,000) in cash or bearer instruments, and also applies to courier services. Declaration of currency exceeding the limit must include origin and destination. There is a fine of up to NAF 500,000 (approximately $281,000) or one year in prison.

In 2000, the National Ordinance on Freezing, Seizing, and Forfeiture of Assets Derived from Crime went into effect. The law allows the prosecutor to seize the proceeds of any crime once the crime is

proven in court. In January 2002, the GONA enacted legislation allowing a judge or prosecutor to freeze assets related to the Taliban *cum suis* and Usama Bin Ladin *cum suis* (*cum suis* means that all companies and persons connected with the Taliban or Usama Bin Ladin are included). The legislation contains a list of individuals and organizations suspected of terrorism. The Central Bank instructed financial institutions to query their databases for information on the suspects and to immediately freeze any assets that were found. In October 2002, the Central Bank instructed the financial institutions under its supervision to continue these efforts and to consult the UN website for updates to the list.

The Netherlands Antilles law allows the exchange of information between the MOT NA and foreign FIUs by means of memoranda of understanding and by treaty. The MOT NA's policy is to answer requests within 48 hours after receipt. A tax information exchange agreement (TIEA) was signed between the Netherlands Antilles and the United States. As of the end of 2005 implementing legislation in the parliament was pending which would allow this agreement to go into effect.

The Mutual Legal Assistance Treaty between the Netherlands and the United States also applies to the Netherlands Antilles. In September 2003, the U.S. Attorney in St. Thomas indicted five defendants, including one from Sint Maarten, for charges including laundering funds totaling $68 million. Cooperation with Sint Maarten under the MLAT was an important element in the investigation.

The MOT NA is an active member of the Egmont Group. The Netherlands Antilles is a member of the Caribbean Financial Action Task Force (CFATF), and as part of the Kingdom of the Netherlands, the Netherlands Antilles participates in the FATF. In 1999, the Netherlands extended application of the 1988 UN Drug Convention to the Netherlands Antilles. The Kingdom of the Netherlands became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. In accordance with Netherlands Antilles law, which stipulates that all the legislation must be in place prior to ratification, the GONA is preparing legislation that will enable the Netherlands Antilles to ratify the Convention.

The Government of the Netherlands Antilles has shown a commitment to combating money laundering. An increase to the MOT NA staff is particularly notable. The Netherlands Antilles should continue its focus on increasing regulation and supervision of the offshore sector and free trade zones and pursuing money laundering investigations and prosecutions. The Netherlands Antilles should criminalize the financing of terrorism, and should enact the necessary legislation to implement the UN International Convention for the Suppression of the Financing of Terrorism.

Nicaragua

Nicaragua is not a regional financial center; however this may soon change. The country is not a major drug producing country, but continues to be a significant transshipment point for South American cocaine and heroin destined for the United States, and, on a smaller scale, for Europe. Reportedly, there is evidence that the problem is growing and is increasingly linked to arms trafficking. This situation makes Nicaragua's financial system an attractive target for narcotics-related money laundering. Nicaraguan officials have expressed concern that, as neighbors have tightened their money laundering laws, established financial intelligence units (FIUs) and taken other actions, more illicit money has moved into the vulnerable Nicaraguan financial system. However, this concern has not resulted in the strengthening of Nicaragua's legal and institutional frameworks to effectively combat money laundering and the financing of terrorism.

Nicaragua's geographical position, with access to both the Atlantic and the Pacific Oceans, makes it an area heavily used by transnational organized crime groups. Organized crime groups also benefit from Nicaragua's weak legal system and its ineffective fight against financial crimes, money laundering, and terrorism.

While Nicaragua has pledged to fight the financing of terrorism, money laundering and other financial crimes, limited resources, corruption (especially in the judiciary), and the lack of political will in some sectors continue to complicate efforts to counteract these criminal activities. Nicaragua has recently made improvements to its oversight and regulatory control of its financial system. However, money laundering unrelated to drug-trafficking is legally undefined, the country does not have an operational FIU and all attempts to correct this deficiency have been stalled in the National Assembly for years.

In May 2005, GE Consumer Finance, one of the largest financial service firms in the world, announced that it was buying a 49.99 percent stake in Banco de America Central (BAC) which operates in several Central American countries, including Nicaragua, where it is one of the largest banks. Also, Banistmo, a Panamanian bank, recently began operations in Nicaragua. The ratification of the Central America/Dominican Republic Free Trade Agreement (CAFTA-DR) and regional integration suggest more involvement from international financial institutions.

Nicaragua does not permit direct offshore bank operations, but it does permit them to operate through nationally chartered entities. Bank and company bearer shares are permitted. Nicaragua has a well-developed indigenous gaming industry, which remains largely unregulated. There are no known offshore or Internet gaming sites in Nicaragua. On October 26, 2005, the National Assembly reformed Nicaragua's General Banks, Non-banking Financial Institutions, and Financial Groups Law, that if enforced would hold bank officials responsible for their institutions' money laundering. Article 164 of the law calls for sanctions for financial institutions and professionals of the financial sector, including internal auditors who do not develop anti money laundering programs or do not report to the appropriate authorities suspicious and unusual transactions that may be linked to money laundering, as required by the anti-money laundering law.

In 1999, Nicaragua passed Law 285 that requires banks to report cash deposits over $10,000 to the Superintendence of Banks and Other Financial Institutions (SIBOIF), which then forwards the reports for analysis to the Commission of Financial Analysis (CAF). Law 285 is not, however, being used as an effective tool against money laundering crimes committed by organized criminal organizations. The National Prosecutor's and the Attorney General's legal positions on the Law 285 differ significantly. The National Prosecutor, who also heads the CAF, is loyal to ex-President Arnoldo Aleman (convicted of laundering stolen government funds) and has sought to limit the application of the money laundering law to drug crimes. The Attorney General has led President Bolanos's charge against public corruption and has argued in and out of court that the money-laundering law as written applies to public corruption and other non-drug crimes. However, there were no money laundering prosecutions in Nicaragua in 2005, even when financial transactions have been linked to narcotics trafficking.

The CAF is not a financial intelligence unit. On paper, the CAF is composed of representatives from various elements of law enforcement and banking regulators and is responsible for detecting money laundering trends, coordinating with other agencies and reporting its findings to Nicaragua's National Anti-Drug Council. The CAF is ineffective due to a lack of budget, trained personnel, equipment, and strategic goals. The CAF is headed by the National Prosecutor who receives the reports from banks and decides whether to refer them to the Nicaraguan National Police (NNP) for further investigation. The Economics Crimes Unit within the NNP is in charge of investigating financial crimes, including money laundering and terrorist financing. The Nicaraguan Deputy Attorney General is critical of the inactivity and ineffectiveness of the CAF. He claimed that of the 354 suspicious activity reports received by the CAF from financial institutions in the first part of 2005, not a single criminal money laundering investigation, including those related to drug trafficking, has been initiated by the National Prosecutor.

Legislation that would improve Nicaragua's anti-money laundering regime has been stalled in the National Assembly for years. There are at least two pending bills. An amended drug and anti-money

laundering law would better define the crime of money laundering, and another special bill that creates a central FIU replacing the CAF and would require more stringent reporting of large and/or suspicious bank deposits. Reportedly, it is unlikely that these reform bills will make it out of the Assembly in the foreseeable future.

Draft legislation to criminalize terrorist financing is under consideration by the National Assembly, reportedly without any sign of imminent passage. It is possible that many elements of terrorist financing can be prosecuted under existing laws. Nicaragua has the authority—through five Bank Superintendence administrative decrees—to identify, freeze, and seize terrorist-related assets, but has not as yet identified any such cases. Reportedly, there are no hawala or other similar alternative remittance systems operating in Nicaragua, and the Nicaraguans have not detected any use of gold, precious metals, or charitable organizations to disguise such transactions. However, there are informal "cash and carry" networks for delivering remittances from abroad.

Corruption within the judiciary is a serious problem; judges often let detained drug suspects go free after a short detention, a practice that puts drug traffickers back on the streets, increasing the threat of money laundering. In a recent high-profile case judges released over $600,000 of funds from a suspected drug trafficker. From all indications, a number of judges may have been involved in the case and may have received payoffs. In another judicial scandal, two Mexican citizens were acquitted and had returned over $300,000 in undeclared currency that Nicaraguan customs seized when they entered the country. This case also involves a judge connected to the first drug-money scandal. Due to the rampant corruption in the Nicaraguan judiciary, the United States has cut off direct assistance to the Nicaraguan Supreme Court.

The SIBOIF is an independent and reputable financial institution regulator. Its financial experts have a good working relationship with the U.S. Government and have reached out to the NNP to work with them. On December 1, the SIBOIF, pursuant to the Nicaraguan Banking Law, closed down a business, Agave Azul, that was operating an illegal Ponzi scheme. Agave Azul opened for business in May 2005 and to date it has over 13,000 investors, according to police accounts. Under the scheme, investors (some of them National Assembly members that had invested up to $60,000) bought shares with the promise/expectation that they would earn a monthly rate of return of at least 15 percent on their investment. Investors recruited others to buy shares in the fake business that claimed to sell tequila. The investors' money was collected and sent via wire transfer to two banks in the United States and one in El Salvador.

Since May 2005 approximately $3,000,000 in U.S. currency has been deposited in Agave Azul accounts in at least two U.S. banks. SIBOIF notified the National Prosecutor about the scheme in early August 2005 and demanded action. The National Prosecutor failed to act. Though Agave Azul was closed by the SIBOIF, continuing inaction by the National Prosecutor is hampering the investigation. Efforts to freeze the business' bank accounts in the United States were unsuccessful due to the failure of the NNP to provide complete financial information and the unwillingness of the National Prosecutor to seek U.S. Government cooperation. Despite the failures in this investigation, the actions of the SIBOIF in cooperation with NNP show a dedication to investigate financial crimes and substantial level of cooperation between the Attorney General's Office and the NNP on financial crimes and money laundering issues.

U.S. Government efforts are focused on formalizing the existing cooperation by creating a vetted Anti-Corruption Unit that would be housed within the NNP and also include officials from the Attorney General's Office, with the aim of leading thorough investigations and strong prosecutions of corruption, money laundering and related crimes. Nicaragua ratified the Inter-American Convention on Mutual Legal Assistance in Criminal Matters in 2002, an agreement that facilitates the sharing of legal information between countries. Nicaragua is a party to the 1988 UN Drug Convention. The country has also ratified the UN Convention on the Suppression of the Financing of Terrorism and the

UN Convention against Transnational Organized Crime. Nicaragua is a member of the Organization of American States (OAS) and the Caribbean Financial Action Task Force (CFATF).

In October 2005, a delegation of the U.S. Department of the Treasury, including officials from the Financial Enforcement Network (FinCEN), Office of Technical Assistance (OTA), and the Internal Revenue Service (IRS), went to Nicaragua. They were accompanied by Delia Cárdenas, the Panamanian Superintendent of Banks and the then President of CFATF. Cárdenas went to Nicaragua to express CFATF's dissatisfaction with Nicaragua's refusal to comply with international standards and to develop a functional financial analysis unit to replace the ineffective CAF. Not long after the visit by Cárdenas, the SIBOIF and other members of the CAF sent a letter to a key National Assembly leader seeking action on creation of a financial intelligence unit.

The Government of Nicaragua needs to move to counter money laundering by expanding the predicate crimes for money laundering beyond narcotics trafficking, criminalizing terrorist financing, and allocating the necessary resources to develop an effective FIU. Nicaragua should develop a more effective method of obtaining information/cooperation from foreign law enforcement agencies and banks. Nicaragua should take steps to immobilize its bearer shares and adequately regulate its gambling industry. These steps, coupled with increased enforcement, would significantly strengthen the country's financial system against money laundering and terrorist financing, and would make progress complying with relevant international anti-money laundering standards and controls.

Nigeria

The Federal Republic of Nigeria is the most populous country in Africa and is West Africa's largest democracy. Nigeria's large economy is also a hub of trafficking of persons and narcotics. Nigeria is a major drug-transit country and is a center of criminal financial activity for the entire continent. It is not an offshore financial center. Individuals and criminal organizations have taken advantage of the country's location, weak laws, systemic corruption, lack of enforcement, and poor economic conditions to strengthen their ability to perpetrate all manner of financial crimes at home and abroad. Nigerian criminal organizations have proven adept at devising new ways of subverting international and domestic law enforcement efforts and evading detection. Their success in avoiding detection and prosecution has led to an increase in many types of financial crimes, including bank fraud, real estate fraud, identity theft, and advance fee fraud. Despite years of government effort to counter rampant crime and corruption, Nigerians continue to be plagued by crime. The establishment of the Economic and Financial Crimes Commission (EFCC) and of the Independent Corrupt Practices Commission (ICPC) and the improvement in training qualified prosecutors in Nigerian courts has yielded some successes in 2005.

In addition to narcotics-related money laundering, advance fee fraud is a lucrative financial crime that generates hundreds of millions of illicit dollars annually for criminals. Initially, Nigerian criminals made advance fee fraud infamous; more recently, nationals of many African countries and from a variety of countries around the world have begun to perpetrate advance fee fraud. This type of fraud is referred to internationally as "Four-One-Nine" fraud (419 is a reference to the fraud section in Nigeria's criminal code). While there are many variations, the main goal of 419 frauds is to deceive victims into payment of an advance fee by persuading them that they will receive a very large benefit in return. These "get rich quick" schemes have ended for some victims in monetary losses, kidnapping, or murder. Through the Internet, businesses and individuals around the world have been and continue to be targeted by perpetrators of 419 scams. The EFCC has tried to combat 419-related cyber crimes, but there have only been a few recorded successes as a result of their cyber crime initiatives.

In June 2001, the Financial Action Task Force (FATF) placed Nigeria on its list of noncooperative countries and territories (NCCT) in combating money laundering. Among the deficiencies cited by the

FATF were the failure to criminalize money laundering for offenses other than those related to narcotics, the lack of customer identification requirements for over-the-counter transactions under a threshold of $100,000, inadequate suspicious transaction reporting requirements, the absence of anti-money laundering measures applied to stock brokerage firms and other financial institutions, and a high level of government corruption. In April 2002, FinCEN, the U.S. financial intelligence unit, issued an advisory to inform banks and other financial institutions operating in the United States of serious deficiencies in the anti-money laundering regime of Nigeria.

In June 2002, the FATF stated that it would consider recommending countermeasures against Nigeria at its October 2002 plenary if Nigeria did not engage with the FATF Africa Middle East Review Group and move quickly to enact legislative reforms that addressed FATF concerns. In October 2002, the FATF recommended countermeasures against Nigeria if the Government of Nigeria (GON) did not enact sufficient legislative reforms by December 15, 2002. That same month, Nigeria submitted an anti-money laundering implementation plan to the FATF, but it was deemed insufficient to justify de-listing Nigeria.

In December 2002, after placement on the NCCT list and under threat of a FATF recommendation for countermeasures, Nigeria enacted three pieces of legislation: an amendment to the 1995 Money Laundering Act that extends the scope of the law to cover the proceeds of all crimes; an amendment to the 1991 Banking and Other Financial Institutions (BOFI) Act that expands coverage of the law to stock brokerage firms and foreign currency exchange facilities, gives the Central Bank of Nigeria (CBN) greater power to deny bank licenses, and allows the CBN to freeze suspicious accounts; and the Economic and Financial Crimes Commission (Establishment) Act that establishes the Economic and Financial Crimes Commission (EFCC), that coordinates anti-money laundering investigations and information sharing. The Economic and Financial Crimes Commission Act also criminalizes the financing of terrorism and participation in terrorism. Violation of the Act carries a penalty of up to life imprisonment. Based on this legislation, FATF decided not to recommend countermeasures against Nigeria; however, Nigeria remains on the NCCT list.

In April 2003, the EFCC was formally constituted, with the primary mandate to investigate and prosecute financial crimes. It has recovered or seized assets from various people guilty of fraud inside and outside of Nigeria, including a syndicate that included highly placed government officials who were defrauding the Federal Inland Revenue Service (FIRS). Several influential individuals have been arrested and are currently awaiting trial. In an effort to expedite the trial process, the Commission has been assigned two high court judges in Lagos and two in Abuja to hear all cases involving financial crimes.

In 2004, the National Assembly passed the Money Laundering (Prohibition) Act (2004), which applies to the proceeds of all financial crimes. It also covers stock brokerage firms and foreign currency exchange facilities, in addition to banks and financial institutions. The legislation gives the CBN greater power to deny bank licenses and freeze suspicious accounts. This legislation also strengthens financial institutions by requiring more stringent identification of accounts, removing a threshold for suspicious transactions, and lengthening the period for retention of records. In November 2004, the EFCC reported that the great majority of Nigeria's banks were not in compliance with the new law, typically by not adhering to the know-your-customer and know-your-customer's-business provisions of the law and by neglecting to file suspicious transactions reports (STRs). The EFCC promised a new initiative to educate bank personnel and the general public about the provisions of the law before imposing sanctions for non-compliance. Nigeria has not yet detected a case of terrorist financing laundered through the banking system.

Under the 2004 Money Laundering (Prohibition) Act and 1995 Foreign Exchange (Monitoring and Miscellaneous Provisions) Act, money laundering controls apply to non-banking financial institutions. These acts effectively cover brokerage houses, stock brokerages, casinos, insurance companies, and

intermediaries such as lawyers and accountants. The Commerce Ministry oversees compliance, which to date has not been very rigorous or effective.

In 2004, the 2002 Economic and Financial Crimes Commission (Establishment) Act was amended. The 2004 EFCC act enlarged the number of EFCC board members, enabled the EFCC police members to bear arms, and banned interim court appeals that hinder the trial court process. The commission's primary mandate is to investigate and prosecute financial crimes, and in particular to coordinate anti-money laundering investigations and information sharing in Nigeria and internationally.

In 2005, the EFCC established the Nigerian Financial Intelligence Unit (NFIU). The NFIU draws its powers from the Money Laundering (Prohibition) Act of 2004 and the Economic and Financial Crimes Commission Act of 2004. It is the central agency for the collection, analysis and dissemination of information on money laundering and terrorism financing. All financial institutions and designated non-financial institutions are required by law to furnish the NFIU with details of their financial transactions. Provisions have been included to give the NFIU power to receive suspicious transaction reports made by financial institutions and non-designated financial institutions, as well as to receive reports involving the transfer to or from a foreign country of funds or securities exceeding $10,000 in value.

The NFIU is a significant component of the EFCC. It complements the EFCC's directorate of investigations but does not carry out its own investigations. It is staffed with competent officials, many with degrees in accounting and law. The NFIU is playing a pivotal role in receiving and analyzing STRs. As a result, banks have improved their responsiveness to forwarding records to the NFIU. Under the EFCC act, whistle-blowers are protected. Nigeria has no secrecy laws that prevent the disclosure of client and ownership information by domestic financial services companies to bank regulatory and law enforcement authorities. The NFIU has access to records and databanks of all government and financial institutions, and it has entered into memorandums of understandings (MOUs) on information sharing with several other financial intelligence centers. The establishment of the NFIU is part of Nigeria's efforts toward removal from the NCCT list.

Nigeria criminalized the financing of terrorism under the Economic and Financial Crimes Commission (Establishment) Act of 2004. The EFCC has authority under the act to identify, freeze, seize, and forfeit terrorist finance-related assets. Statistics do not exist to show any shift in the number of financial crimes committed that are not related to laundering or terrorist financing. However, due to the recent creation of the EFCC, the enactment of new laws, and a successful public enlightenment campaign, crimes such as bank fraud and counterfeiting are being reported and prosecuted for the first time. In addition to the EFCC, the National Drug Law Enforcement Agency (NDLEA), the Independent Corrupt Practices Commission (ICPC), and the Criminal Investigation Department of the Nigeria Police Force (NPF/CID) are empowered to investigate financial crimes. The NDLEA is adequately staffed to meet the basic requirements of the mandate, but its performance has been uneven this year and there have been allegations of corruption. The NDLEA chairman was recently relieved of his duties after a five-year stint, and a new chairman was appointed to improve the agency's performance. The Nigerian Police Force is incapable of handling financial crimes because of corruption and poor institutional capacity. The EFCC is the agency most capable of effectively investigating and prosecuting financial crimes, including money laundering and terrorist financing. The EFCC coordinates all other agencies in financial crimes investigations.

In 2005, the EFCC marked significant successes in combating financial crime. Two fraudsters in a Brazilian bank scam involving a total of $242 million in assets were successfully prosecuted and convicted for terms of 25 and 12 years in prison, respectively. Their assets were seized, and they were ordered to give $110 million in restitution to the bank. Last in 2005, the EFCC returned $4.481 million to an elderly woman swindled by a Nigerian 419 kingpin in 1995. The kingpin was arrested, prosecuted, convicted, and is serving his prison sentence. A former inspector general of police was

arrested and prosecuted for financial crimes valued at over $13 million. His assets were seized and bank accounts frozen. He is currently serving a prison sentence of six months and still faces 92 charges of money laundering and official corruption. Two sitting state governors are currently the subject of money laundering investigations. The EFCC, working with the FBI, also has an active case involving a group of money brokers using banks in the United States to launder money. The money laundering legislation of 2004 has given the EFCC the authority to investigate and prosecute such cases. The EFCC also has the authority to prevent the use of charitable and non-profit entities as laundering vehicles, though no such case has yet been reported. There were 23 money-laundering convictions in 2005. The trial court process has improved after several experienced judges were assigned specifically to handle EFCC cases; this has motivated EFCC officials to bring more cases to court. During 2005, the EFCC seized money laundering-related assets worth $1billion, more than a 100 percent increase from 2004.

Depending on the nature of the case, the tracing, seizing, and freezing of assets may be done by the NDLEA, NPF, or the ICPC, in addition to the EFCC. The proceeds from seizures and forfeitures are remitted to the federal government, and a portion of the recovered sums is used to provide restitution to the victims of the criminal acts. The NDLEA handles all narcotics-related cases. While the NDLEA has adequate resources to trace, seize, and freeze assets, it made no significant asset seizures in 2005.

For cases that are investigated by the EFCC, the seizure of property is governed by the EFCC (Establishment) Act of 2004. Section 20 of the act provides for the forfeiture of assets and properties to the federal government after the accused has been convicted of money laundering, including foreign assets acquired as a result of such crime. The properties subject to forfeiture are set forth in Section 24. They include any real or personal property that represents the gross receipts a person obtains directly as a result of the violation of the act or which is traceable to such gross receipts. They also include any property that represents the proceeds of an offense under the laws of a foreign country within whose jurisdiction such offense or activity would be punishable for a term exceeding one year. Section 25 states that all means of conveyance, including aircraft, vehicles, or vessels that are used or intended to be used to transport or in any manner to facilitate the transportation, sale, receipt, possession or concealment of economic or financial crimes would be punishable. Section 26 provides for circumstances under which property subject to forfeiture may be seized. Under the NDLEA act, farms on which illicit crops are cultivated can be destroyed. The banking community is cooperating with law enforcement to trace funds and seize or freeze bank accounts. It should be noted, however, that forfeiture is currently possible only under the criminal law. There is no comparable law governing civil forfeiture, but a committee has been set up by the EFCC to draft such legislation.

Nigeria 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, and it has signed the UN Convention against Corruption. The United States and Nigeria have a Mutual Legal Assistance Treaty, which entered into force in January 2003. Nigeria has signed memoranda of understanding with Russia, Iran, India, Pakistan and Uganda to facilitate cooperation in the fight against narcotics trafficking and money laundering. Nigeria has also signed bilateral agreements for exchange of information on money laundering with South Africa, the United Kingdom, and all Commonwealth and Economic Community of West African States countries. Nigeria has been instrumental in the establishment of a permanent secretariat for the intergovernmental task force against money laundering in West Africa (GIABA). Nigeria has also ratified the African Union Convention on Preventing and Combating Corruption, which was adopted in Mozambique in July 2003.

The Government of Nigeria has done a better job preventing and pursuing money laundering both within and outside the country in 2005. It should continue to engage with the FATF to ensure that Nigeria's remaining anti-money laundering deficiencies are corrected. The Nigerian Government should continue to pursue their anticorruption program and support both the ICPC and EFCC in their

mandates to investigate and prosecute corrupt government officials and individuals, while at the same time maintaining the independence of those entities from the realm of politics. The supervision of banking and non-banking financial institutions should be strengthened and moved from the Ministry of Commerce. Nigeria should construct a comprehensive anti-money laundering regime that willingly shares information with foreign regulatory and law enforcement agencies, is capable of thwarting money laundering and terrorist financing, and conforms to all relevant international standards.

Pakistan

Financial crimes related to narcotics trafficking, terrorism, smuggling, tax evasion, and corruption remain a significant problem in Pakistan. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets. Pakistan is a major drug-transit country. The proceeds of narcotics trafficking and funding for terrorist activities are often laundered by means of the alternative remittance system called hawala. This system is also widely used by the Pakistani people for legitimate purposes. Reportedly, a network of private unregulated charities has also emerged as a significant source of illicit funds for international terrorist networks.

Pakistan does not have a comprehensive anti-money laundering law. Its current anti-money laundering (AML) regime is weak, outdated and based on a loose patchwork of laws and regulations. The National Accountability Bureau (NAB), the Anti-Narcotics Force (ANF), the Federal Investigative Agency (FIA), and the Customs authorities oversee Pakistan's AML law enforcement efforts. These agencies have had some success in investigating and prosecuting corruption, drug trafficking, and terrorism. The major laws in these areas include: The Anti-Terrorism Act of 1997 which defines the crimes of terrorist finance and money laundering and establishes jurisdictions and punishments (amended in October 2004 to increase maximum punishments); The National Accountability Ordinance of 1999, which requires financial institutions to report suspicious transactions to the NAB and establishes accountability courts; and, The Control of Narcotic Substances Act of 1997, which also requires the reporting of suspicious transactions to the ANF, contains provisions for the freezing and seizing of assets associated with narcotics trafficking, and establishes special courts for offenses (including financing) involving illegal narcotics. All these laws include provisions to allow investigators to access financial records and conduct financial investigations.

Since 2002, Pakistan's Ministry of Finance has been coordinating an inter-ministerial effort to draft AML and counterterrorism financing legislation, with the goal of bringing Pakistan into compliance with international norms. As of December 2005, draft AML legislation was approved by the cabinet and has been transferred to the National Assembly. The draft law provides for the establishment of a Financial Intelligence Unit (FIU). However, the draft legislation does not comport with international standards in several key respects, including its definition of money laundering, which is not consistent with the1988 UN Drug Convention or the UN Convention on Transnational Organized Crime or the FATF recommendations; the forfeiture scheme, particularly where its application is dependent upon a prosecution for the predicate offense; and, the imposition of a threshold requirement for the filing of suspicious transactions reports.

The State Bank of Pakistan (SBP) and the Securities and Exchange Commission of Pakistan (SECP) are the primary financial regulators. Notwithstanding the absence of stand-alone AML legislation, the SBP and SECP, have independently established AML units to enhance their oversight of the financial sector. The SBP has introduced regulations intended to be consistent with FATF recommendations in the areas of "know your customer" policy, record retention, due diligence of correspondent banks, and the reporting of suspicious transactions. The SECP, which has regulatory oversight for non-bank financial institutions, has applied "know your customer" regulations to stock exchanges, trusts, and other non-bank financial institutions. Pakistan's cooperation in the global war on terrorism has brought

renewed focus on the role of informal financial networks in financing terrorist activity. In June 2004, the SBP required all hawalas to register as authorized foreign exchange dealers and to meet minimum capital requirements. Failure to comply was punished by forced closures. However, despite increased enforcement efforts, unregistered hawalas continue to operate illegally. A large percentage of hawala transfers to Pakistan are for the repatriation of wages from the roughly five million Pakistani expatriates residing abroad. The U.S. Government has observed an increasing migration of transactions from the informal to the formal financial institutions sector, due to the GOP's increased regulation of the domestic hawala business, post-September 11 changes in the behavior patterns of overseas Pakistanis, and a substantial increase in credit available in the formal financial sector.

Smuggling, trade-based money laundering and physical cross-border cash transfers are prevalent methods used to launder money and finance terrorism in Pakistan. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets. Goods such as foodstuffs, electronics, vegetable oils, and other products that are primarily exported from Dubai to Karachi are falsely documented as being forwarded to Afghanistan via the "Afghan transit trade". Through smuggling, corruption, avoidance of customs duties and taxes, as well as barter deals for narcotics, many of the goods destined for Afghanistan find their way into the burgeoning Pakistani black market. The trading in these goods and commodities is also believed to be used to provide counter valuation in hawala transactions. A nexus of private, unregulated charities has also emerged as a major source of illicit funds for international terrorist networks.

While a range of terrorist financing risks and vulnerabilities continue to exist, Pakistan has taken significant steps to combat organizations used for terrorist financing and a number of groups have been proscribed as terrorist organizations under the Anti Terrorism Act of 1997. As of December 20, 2005, Pakistan's Central Bank had frozen roughly $10.5 million belonging to 12 entities and individuals associated with Usama Bin Laden, Al Qaeda, or the Taliban, pursuant to UNSCR 1267.

Pakistan is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, either the UN Convention against Transnational Organized Crime or the UN Convention Against Corruption. As of December 2005, Pakistan had not signed the UN International Convention for the Suppression of the Financing of Terrorism. Pakistan is an active member of the Asia/Pacific Group on Money Laundering (APG). In 2005, the APG conducted a peer review (mutual evaluation) of Pakistan's AML/CTF laws, rules and procedures. The APG delegation identified a number of deficiencies and highlighted the need for a comprehensive AML law.

The Government of Pakistan should move quickly to enact an AML law that comports with international standards. It also should issue financial regulations to consolidate and de-conflict the reporting of all suspicious transactions, and establish an FIU consistent with international standards. In addition, in light of the role that private charities have played in terrorist financing, Pakistan should develop a system to regulate the finances of charitable organizations and to close those that finance terrorism. Pakistan also needs to exert greater efforts to track and suppress cash couriers and trade-based money laundering. Pakistan should become a party to the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of Terrorist Financing, and the UN Convention Against Corruption.

Palau

Palau is an archipelago of more than 300 islands in the Western Pacific with a population of nearly 20,000 and per capita GDP of about $6,000. Upon its independence in 1994, the Republic of Palau entered the Compact of Free Association with the United States. The U.S. dollar is legal tender. Palau is not a major financial center. Nor does it offer offshore financial services. There are no offshore banks, trust companies, securities brokers/dealers or casinos in Palau. Palauan authorities believe that drug trafficking and prostitution are the primary sources of illegal proceeds that are laundered.

In January 2005, Palau prosecuted its first ever case under the Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 (MLPCA) against a foreign national engaged in a large prostitution operation. The defendant was convicted on all three counts as well as a variety of other counts.

Amid reports in late 1999 and early 2000 that offshore banks in Palau had carried out large-scale money laundering activities, a few international banks banned financial transactions with Palau. In response, Palau established a Banking Law Review Task Force that recommended financial control legislation to the Olbill Era Kelulau (OEK), the national bicameral legislature, in 2001. Following that, Palau took several steps toward addressing financial security through banking regulation and supervision and putting in place a legal framework for an anti-money laundering regime. Several pieces of legislation were enacted in June 2001.

The Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 criminalized money laundering and created a financial intelligence unit. This legislation imposes suspicious transactions reporting (for suspicious transactions over $10,000) and record keeping requirements for five years from the date of the transaction. Credit and financial institutions are required to keep regular reports of all transactions made in cash or bearer securities in excess of $10,000 or its equivalent in foreign cash or bearer securities. This threshold reporting also covers domestic or international transfers of funds of currency or securities involving a sum greater than $10,000. All such transactions (domestic and/or international) are required to go through a credit or financial institution licensed under the laws of the Republic of Palau.

The Financial Institutions Act of 2001 established the Financial Institutions Commission, an independent regulatory agency, which is responsible for licensing, supervising and regulating financial institutions, defined as banks and security brokers and dealers in Palau. The insurance industry is not currently regulated by the FIC and insurance companies in Palau are primarily agents for companies registered in the U.S. or out of the U.S. Territory of Guam. Currently, there are seven fully licensed banks in Palau and one with a conditional license. Seven of the banks are majority foreign owned, and one is wholly Palauan owned. Three other banks had their licenses invalidated in 2002 and a license of another bank was revoked in 2003. One bank had its license revoked in early 2005 and one bank that is operating on a conditional license has met the conditions for reopening and is now functioning under the supervision of the FIC under a Consent Order. The FIC, Senate and private banks recently met and agreed on revisions to the FIA that are intended to strengthen the supervisory powers of the FIC and promote greater financial stability within Palau's bank market. There has been no indication when these amendments will be heard by the full Senate.

Other entities subject to the provisions of the MLPCA, such as the seven money services businesses, two finance companies and five insurance companies, are essentially unsupervised. Once the amendments to the MLPCA are passed, all alternative money remittance systems will be licensed and regulated by the FIC. The amendments to the MLPCA are have been pending since January 2004 and have no advanced past first reading in the Senate. Credit and financial institutions are required to verify customers' identity and address. In addition, these institutions are required to check for information by "any legal and reasonable means" to obtain the true identity of the principal/party upon whose behalf the customer is acting. If identification cannot, in fact, be obtained, all transactions must cease immediately.

The lack of both and human and fiscal resources has hampered the development of a viable anti-money laundering regime in Palau. The Republic has only recently established a functioning Financial Intelligence Unit (FIU), though its operations are severely restricted by a lack of dedicated human and no dedicated budget. The implementing regulations to ensure compliance with the MLPCA have yet to be written but the authorities have stated that they will be drafted once the revisions to the MLPCA have been passed. The will of the Executive branch to comply with international standards, however, was clearly demonstrated by President Remengesau in 2003, when he vetoed a bill that would have

extended the deadline for bank compliance and would have reduced the minimum capital for a bank from $500,000 to $250,000. Additionally, the President established the Anti-Money Laundering Working Group that is comprised of the Office of the President, the FIC, the Office of the Attorney General, Customs, the FIU, Immigration and the Bureau of Public Safety.

Palau has enacted several legislative mechanisms to foster international cooperation. The Mutual Assistance in Criminal Matters Act (MACA), passed in June 2001, enables authorities to cooperate with other jurisdictions in criminal enforcement actions related to money laundering and to share in seized assets. The Foreign Evidence Act of 2001 provides for the admissibility in civil and criminal proceedings of certain types of evidence obtained from a foreign State pursuant to a request by the Attorney General under the MACA. Under the Compact of Free Association with the United States, a full range of law enforcement cooperation is authorized and in 2004 Palau was able to assist the Department of Justice in a money laundering investigation by securing evidence critical to the case and freezing the suspected funds. Palau has also entered into an MOU with the Taiwan, R.O.C. and the Philippines for mutual sharing of information and inter-agency cooperation in relation to financial crimes and money laundering.

Pursuant to the adoption of the Asia/Pacific Group's (APG) mutual evaluation of Palau at its September 2003 Plenary, the Government of Palau (GOP) has proposed amendments to the MLPCA that, if enacted, would strengthen Palau's anti-money laundering regime. Among the more significant proposals are the following: the promulgation of reporting regulations for all covered financial institutions as well as alternative remittance providers; the requirement to obtain the identification of the beneficial owner of any type of account; mandatory reporting of suspicious transaction reports to the FIU regardless of the amount of the transaction; the requirement that any currency transaction over $5000 be done by wire transfer; the requirement that alternative remittance systems providers report any cash remittance over $500; and, a burden shifting regime for the seizure and forfeiture of assets upon a conviction for money laundering.

The President has also recently proposed the Cash Courier Act of 2004 that was drafted by the Palau Anti-Money Laundering Working Group. To date the CCA has not advanced past first reading in the Senate.

The Omnibus Terrorism Act is currently pending in the OEK since September 2002. If enacted with changes proposed by the President of the Republic, the Act would comport with current international standards, including provisions for the freezing of assets of entities and persons designated by the United Nations as terrorists or terrorist organizations, provisions for the regulation of non-profit entities to prevent abuses by criminal organizations and terrorists and provisions for criminalizing the financing of terrorism. The OEK has issued resolutions ratifying Palau's accession to all the United Nation's Conventions and Protocols relating to terrorism.

The Government of Palau has taken several steps toward enacting a legal framework by which to combat money laundering. It has signed Pacific Island Forum anti-money laundering initiatives and as a member of the Asia/Pacific Group on Money Laundering, Palau is committed to implement the Financial Action Task Force Revised Forty Recommendations and its Nine Special Recommendations on Terrorist Financing. As a party to the UN Convention for the Suppression of the Financing of Terrorism, Palau should criminalize the financing of terrorism. In continuing it efforts to comport with international standards, Palau should enact legislation and promulgate implementing regulations to the MLPCA, as recommended by the APG, including but not limited to establishing funding for the FIU, eliminating the threshold for reporting suspicious transactions and beginning a broad-based implementation of the legal reforms already put in place.

Panama

Panama is a major drug-transit country, and particularly vulnerable to money laundering because of its proximity to major drug-producing countries, its sophisticated international banking sector, its U.S. dollar-based economy, and the Colon Free Zone (CFZs). Some goods originating in or transshipped through the CFZ are purchased with narcotics proceeds (mainly via dollars obtained in the United States) through the Colombian Black Market Peso Exchange. Despite significant progress to strengthen Panama's anti-money laundering regime, Panama must remain vigilant to the threat that money laundering continues to pose to the stability of the country's legitimate financial institutions. The economy of Panama is 80 percent service-based, 14 percent industry and 6 percent agriculture. The service sector is comprised mainly of maritime transportation, commerce, tourism, banking, and financial services.

After Hong Kong and the British Virgin Islands, Panama has the highest number of offshore-registered companies, approximately 350,000. Panama's large offshore financial sector includes international business companies, 34 offshore banks, captive insurance companies (corporate entities created and controlled by a parent company, professional association, or group of businesses), and fiduciary companies. Transfer of negotiable (bearer) bonds is another potential vulnerability that could be exploited by money launderers. The high volume of trade occurring through the CFZ (there are approximately 2,600 businesses established in the Zone) presents opportunities for trade-based money laundering.

Law No. 41 (Article 389) of October 2, 2000, amends the Penal Code by expanding the predicate offenses for money laundering beyond narcotics trafficking, to include criminal fraud, arms trafficking, trafficking in humans, kidnapping, extortion, embezzlement, corruption of public officials, terrorism, international theft, and trafficking of motor vehicles. Law No. 41 establishes a punishment of 5 to 12 years imprisonment and a fine. Law No. 42 of October 2, 2000, requires financial institutions (banks, trust companies, money exchangers, credit unions, savings and loans associations, stock exchanges and brokerage firms, and investment administrators) to report to the Unidad de Análisis Financiero (UAF), Panama's Financial Intelligence Unit (FIU), currency transactions in excess of $10,000 and suspicious financial transactions. Law 42 also mandates that casinos, CFZ businesses, the national lottery, real estate agencies and developers, and insurance/reinsurance companies report to the UAF currency or quasi-currency transactions that exceed $10,000. Furthermore, Law 42 requires Panamanian trust companies to identify to the Superintendence of Banks the real and ultimate beneficial owners of trusts.

In June 2003, the Panamanian Legislative Assembly approved the Financial Crimes Bill (Law No. 45 of June 4, 2003), which establishes criminal penalties of up to ten years in prison and fines of up to one million dollars for financial crimes that undermine public trust in the banking system, the financial services sector, or the stock market. The legislation criminalized a wide range of activities related to financial intermediation, including the following: illicit transfers of monies, accounting fraud, insider training, and the submission of fraudulent data to supervisory authorities. Law No. 1 of January 5, 2004, adds crimes against intellectual property as a predicate offense for money laundering.

Also in June 2003, the Panamanian Legislative Assembly approved Law No. 48 that regulates money remitters. On May 25, 2005, the Panamanian Legislative Assembly approved Law No. 16 that regulates activities of pawnshops and establishes the obligation to report suspicious transactions in these businesses to the UAF.

Executive Order 213 of October 3, 2000, amending Executive Order 16 of 1984 relating to trust operations, provides for the dissemination of information related to trusts to appropriate administrative and judicial authorities. Furthermore, in October 2000, Panama's Superintendence of Banks issued Agreement No. 9 of 2000 that defines requirements that banks must follow for identification of customers, exercise of due diligence, and retention of transaction records and increased the number of

finance company inspections. In 2005, the Superintendence of Banks modified that Agreement, in order to include fiduciary companies within the prevention measures and to bring the Banking Center into line with international standards to be in compliance with Financial Action Task Force (FATF) recommendations.

The Ministry of Commerce and Industries, by means of the Resolutions No. 327 and 328 of August 9, 2004, sought to prevent operations of promotional companies, real estate agents, and money remittance houses being used to commit the crime of money laundering and the financing of terrorism. As a result, these companies are now compelled to identify their clients, declare cash transactions over $10,000, and report suspicious transactions to the UAF.

The Autonomous Panamanian Cooperative Institute established a specialized unit for the supervision of loans and credit cooperatives regarding compliance with the requirements of Law 42. In 2004, the Stock Commission announced that it would begin investigating suspicious activity. During 2005, the National Securities Commission carried out numerous training sessions and workshops for its personnel and regulated entities on money laundering. The CFZ Administration prepared and issued a procedures manual for the users of the CFZ, outlining their responsibilities regarding prevention of money laundering and requirements under Law 42. The UAF continues efforts to raise the level of compliance for reporting suspicious financial transactions, particularly by non-bank financial institutions and businesses in the CFZ.

With support from the Inter-American Development Bank (IDB), the Government of Panama (GOP) is implementing a "Program for the Improvement of the Transparency and Integrity of the Financial System." The Program is targeted, through enhanced communication and information flow, training programs, and technology, at strengthening the capabilities of government institutions responsible for preventing and combating financial crimes and terrorist financed activities. Overall, 1500 employees from 14 institutions have benefited from this training, including representatives of the private sector, stock markets, credit unions, bank compliance officials etc. In addition, with the help of this program, Panama has launched an educational campaign to prevent money laundering and terrorist financing. The program began in 2002 and is intended to raise citizens' awareness of these crimes. In 2004, this program included a training course for the Gaming Control Board and a Hemispheric Congress on Prevention of Money Laundering.

In 2005, a pilot program was developed for money laundering prevention training that was financed by the IDB and executed by the Caribbean Financial Action Task Force (CFATF). Over 5,000 public and private sector employees were trained through this program. Participants included representatives from banks, credit unions, real estate agencies, stockbrokers, insurance companies, CFZ trading companies, financial institutions, and money order companies. The U.S. Government also provided anti-money laundering training in 2005, through the Departments of Justice and Homeland Security.

By means of Law No. 22 of 9 of May of 2002, the GOP adopted the UN International Convention for the Suppression of the Financing of Terrorism. In 2002 the Institute of Autonomous Panamanian Cooperatives, UAF, and the U.S. Embassy Narcotics Assistance Section cosponsored a roundtable on money laundering that offered practical training to financial institutions to assist in meeting the reporting requirements under Law No. 42.

To increase GOP interagency coordination, the UAF and Panamanian Customs are developing an office at the Tocumen International Airport to expedite the entry of customs currency declaration information into the UAF's database. This will enable the UAF to begin more timely investigations. Panamanian Customs continued a program at Tocumen International Airport to deter currency smuggling by seizing and forfeiting all undeclared funds in excess of $10,000 from arriving passengers. Bulk cash shipments, including through Tocumen Airport, continue to be of great concern, with smugglers often under-declaring the amount of cash being brought into the country.

Executive Order No. 163 of October 3, 2000, which amends the June 1995 decree that created the UAF, also allows the UAF to provide information related to possible money laundering directly to the Office of the Attorney General for investigation. The UAF routinely transfers cases to the financial investigations unit (Unidad de Investigaciones Financiera—UIF) for investigation. During 2004 the Financial Fraud Prosecutor's office investigated 2,459 cases related to financial crimes, 86 of which led to a conviction. These included credit card fraud and fraud involving banking institutions. Since money laundering was criminalized in 2000, there have been, to May 2005, ten investigations of money laundering and one conviction. Seven of those cases were tried to a conclusion, one case remains active, and two cases were dismissed. The average prosecution time for money laundering cases is 18.9 months.

GOP cooperation in the investigation of the Western Hemisphere's largest Black Market Peso Exchange money laundering scheme was instrumental in the U.S. conviction in 2002 of Yardena Hebroni, owner of Speed Joyeros, a CFZ enterprise. The GOP also revoked the Panamanian residency of Hebroni, an Israeli national, after she was ordered deported from the United States. In an investigation that was initiated in 2004, the GOP received cooperation from the Government of Nicaragua in a money laundering case against former Nicaraguan President Arnoldo Aleman. In 2005, the Panamanian Judicial System formally indicted Aleman for money laundering and he awaits a preliminary hearing to determine whether the case should go to trial. Also during 2004-2005, there were investigations into possible money laundering and corruption by high-level Costa Rican and Peruvian government officials.

During November 2005, Panamanian authorities initiated their takedown of Operation Nino, which resulted in the arrest of 12 defendants and the seizure of over $1 million as well as a cache of small arms. This case was initiated in late 2004, when Mexican and Colombian-based narcotics traffickers solicited a Panamanian customs inspector to facilitate the smuggling of bulk currency into Panama. The case was significant because over $13 million was smuggled into Panama in an eight-month period. The investigation involved multiple agencies, used Panamanian undercover authority, and targeted bulk currency.

The GOP identified the combating of money laundering as one of five goals in its five-year National Drug Control Strategy issued in 2002. The Strategy commits the GOP to devoting $2.3 million to anti-money laundering projects, the largest being institutional development of the UAF. The UAF currently maintains inter-institutional cooperation agreements with the Attorney General's Office and the Superintendence of Banks, and have signed a cooperation agreement with the Public Registry of Panama.

Decree No. 22 of June 2003, gave the Presidential High Level Commission against Narcotics Related Money Laundering responsibility for combating terrorist financing. Law No. 50 of July 2003 criminalizes terrorist financing and gives the UAF responsibility for prevention of this crime. The Panama Public Force (PPF) and the judicial system have limited resources to deter terrorists, due to insufficient personnel and lack of expertise in handling complex international investigations. On January 18, 2003, the GOP entered into a border security cooperation agreement with Colombia, and also increased funds to the PPF to help secure the frontier. In response to United States efforts to identify and block terrorist-related funds, the GOP continues to monitor suspicious financial transactions.

The GOP also created the Department of Analysis and Study of Terrorist Activities. This department is tasked with working with the United Nations and the Organization of American States to investigate transnational issues, including money laundering. Panama has an implementation plan for compliance with the FATF Forty Recommendations on Money Laundering and its nine Special Recommendations on Terrorist Financing.

Panama and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. The GOP has also assisted numerous countries needing help in strengthening their anti-money laundering programs, including Guatemala, Costa Rica, Russia, Honduras, and Nicaragua. Panama also hosted the Seventh Hemispheric Congress on the Prevention of Money Laundering in August 2003. Executive Decree No. 163 authorizes the UAF to share information with FIUs of other countries, subject to entering into a memorandum of understanding or other information exchange agreement. The UAF has signed more than 27 memoranda of understanding with FIUs, including the Financial Crimes Enforcement Network (FinCEN), the U.S. FIU.

Panama is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD), and is the current Chair of the Caribbean Financial Action Task Force. Panama is also a member of the Offshore Group of Banking Supervisors, and the UAF is a member of the Egmont Group. Panama is a party to the 1988 UN Drug Convention. Panama is a signatory to 11 of the UN terrorism conventions and protocols. During 2002, the GOP became a party to the UN International Convention for the Suppression of the Financing of Terrorism, and in 2004, of the UN Convention against Transnational Organized Crime.

In May 2005, the International Monetary Fund (IMF) conducted an assessment of Panama's Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) regime.

The Government of Panama should continue its regional assistance efforts. It should also continue implementing the reforms it has undertaken to its anti-money laundering regime in order to reduce the vulnerability of Panama's financial sector and to enhance Panama's ability to investigate and prosecute financial crimes, including money laundering and potential terrorist financing.

Paraguay

Paraguay is a principal money laundering center, involving both the banking and non-banking financial sectors. The multi-billion dollar contraband re-export trade that occurs largely on the border shared with Argentina and Brazil (the Triborder Area) facilitates much of the money laundering in Paraguay. Paraguay is a major drug-transit country. The Government of Paraguay (GOP) suspects that proceeds from narcotics trafficking are often laundered, but it is difficult to determine the percentage of the total amount of laundered funds generated from narcotics sales. Weak controls in the financial sector, an open border, and minimal enforcement activity for financial crimes allow money launderers and terrorist financiers to take advantage of Paraguay's financial system. Although the Government of Paraguay (GOP) has made some progress in 2005, it will need to pursue more aggressive policies in 2006 in order to increase its effectiveness in combating money laundering and terrorist financing.

Paraguay is particularly vulnerable to money laundering, as little personal background information is required to open a bank account or to make financial transactions in Paraguay. Paraguay is an attractive financial center for neighboring countries, particularly Brazil. Foreign banks are registered in Paraguay and nonresidents are allowed to hold bank accounts, but current regulations forbid banks from advertising or seeking deposits from outside the country. Paraguay is not considered to be an offshore financial center, but the GOP does allow representative offices of offshore banks to maintain a presence in the country. Shell companies are not permitted; trusts, however, are permitted and are regulated by the Central Bank. The Superintendent of Banks audits financial institutions and supervises all banks under the same rules and regulations. However, there are few effective controls over businesses, and a large informal economy exists outside the regulatory scope of the GOP.

Money laundering in Paraguay is facilitated by the multi-billion dollar contraband re-export trade that occurs largely in the Triborder Area shared by Paraguay, Argentina, and Brazil. Ciudad del Este (CDE), on the border between Brazil and Paraguay, represents the heart of Paraguay's informal economy. The area is well known for arms and narcotics trafficking, as well as crimes against

intellectual property rights. A wide variety of counterfeit goods, including cigarettes, CDs, DVDs, and computer software, are imported from Asia and transported primarily across the border into Brazil, with a significantly smaller amount remaining in Paraguay for sale in the local economy. Some senior government officials, including members of Congress, have been accused of involvement in the smuggling of contraband or pirated goods. To date, there have been few criminal investigations, much less prosecutions of senior GOP officials' involvement in smuggling contraband or pirated goods. Government officials, in both Paraguay and the United States, also suspect the area to be a source of terrorist financing. Raids in CDE have led to the seizure of extremist Islamic materials and receipts of wire transfers from Paraguay to the Middle East and the United States. Paraguay has taken some measures to tackle this "gray" economy and to develop strategies to implement a formal, diversified economy.

A new law to improve the effectiveness of Paraguay's anti-money laundering regime was drafted in late 2003 and was formally introduced to Congress in May 2004. The new money laundering legislation, if approved, will institute important reforms. In addition to confirming the UAF's role as the sole FIU, it establishes SEPRELAD as an independent secretariat or agency reporting directly to the Office of the President. The draft law also establishes money laundering as an autonomous crime punishable by a prison term of five to 20 years. It establishes predicate offenses as any crimes that are punishable by a prison term exceeding six months, and specifically criminalizes money laundering tied to the financing of terrorist groups or acts. The full range of covered institutions will be required to report suspicious transactions to the UAF and to maintain registries of large currency transactions that equal or exceed $10,000.

Other provisions of the draft law include penalties for failure to file or falsification of reports, "know your client provisions," and standardized record keeping for a minimum of seven years. The UAF will continue to refer cases as appropriate for further police (SENAD) investigation and to the Attorney General's Office for prosecution. It will also serve as the central entity for related information exchanges with other concerned foreign entities. The law further specifies that the financial crimes investigative unit of SENAD is the principal authority for carrying out all counternarcotics and other financial investigations, including money laundering, and will also have the authority to initiate investigation of cases on its own.

There are other challenges, however, that the new money laundering legislation, when passed, will not address. With only eight positions available for prosecutors dedicated to financial crimes, of which only six are filled, Paraguay currently has limited resources to investigate and prosecute money laundering and financial crimes. New criteria were issued in 2005 for the selection of judges, prosecutors and public defenders; however, the process remains one that is largely based on politics, nepotism and influence peddling, affording the ruling party an opportunity to manipulate the justice system to its advantage.

Moreover, unless the new law is enacted, most judges have little incentive to investigate money laundering cases because many believe that sentencing on predicate offenses is sufficient punishment. Thus, there have not been any successful money laundering prosecutions in Paraguay so far, and improvement is unlikely until the new law becomes a reality. As it is, those individuals implicated in money laundering are typically prosecuted on tax evasion charges. For example, in May 2004, Assad Barakat—widely alleged to be involved in money laundering—was convicted of tax evasion and sentenced to six and one-half years in prison. In late 2004, prosecutors began investigating several tax evasion cases involving suspected money laundering by both authorized and unauthorized money exchange offices in Ciudad del Este. A preliminary hearing is scheduled in December 2005 for Kassem Hijazi, who is suspected of having laundered proceeds from illicit activities in the Triborder Area and sending a portion of those funds to support Lebanese Hizbollah activities.

In 2005, in cooperation with the U.S. Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Paraguay began the process of developing a prototype Trade Transparency Unit (TTU) that will examine discrepancies in trade data that could be indicative of customs fraud or trade-based money laundering. The development of such a unit constitutes a positive step with respect to Special Recommendation VI of the Financial Action Task Force (FATF) on the use of alternative remittance systems. Trade-based systems such as hawala and black market exchanges often use fraudulent trade documents and over and under-invoicing schemes to provide countervaluation in transferring value and settling accounts.

In 2003, the GOP noted that it was trying to introduce "maquilas" (assembly line industries). In 2005, the maquilas sector experienced rapid growth with 23 maquilas currently in operation. The largest maquila, a synthetic rubber factory, is Brazilian-owned and located just outside of Ciudad del Este. The company has invested $18 million in the project, one of the largest foreign investments in the Paraguayan economy. The GOP is trying to strengthen its tourism industry by proposing advances to its tourism infrastructure such as the international airport in Asuncion, making it a regional transportation hub for cargo and possibly passenger airlines. The new customs code implemented in early 2004 provides for the creation of formal free trade zones. One zone currently exists in Ciudad del Este and another is planned for the town of Villeta, near Asuncion. Paraguay's customs agency is responsible for monitoring these zones; however, there is little oversight. As a result, the addition of free trade zones may provide additional venues for money laundering.

There are no effective controls on the amount of currency that can be brought into or out of Paraguay. Cross-border reporting requirements are limited to those issued by airlines at the time of entry into Paraguay. Persons transporting $10,000 into or out of Paraguay are required to file a customs report, but these reports are often not actually collected or checked. Customs operations at the airports or land ports of entry provide no control of the cross-border movement of cash. The non-bank financial sector, particularly exchange houses, is used to move illegal proceeds both from within and outside of Paraguay into the formal banking system of the United States. Most of these funds move from Brazil through Ciudad del Este to the banking sector. Paraguay exercises a dual monetary system in which most high-priced goods are paid for in U.S. dollars. Large sums of dollars generated from normal commercial activity and suspected illicit commercial activity are transported physically from Paraguay through Uruguay to banking centers in the United States. Within the past year, the GOP has begun to recognize and address the problem of the international transportation of currency and monetary instruments derived from illegal sources.

Bank fraud, which has led to several bank failures, and other financial crimes related to corruption, are serious problems in Paraguay. Following bank failures in 2002 and 2003, Paraguay continues to experience problems in the banking industry. In 2004, Citibank decided to end its participation in small-consumer banking in Paraguay, and subsequently closed almost all of its branches nationwide. The GOP continues to work with the U.S. Treasury and Justice Departments to trace, account for, and return the missing $16 million diverted from the Central Bank in 2002 to private accounts allegedly linked to the family of former President Luis Gonzalez Macchi.

Money laundering is a criminal offense under Paraguay's two anti-money laundering statutes, Law 1015 of 1996 and Article 196 of Paraguay's Criminal Code, adopted in 1997. The existence of the two laws has led to substantial confusion due to overlapping provisions. Under Article 196, the scope of predicate offenses includes only offenses that carry a maximum penalty of five years or more; Law 1015 includes additional offenses. Article 196 also establishes a maximum penalty of five years for money laundering offenses, while Law 1015 carries a prison term of two to ten years. This is particularly significant because, under the new Criminal Code and Criminal Procedure Code, defendants who accept charges that carry a maximum penalty of five years or less are automatically entitled to a suspended sentence and a fine instead of jail time, at least for the first offense. Since a defendant cannot be charged with money laundering unless he or she has first been convicted of the

predicate offense, many judges are apparently reluctant to prosecute any defendant on money laundering charges because a sentence has already been issued for a predicate offense.

Law 1015 of 1996 also contains "due diligence" and "banker negligence" provisions and applies money laundering controls to non-banking financial institutions, such as exchange houses. Bank secrecy laws do not prevent banks and financial institutions from disclosing information to bank supervisors and law enforcement entities. Under Paraguay's Commercial Law 1023 and Law 1015, banks are required to maintain account records for five years, but there is little government enforcement of this regulation. However, bankers and others are protected under the anti-money laundering law with respect to their cooperation with law enforcement agencies. Additional provisions of Law 1015 require banks and financial institutions to know and record the identity of customers engaging in significant currency transactions and to report those, as well as suspicious activities, to Paraguay's financial intelligence unit (FIU), the Unidad de Análisis Financiera (UAF).

The UAF began operating in 1997 within the Secretary for the Prevention of Money Laundering (SEPRELAD), under the auspices of the Ministry of Industry and Commerce (MIC). In recent years, the GOP has made significant efforts to strengthen SEPRELAD, which for years had suffered from a burdensome bureaucratic structure, lack of financial support, and the inability to keep trained personnel. As a result, cooperation between SEPRELAD and other government agencies on anti-money laundering issues has improved significantly over the last two years. Initially reluctant to seek SEPRELAD's assistance due to past weaknesses, most government entities are increasingly prepared to work with SEPRELAD. Reporting from obligated entities has also increased, with the UAF receiving over 1,000 suspicious activity reports in 2005. In 2004, SEPRELAD helped to create and coordinate an interagency money laundering working group, whose members include the director of the UAF, the director of the Financial Crimes Investigation Unit of the National Anti-Drug Secretariat (SENAD), the Assistant Attorney General for Economic Crimes, the Superintendent of Banks, the Vice Minister for Tax Administration of the Ministry of Finance, the director of Customs, and a criminal appellate judge. SEPRELAD has signed several agreements with other government entities to strengthen interagency cooperation, including memoranda of understanding with the Public Ministry and the Superintendence of Banks.

The UAF and the Superintendence of Banks have also improved cooperation between their two entities, which had been strained by the creation of a second FIU in the Superintendence in 2001. In 2003, the "Risk Control Division" was created to replace the Superintendent of Banks' FIU and eliminate its duplicative function with the UAF. The Risk Control Division has the primary responsibility of reviewing the records of national financial institutions for suspected terrorist activity and is empowered to coordinate information exchange with the Central Banks of other MERCOSUR countries. According to SEPRELAD officials, cooperation between the UAF and the Risk Control Division improved significantly in 2005. The two groups signed a memorandum of understanding (MOU) in October 2005, laying out the provisions for increased cooperation. The MOU includes provisions for SEPRELAD to issue regulations for the banking industry, including the designations of a compliance officer and utilizing due diligence and "know your customer" policies. The UAF has since issued these regulations in Resolution 233 of October 11, 2005.

The UAF is seeking to strengthen its relationship with other financial intelligence units and has signed agreements for information exchange with regional financial intelligence units. In March 2005, the UAF and the U.S. financial intelligence unit, the Financial Crimes Enforcement Network (FinCEN), signed an MOU to resume information exchange following a four-year suspension. The sharing of financial information between the two units had been suspended by FinCEN in May 2001 following an unauthorized disclosure of FinCEN information by the GOP. Information exchange was resumed following an evaluation of the progress made by the UAF and the strengthening of internal procedures for disseminating financial information. The UAF also increased its role in regional and international anti-money laundering groups, including the Egmont Group and the Financial Action Task Force for

South America (GAFISUD). The UAF's director participates in the GAFISUD FIU Working Group and a committee within the Egmont Group, further expanding Paraguay's role in these organizations. GAFISUD conducted its second mutual evaluation of Paraguay in September 2005. The results of this evaluation, which have not yet been made public, were presented at the GAFISUD plenary meetings in December.

Under current laws, the GOP has limited authority to freeze, seize, or forfeit assets of suspected money launderers. In most cases, assets that the GOP is permitted to freeze, seize, or forfeit are limited to transport vehicles, such as planes and cars, and normally do not include bank accounts. However, authorities may not auction off these assets until a conviction is announced by the judicial system. At best, the GOP can establish a "preventative embargo" against assets of persons under investigation for a crime in which the state risks loss of revenue from furtherance of a criminal act, such as tax evasion. However, in those cases the limit of the embargo is set as the amount of liability of the suspect to the government. The new anti-money laundering legislation will, when passed, allow prosecutors to recommend that judges freeze or confiscate assets connected to money laundering and its predicate offenses. The draft law also provides for the creation of a special asset forfeiture fund to be administered by a consortium of national governmental agencies, which will support programs for crime prevention and suppression, including combating money laundering, and related training.

The GOP currently has no authority to freeze, seize, or forfeit assets related to the financing of terrorism. The financing of terrorism is not criminalized under current Paraguayan law. However, the Ministry of Foreign Affairs often provides the Central Bank and other government entities with the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee consolidated list. Through 2005, the GOP has not identified, seized, or forfeited any such assets linked to these groups or individuals. The current law also does not provide any measures for thwarting the misuse of charitable or non-profit entities that can be used as conduits for the financing of terrorism. Following the submission of the draft anti-money laundering law to Congress in May 2004, a working group began drafting legislation to address terrorism and terrorist financing. The draft legislation will allow the GOP to conform to international standards on the suppression of terrorist financing. The draft anti-money laundering legislation will also specifically criminalize money laundering tied to the financing of terrorist groups or acts.

The GOP ratified the UN International Convention for the Suppression of the Financing of Terrorism in November 2004 and the Inter-American Convention on Terrorism in January 2005. In June 2005, Paraguay ratified the UN Convention against Corruption. Paraguay is also a party to the UN Convention against Transnational Organized Crime, which it ratified in September 2004, as well as the 1988 UN Drug Convention. The GOP participates in Summit of the Americas and Inter-American Drug Abuse Control Commission (CICAD)-related meetings on money laundering, and is a member of the South American Financial Action Task Force (GAFISUD), the Egmont Group, and the "3 Plus 1" Security Group between the United States and the Triborder Area countries.

While the Government of Paraguay took a number of positive steps in 2005, there are other initiatives that should be pursued to increase the effectiveness of Paraguay's efforts to combat money laundering and terrorist financing. Most important is enactment of the new money laundering law intended to meet international standards. Uneven political support for the new money laundering law has hindered its passage in Congress. Paraguay also needs to continue its efforts to combat corruption and increase information sharing among concerned agencies when and if the corruption issues are resolved. Paraguay does not have a counterterrorism law or a law criminalizing terrorist financing; while the new money laundering law would increase the GOP's abilities to combat terrorist financing, it should also take steps as quickly as possible to ensure that comprehensive counterterrorism legislation is passed. Reforms to the criminal procedure code that would allow prosecutors to carry out long-term criminal investigations should be considered. Further reforms in the selection of judges, prosecutors and public defenders are needed. Reforms to the customs agency are also necessary in order to allow

for increased inspections and interdictions at ports of entry and to develop strategies targeting the physical movement of bulk cash. It is essential that the Unidad de Análisis Financiera (UAF) continue to receive the financial and human resources necessary to operate as an effective, fully functioning financial intelligence unit capable of effectively combating money laundering, terrorist financing, and other financial crimes.

Peru

Peru is not a major regional financial center, nor is it an offshore money laundering haven. Peru is a major drug producing and drug-transit country. Narcotics-related and other money laundering does occur, and the Government of Peru (GOP) has taken several steps to improve its money laundering legislation and enforcement abilities. Nevertheless, more reliable and adequate mechanisms are necessary to better assess the scale and methodology of money laundering in Peru. Peru is the world's second largest producer of cocaine, and, although no reliable figures exist regarding the exact size of the narcotics market in Peru, conservative estimates indicate that the cocaine trade generates between 1.5 to two billion dollars per year. As a result, money laundering is believed to occur on a significant scale in order to integrate these illegal proceeds into the Peruvian economy.

Money laundering has historically been facilitated by a number of factors, primarily Peru's cash-based economy. Peru's economy is heavily dependent upon the U.S. dollar, and approximately 65 percent of the economy is dollarized, allowing traffickers to handle large bulk shipments of U.S. currency with minimal complications. Currently no restrictions exist on the amount of foreign currency an individual can exchange or hold in a personal account, and until recently, there were no controls on bulk cash shipments coming into Peru.

Corruption remains an issue of serious concern in Peru. It is estimated that 15 percent of the public budget is lost due to corruption. A number of former government officials, most from the Fujimori administration, are under investigation for corruption-related crimes, including money laundering. These officials have been accused of transferring tens of millions of dollars in proceeds from illicit activities (e.g., bribes, kickbacks, or protection money) into offshore accounts in the Cayman Islands, the United States, and/or Switzerland. The Peruvian Attorney General, a Special Prosecutor, the office of the Superintendent of Banks (SBS) and the Peruvian Congress have conducted numerous investigations, some of which are ongoing, involving dozens of former GOP officials. In 2004, the GOP continued to make strong efforts at uncovering and recovering the millions of U.S. dollars believed to be the proceeds of money laundering activities carried out by Vladimiro Montesinos, former director of the Peruvian National Intelligence Service. However, anti-money laundering legislation was very limited prior to 2002. Therefore, obtaining money laundering convictions for crimes committed prior to 2002 will be challenging.

In 2005, the GOP obtained its first two convictions against money laundering. One case was related to public corruption, the other involved the laundering of drug proceeds. There are three cases currently being prosecuted in the Peruvian court system.

Beginning in June 2002, Peru has adopted substantial changes to its existing anti-money laundering regime, significantly broadening the definition of money laundering beyond a crime associated with narcotics trafficking. Prior to the changes, money laundering was only a crime when directly linked to narcotics trafficking and "narcoterrorism," It also included nine predicate offenses that did not include corruption, bribery or fraud. Under Law 27.765 of 2002, predicate offenses for money laundering were expanded to include the laundering of assets related to all serious crimes, such as narcotics trafficking, terrorism, corruption, trafficking of persons, and kidnapping. However, there remains confusion on the part of some GOP officials and attorneys as to whether money laundering must still be linked to the earlier list of predicate offenses. The law's brevity and lack of implementing regulations are also likely to limit its effectiveness in obtaining convictions. However, reportedly, money laundering is an

autonomous offense. There does not have to be a conviction relating to the predicate offense. Rather it must only be established that the predicate offense occurred and that the proceeds of crime from that offense were laundered.

The penalties for money laundering were also revised in 2002. Instead of a life sentence for the crime of laundering money, Law 27.765 sets prison terms of up to 15 years for convicted launderers, with a minimum sentence of 25 years for cases linked to narcotics trafficking, terrorism, and laundering through banks or financial institutions. In addition, revisions to the Penal Code criminalize "willful blindness," the failure to report money laundering conducted through one's financial institution when one has knowledge of the money's illegal source, and imposes a three to six year sentence for failure to file suspicious transaction reports.

Law 27.693 of 2002 provided for the creation of Peru's financial intelligence unit, the Unidad de Inteligencia Financiera (UIF). Reportedly, recent changes have the UIF under the Ministry of Justice. The UIF began operations in June 2003 and today has 52 personnel. As Peru's financial intelligence unit, the UIF is the government entity responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs) filed by obligated entities. Law 27.693 and Law 28.306 of 2004 expanded the entities obligated to report suspicious transactions beyond just banks and financial institutions. In addition to financial institutions, insurance companies, stock funds and brokers, the stock and commodities exchanges, credit and debit card companies, money exchange houses, mail and courier services, travel and tourism agencies, hotels and restaurants, notaries, the customs agency, casinos, auto dealers, construction or real estate firms, notary publics, and dealers in precious stones and metals are all required to report suspicious transactions to the UIF within 30 days. The FIU cannot receive STRs electronically; covered entities must hand-deliver STRs to the UIF.

In addition to the predicate offenses in Law 27.693, Law 28.306 of 2004 mandates that obligated entities also report suspicious transactions related to terrorist financing, and expanded the UIF's functions to include the ability to analyze reports related to terrorist financing. Terrorist financing is criminalized under Executive Order 25.475.

Obligated entities are also required to maintain reports on large cash transactions. Individual cash transactions exceeding $10,000 or transactions totaling $50,000 in one month must be maintained in internal databases for a minimum of five years and made available to the UIF upon request. Non financial institutions, such as exchange houses, casinos, lotteries or others, must report individual transactions over $2,500 or monthly transactions over $10,000. Individuals or entities transporting more than $10,000 in currency or monetary instruments into or out of Peru must file reports with the customs agency, and the UIF may have access to those reports upon request.

Reporting requirements for suspicious transactions entered into effect in September 2003, and as of November 2005, the UIF had received 869 STRs. Of those, the UIF asked the submitting entity for additional information on approximately 70 percent of the reports. Under Law 28.306, the UIF is able to sanction persons and entities for failure to report suspicious transactions, large cash transactions, or the transportation of currency or monetary instruments. The UIF also has regulatory responsibilities for all obligated entities that do not fall under the supervision of another regulatory body (such as the Superintendence of Banks).

The UIF currently does not receive cash transactions reports (CTRs) or reports on the international transportation of currency or monetary instruments. CTRs are maintained in internal registries within the obligated entities, and reports on the international transportation of currency or monetary instruments are maintained by the customs agency. If the UIF receives an STR and determines that the STR warrants further analysis, it contacts the covered entity that filed the report for additional background information—including any CTRs that may have been filed—and/or the customs agency to determine if the subject of the STR had reported the transportation of currency or monetary instruments. Some requests for reports of transactions over $10,000—such as those that are deposits

into savings accounts—are protected under the constitution by bank secrecy provisions and require an order from the Public Ministry or SUNAT, the tax authority. A period of 15-30 days is required to lift the bank secrecy restrictions. All other types of cash transaction reports, however, may be requested directly from the reporting institution. There are two bills under consideration in Congress that would make bank secrecy provisions less stringent and strengthen disclosure requirements.

To assist with its analytical functions, the UIF may request information from such government entities as the National Superintendence for Tax Administration, Customs, the Securities and Exchange Commission, the Public Records Office, the Public or Private Risk Information Centers, and the National Identification Registry and Vital Statistics Office, among others. However, the UIF can only share information with other agencies—including foreign entities—if there is a joint investigation underway. Once the UIF has completed the analysis process and determined that a case warrants further investigation or prosecution, the case is sent to the Public Ministry.

As of November 2005, the UIF had sent 36 suspected cases of money laundering to the Public Ministry for investigation. Of those cases, six investigations have been completed and are being presented to the judiciary for prosecution. The UIF has also assisted the Public Ministry with two cases that resulted in money laundering convictions. Although the cases did not originate with the UIF, the UIF's assistance in analyzing financial information was fundamental in gaining the two convictions for money laundering.

Within the counternarcotics section of the Public Ministry, two specialized prosecutors are responsible for dealing with money laundering cases. In addition to being able to request any additional information from the UIF in their investigations, the Public Ministry may also request the assistance of the Directorate of Counter-Narcotics (DINANDRO) of the Peruvian National Police. With the passage of Law 28.306 in July 2004, DINANDRO and the UIF are now able to collaborate on investigations, although each agency must go through the Public Ministry in order to do so. DINANDRO may provide the UIF with intelligence for the cases the UIF is analyzing, while it provides the Public Ministry with assistance on cases that have been sent to the Public Ministry by the UIF.

The UIF was given regulatory responsibilities in July 2004 under Law 28.306. Most covered entities fall under the supervision of the Superintendence of Banks and Insurance (banks, the insurance sector, financial institutions), the Peruvian Securities and Exchange Commission (securities, bonds), and the Ministry of Tourism (casinos). All entities that are not supervised by these three regulatory bodies, such as auto dealers, construction and real estate firms, etc., fall under the supervision of the UIF. However, some covered entities remain unsupervised. For instance, although money remittance businesses are regulated by the Superintendence of Banks, the Superintendence is not required to supervise any money remittance business that does less than 1,240,000 soles (about $400,000) in transfers per year. There is also difficulty in regulating casinos, as roughly 60 percent of that sector is informal. An assessment of the gaming industry conducted by GOP and U.S. officials in 2004 identified alarming deficiencies in oversight and described an industry that is vulnerable to being used to launder large volumes of cash. Approximately 580 slot houses operate in Peru, with less than 65 percent or so paying taxes. Estimates indicate that less than 42 percent of the actual income earned is being reported, while official gaming revenues totaled $650 million in 2003. This billion-dollar cash industry continues to operate with little supervision.

Peru currently lacks comprehensive and effective asset forfeiture legislation. The Financial Investigative Office of DINANDRO has seized numerous properties over the last several years, but few were turned over to the police to support counternarcotics efforts. While Peruvian law does provide for asset forfeiture in money laundering cases, and these funds can be used in part to finance the UIF, no clear mechanism exists to distribute seized assets among government agencies. The government's "Fedadoi" fund currently holds around $75 million in monies recovered after having

been stolen or diverted during the Fujimori administration. A bill to amend the asset forfeiture regime is being considered by Congress.

Terrorism is considered a problem in Peru, which is home to the terrorist organization Shining Path. Although the Shining Path has been designated by the United States as a foreign terrorist organization pursuant to Section 219 of the Immigration and Nationality Act and under Executive Order (E.O.) 13224, and the United States and 100 other countries have issued freezing orders against its assets, the GOP has no legal authority to quickly and administratively seize or freeze terrorist assets. In the event that such assets are identified, the Superintendent for Banks must petition a judge to seize or freeze them and a final judicial decision is then needed to dispose of or use such assets. Peru also has not yet taken any actions to thwart the misuse of charitable or non-profit entities that can be used as conduits for the financing of terrorism.

Foreign Ministry Officials are working with other GOP agencies to complete the necessary legal revisions that will permit asset-freezing actions. The Office of the Superintendent of Banks routinely circulates to all financial institutions in Peru updated 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, the Taliban, and al-Qaida, as well as those on the list of Specially Designated Global Terrorist Entities designated by the United States pursuant to E.O. 13224 on terrorist financing. To date, no assets connected to designated individuals or entities have been identified, frozen, or seized.

Peru ratified the UN International Convention for the Suppression of the Financing of Terrorism on November 10, 2001, and the Organization of American States Inter-American Convention on Terrorism in 2003. Peru is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GOP participates in the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group. Peru is also a member of the South American Financial Action Task Force (GAFISUD), and in 2005 held the GAFISUD presidency. Peru also underwent a mutual evaluation by GAFISUD in 2005, the results of which were reported to the GAFISUD plenary in July. In June 2005, the UIF became a member of the Egmont Group of financial intelligence units. An extradition treaty between the U.S. Government and the GOP entered into force in 2003.

The Government of Peru has made significant advances in strengthening its anti-money laundering regime in recent years. However, some progress is still required. There are still a number of weaknesses in Peru's anti-money laundering system: bank secrecy must be lifted in order for the Unidad de Inteligencia Financiera to have access to certain cash transaction reports, smaller financial institutions are not regulated, and the UIF is not able to work directly with law enforcement agencies; rather, the Public Ministry must coordinate any collaboration between the UIF and the other agency. Anticorruption efforts in Peru should be a priority, and Peru should also enact legislation that allows for administrative as well as judicial blocking of terrorist assets. These issues should be addressed in order to strengthen Peru's ability to combat money laundering and terrorist financing.

Philippines

The Philippines is a regional financial center. In the past few years, the illegal drug trade in the Philippines reportedly has evolved into a billion-dollar industry. The Philippines continues to experience an increase in foreign organized criminal activity from China, Hong Kong, and Taiwan. Reportedly, insurgency groups operating in the Philippines fund their activities, in part, through the trafficking of narcotics and arms, as well as engaging in money laundering through alleged ties to organized crime. The proceeds of corrupt activities by government officials are also a source of laundered funds. Most of the narcotics trafficking transiting through the Philippines is exchanged using letters of credit. There is little cash and negligible amounts of U.S. dollars used in the

transactions, except for the small amounts of narcotics that make it all the way to the United States for street sale. Drugs circulated within the Philippines are usually exchanged for local currency.

In June 2000, the Financial Action Task Force (FATF) placed the Philippines on its list of Non-Cooperative Countries and Territories (NCCT) for lacking basic anti-money laundering regulations, including customer identification and record keeping requirements, and excessive bank secrecy provisions.

The Government of the Republic of the Philippines (GORP) initially established an anti-money laundering regime by passing the Anti-Money Laundering Act of 2001 (AMLA). The GORP enacted Implementing Rules and Regulations (IRR) for the AMLA in April 2002. The AMLA criminalized money laundering, an offense defined to include the conduct of activity involving the proceeds from unlawful activity in any one of 14 major categories of crimes, and imposes penalties that include a term of imprisonment of up to 14 years and a fine no less than 3,000,000 pesos (approximately $54,000); but no more than twice the value or property involved in the offense. The Act also imposed identification, record keeping, and reporting requirements on banks, trusts, and other institutions regulated by the Central Bank, insurance companies, securities dealers, foreign exchange dealers, and money remitters, as well as any other entity dealing in valuable objects or cash substitutes regulated by the Securities and Exchange Commission (SEC).

However, the FATF deemed the original legislation inadequate and pressured the Philippines to amend the legislation to be more in line with international standards. The GORP subsequently made important progress in developing its anti-money laundering and terrorist financing regime, with the enactment of amendments to the Anti-Money Laundering Act of 2001 in March 2003. The amendments to the AMLA lowered the threshold amount for covered transactions (cash or other equivalent monetary instrument) from 4,000,000 pesos to 500,000 pesos ($80,000 to $10,000) within one banking day; expanded financial institution reporting requirements to include the reporting of suspicious transactions, regardless of amount; authorized the Central Bank (Bangko Sentral ng Pilipinas or BSP) to examine any particular deposit or investment with any bank or non-bank institution in the course of a periodic or special examination (in accordance with the rules of examination of the BSP); ensured institutional compliance with the Anti-Money Laundering Act; and deleted the prohibitions against the Anti-Money Laundering Council's examining particular deposits or investments opened or created before the Act.

The FATF deemed those amendments to have sufficiently addressed the main legal deficiencies in the original Philippines anti-money laundering regime, and decided not to recommend the application of countermeasures. The FATF removed the Philippines from its Non-Cooperating Countries and Territories (NCCT) List in February 2005.

The AMLA established the Anti-Money Laundering Council (AMLC) as the country's financial intelligence unit (FIU). The Council is composed of the Governor of the Central Bank, the Commissioner of the Insurance Commission, and the Chairman of the Securities and Exchange Commission. By law, the AMLC Secretariat is an independent agency responsible for receiving, maintaining, analyzing, and evaluating covered and suspicious transactions. It provides advice and assistance to relevant authorities and issues relevant publications. The AMLC completed the first phase of its information technology upgrades in 2004. This was a significant milestone that allowed AMLC to electronically receive, store, and search CTRs filed by regulated institutions. Through 2005, the AMLC had received more than 1,760 suspicious transaction reports (STRs) involving 8,144 suspicious transactions, and had received over 44 million covered transaction reports (CTRs). AMLC is currently in the process of acquiring software to implement link analysis and visualization to enhance its ability to produce information in graphic form from the CTRS and STRs filed electronically by regulated institutions.

AMLC's role goes well beyond traditional FIU responsibilities and includes the investigation and prosecution of money laundering cases. AMLC has the ability to seize terrorist assets involved in money laundering on behalf of the Republic of the Philippines after a money laundering offense has been proven beyond a reasonable doubt. In order to freeze assets allegedly connected to money laundering, the AMLC must establish probable cause that the funds relate to an offense enumerated in the Act, such as terrorism. The Court of Appeals then may freeze the bank account for 20 days. The AMLC may apply to extend a freeze order prior to its expiration. The AMLC is required to obtain a court order to examine bank records for activities not listed in the Act, except for certain serious offenses such as kidnapping for ransom, drugs, and terrorism-related crimes. The AMLC and the courts are working to shorten the time needed so funds are not withdrawn before the freeze order is obtained.

The Philippines has no comprehensive legislation pertaining to civil and criminal forfeiture. Various government authorities, including the Bureau of Customs and the Philippine National Police, have the ability to temporarily seize property obtained in connection with criminal activity. Money and property must be included in the indictment, however, to permit forfeiture. Because ownership is difficult to determine in these cases, assets are rarely included in the indictment and are rarely forfeited. The AMLA gives the AMLC the authority to seize assets involved in money laundering operations that may end up as forfeited property after conviction, even if it is a legitimate business. In December 2005, the Supreme Court issued a new criminal procedure rule covering civil forfeiture, asset preservation, and freeze orders. The new rule provides a way to preserve assets prior to any forfeiture action and lists the procedures to follow during the action. The rule also contains clear direction to the AMLC and the court of appeals on the issuance of freeze orders for assets under investigation that had been confused by changes in the amendment to the AMLA in 2003. There are currently 88 prosecutions underway in the Philippine court system that involved AMLC investigations or prosecutions, including 34 for money laundering, 24 for civil forfeiture, and the rest pertaining to freeze orders and bank inquiries. Although some of these cases may conclude shortly, to date the Philippines has not had a money laundering conviction.

The GORP is quick to respond when new terrorist entities are added to the list of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. Upon notification that the UN 1267 Sanctions Committee has approved an additional name to the consolidated list, the AMLC takes immediate steps to inform the local banks and issue orders to freeze the assets in the banking system. Under the AMLA and the bank secrecy act, officers, employees, representatives, agents, consultants, and associates of financial institutions are exempt from civil or criminal prosecution for reporting covered transactions. These institutions must maintain and store records of transactions for a period of five years, extending beyond the date of account or bank closure. The AMLC has frozen funds at the request of the UN Security Council, the United States and other foreign governments. Through November 2005, the AMLC has frozen funds in excess of 500 million Philippine pesos ($ approximately $9,700,000).

Questions remain regarding the covered institutions fully complying with the Philippine anti-money laundering regime. For example, the BSP does not have a mechanism in place to ensure that the financial community is adhering to the reporting requirements. Banks in more distant parts of the country, especially Mindinao where terrorist groups operate more freely, may feel threatened and inhibited from providing information about financial transactions requested by AMLC. While bank secrecy provisions to the BSP's supervisory functions were lifted in Section 11 of the AMLA, implementation still appears to be incomplete. Due to the Philippines' "privacy issues," examiners of the BSP are not allowed to review documents held by covered institutions in order to determine if the covered institutions are complying with the reporting requirement. BSP examiners are only allowed to ask AMLC, as a result of their examination, if a STR has been filed. If AMLC determines one was not

filed, then the AMLC has the responsibility to make inquiries of the covered institution. This process is slow and cumbersome; AMLC is working with the BSP to find ways of streamlining the process.

An important development in 2005 was the AMLC's effectiveness in including foreign exchange offices as covered institutions subject to the money laundering provisions. The Monetary Board issued a decision in February 2005 defining the 15,000 exchange houses as financial institutions and instituting a new licensing system to bring them under the provisions of the AMLA. Under this decision, all exchange dealers were to have received training from the AMLC by July 2005 to obtain licenses and ensure compliance with the Act. With so many dealers and with continued misunderstanding of the new regulations, only 2,500 exchange dealers were trained and registered by the end of July. Training teams from the AMLC have held over 1,000 classes for dealers and bankers throughout the country to implement this decision. By the end of November, an estimated half of the foreign exchange offices still in operation have received the mandatory training and have been registered. This requirement reduced the number of foreign exchange dealers dramatically; as less reputable offices chose to close down rather than seek licensing.

There are still several sectors operating outside of AMLC control, under the revised AMLA. Although the revised AMLA specifically covers exchange houses, insurance companies, and casinos, it does not cover stockbrokers or accountants. Although covered transactions for which AMLC solicits reports include asset transfers, the law does not require direct oversight of car dealers and sales of construction equipment, which are emerging as creative ways to launder money and avoid the reporting requirement. The AMLC has the authority to request the chain of casinos operated by the state-owned Philippine Amusement and Gaming Corporation (PAGCOR) to submit covered and suspicious transaction reports, but it has not yet done so.

There is increasing recognition that the nearly 20 casinos nationwide offer abundant opportunity for money laundering, especially with many of these casinos catering to international clientele arriving on charter flights from around Asia. Several of these gambling facilities are located near small provincial international airports that may have less rigid enforcement procedures and standards for cash smuggling. PAGCOR is the sole franchisee in the country for all games of chance, including lotteries conducted through cell phones. At present, there are no offshore casinos or Internet gaming sites.

The Philippines has over 5,000 non-governmental organizations (NGOs) that do not fall under the requirements of the AMLA. Charitable and non-profit entities are not required to make covered or suspicious transaction reports. The SEC provides limited regulatory control over the registration and operation of NGOs. These entities are rarely held accountable for failure to provide year-end reports of their activities, and there is no consistent accounting and verification of their financial records. Because of their ability to circumvent the usual documentation and reporting requirements imposed on banks for financial transfers, NGOs could be used as conduits for terrorist financing without detection. The AMLC is aware of the problem and is working to bring charitable and not-for-profit entities under the interpretation of the amended implementing regulations for covered institutions.

There are nine offshore banking units (OBUs) established since 1976. At present, OBUs account for less than two percent of total banking system assets in the country. The Bangko Sentral ng Pilipinas (BSP) regulates onshore banking, exercises regulatory supervision over OBUs, and requires them to meet reporting provisions and other banking rules and regulations. In addition to registering with the SEC, financial institutions must obtain a secondary license from the BSP subject to relatively stringent standards that would make it difficult to establish shell companies in financial services of this nature. For example, a financial institution operating an OBU must be physically present in the Philippines. Anonymous directors and trustees are not allowed. The SEC does not permit the issuance of bearer shares for banks and other companies.

Despite the efforts of the GORP authorities to publicize regulations and enforce penalties, cash smuggling remains a major concern for the Philippines. Although there is no limit on the amount of

foreign currency an individual or entity can bring into or take out of the country, any amount in excess of $10,000 equivalent must be declared upon arrival or departure. Based on the amount of foreign currency exchanged and expended, there is systematic abuse of the currency declaration requirements and a large amount of unreported cash entering the Philippines.

The problem of cash smuggling is exacerbated by the large volume of foreign currency remitted to the Philippines by Overseas Filipino Workers (OFWs). The amount of remitted funds grew by 25 percent during the first ten months of 2005, and should exceed $10 billion for the year, equal to 11 percent of GDP. The BSP estimates that an additional $2-3 billion is remitted outside the formal banking system. Most of these funds are brought in person by OFWs or by designated individuals on their return home and not through any alternative remittance system. Since most of these funds enter the country in smaller quantities than $10,000, there is no declaration requirement and the amounts are difficult to calculate. The GORP encourages local banks to set up offices in remitting countries and facilitate fund remittances, especially in the United States, to help reduce the expense of remitting funds.

The Philippines is a member of the Asia/Pacific Group on Money Laundering and became the 101st member of the Egmont Group of FIUs in July 2005. The GORP is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime (2002) and to all 12 international conventions and protocols related to terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism (2004). The Anti-Money Laundering Council is able to freeze funds and transactions identified with or traced to suspected terrorists and terrorist organizations listed on the UN 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 other foreign governments.

For several years, the GORP has realized the need to enact and implement an antiterrorism law that among other things would define and criminalize terrorism and terrorist financing, and give military and law enforcement entities greater tools to detect and interdict terrorist activity. President Arroyo declared in her State of the Nation address in June 2005 that the passage of such a law was one of her priorities for the remainder of the year. The Philippines legislature took steps to achieve that result in fall 2005 in consolidating bills and bringing them to the floor for full consideration. The Senate tabled its version of an antiterrorism bill (SB 2137) in October and the house calendared its own Bill (HV 4839) in November. The Senate and house held hearings in late 2005; the bill passed its second reading in the house in December with the third and final reading expected in mid-January 2006.

Reportedly, the GORP remains optimistic that both houses will pass a comprehensive law addressing terrorism in 2006. In lieu of specific counterterrorist legislation, the government has broadly criminalized terrorist financing through Republic Law legislation, which defines "hijacking and other violations under Republic Act No. 6235; destructive arson and murder, as defined under the Revised Penal Code, as amended, included those perpetrated by terrorists against non-combatant persons and similar targets" as one of the violations under the definition of unlawful acts. The Revised Implementing Rules and Regulations R.A. No. 9160, as amended by R.A. No.9194, further state that any proceeds derived or realized from an unlawful activity includes all material and monetary effects will be deemed a violation against the law.

The Government of the Republic of the Philippines has made significant progress enhancing and implementing its amended anti-money laundering regime. To fully comport with international standards and become a more effective partner in the global effort to staunch money laundering and thwart terrorism and its financing, it should enact and implement new legislation that criminalizes terrorism and terrorist financing. Additionally, the Central Bank should be empowered to levy administrative penalties against covered entities in the financial community that do not comply with reporting requirements. Stockbrokers and accountants should be required to report CTRS and STRs and AMLC should use its authority to require all casinos to file CTRs and STRs. The GORP should

enact comprehensive legislation regarding freezing and forfeiture of assets that would empower AMLC to issue administrative freezing orders to avoid funds being withdrawn before a court order is issued. The creation of an asset forfeiture fund would enable law enforcement agencies to draw on the fund to augment their budgets for investigative purposes. Such a fund would benefit the AMLC and enable it to purchase needed equipment. Finally, AMLC should consider clearly separating its analytical and investigative responsibilities and establish a separate investigative division that would focus its attention on dismantling money laundering and terrorist financing operations.

Poland

Poland's geographic location places it directly along one of the main routes between the former Soviet Union republics and Western Europe that is used by narcotics traffickers and organized crime groups. According to Polish Government estimates, narcotics trafficking, organized crime activity, auto theft, smuggling, extortion, counterfeiting, burglary, and other crimes generate criminal proceeds in the range of $2-3 billion yearly. The Government of Poland (GOP) estimates that the unregistered or gray economy, used primarily for tax evasion, may be as high as 15 percent of Poland's $280 billion GDP; it believes the black economy is only one percent of GDP. Poland's entry into the European Union (EU) in May 2004 increased its ability to control its eastern borders, thereby allowing Poland to become more effective in its efforts to combat all types of crime, including narcotics trafficking and organized crime.

Poland's banks serve as transit points for the transfer of criminal proceeds. As of December 2004, 55 commercial banks were licensed for operation in Poland, as were slightly less than 590 "cooperative banks" that serve the rural and agricultural community. The GOP considers the nation's banks, insurance companies, and brokerage houses to be important venues of money laundering. Polish casinos may likewise be sites for money laundering activity. According to the GOP, fuel smuggling, by which local companies and organized crime groups seek to avoid excise taxes by forging gasoline delivery documents, is a major source of proceeds to be laundered. It is also believed that some money laundering in Poland derives from Russia or other countries of the former Soviet Union.

The Criminal Code criminalizes money laundering. Article 299 of the Criminal Code addresses self-laundering and criminalizes tipping off. In June 2001, the parliament passed amendments that broadened the definition of money laundering to encompass all serious crimes ("Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources," known as the "Act of 16 November"). In March 2003, Parliament further amended the law to broaden the definition of money laundering to include assets originating from illegal or undisclosed sources.

Poland has adopted a National Security Strategy that treats the anti-money laundering effort as a top priority. The GOP has worked diligently to bring its laws into full conformity with EU obligations. On November 16, 2000, a law went into effect that improves Poland's ability to combat money laundering (entitled the November 2000 Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources). The GOP has updated this law several times to bring it into conformity with EU standards and to improve its operational effectiveness. This law increases penalties for money laundering and contains safe harbor provisions that exempt financial institution employees from normal restrictions on the disclosure of confidential banking information. The law also provides for the creation of a financial intelligence unit (FIU), the General Inspectorate of Financial Information (GIIF), housed within the Ministry of Finance, to collect and analyze large and suspicious transactions.

A major weakness of Poland's initial money laundering regime was that it did not cover many non-bank financial institutions that had traditionally been used for money laundering. To remedy this situation, between 2002 and 2004 the Parliament passed several amendments to the 2000 money

laundering law. The amendments expand the scope of institutions subject to identity verification, record keeping, and suspicious transaction reporting requirements. Financial institutions subject to the reporting requirements prior to March 2004 amendments included banks, the National Depository for Securities, post offices, auction houses, antique shops, brokerages, casinos, insurance companies, investment and pension funds, leasing firms, private currency exchange offices, real estate agencies, and notaries public. The March 2004 amendments to the money laundering law widen the scope of covered institutions to include lawyers, legal counselors, auditors, and charities, as well as the National Bank of Poland in its functions of selling numismatic items, purchasing gold, and exchanging damaged banknotes. The law also requires casinos to report the purchase of chips worth 1,000 euros or more. The law's extension to the legal profession was not without controversy. Lawyers strongly opposed the new amendments, claiming that the law violates attorney-client confidentiality privileges.

In 2002, Parliament adopted measures to bring the nation's anti-money laundering legislation into compliance with EU standards regarding the reporting threshold, and also amended Poland's customs law to require the reporting of any cross-border movement of more than 10,000 euros in currency or financial instruments. In addition to requiring that the GIIF be notified of all financial deals exceeding 15,000 euros, covered institutions are also required to file reports of suspicious transactions, regardless of the size of the transaction. Polish law also requires financial institutions to put internal anti-money laundering procedures into effect, a process that is overseen by the GIIF.

The GIIF began operations on January 1, 2001. In its first year of existence, the GIIF received over 350 suspicious transaction reports (STRs). In 2002, the GIIF received 614 STRs, from which prosecutors prepared 70 cases. In 2003, the GIIF received 965 STRs, resulting in the development of 152 cases by the Prosecutor's Office. In 2004, the GIIF received 1,397 STRs, which resulted in the development of 148 cases by the Prosecutor's Office. Between January and October 2005, the GIIF received 1,425 STRs, resulting in the creation of 169 cases. Banks filed eighty percent of the STRs submitted in 2004. At a minimum, all reports submitted by the GIIF to the Prosecutor's Office have resulted in the instigation of initial investigative proceedings. Although there were only four convictions under the money laundering law in 2004 (this figure is twice the number from 2003), many of the investigations begun by the GIIF have resulted in convictions for other non-financial offenses. As of October 2005, the GIIF received 26.1 million reports on transactions exceeding the threshold level. The GIIF receives approximately 1.8 million reports per month.

The vast majority of required notifications to the GIIF are sent through a newly developed electronic reporting system, which is Europe's most technically sophisticated and collects more complete information than the previously required report regarding the transaction in question (e.g., how payment was made-cash or credit, where and when). Only a small percentage of notifications are now submitted by paper, mainly from small institutions that lack the equipment to use the electronic system. Although the new system is an important advance for Poland's anti-money laundering program, the processing and analyzing of the large number of reports that are sent to the GIIF will prove to be a challenge for the understaffed FIU. To help improve the FIU's efficiency in handling the large volume of reports filed by obliged institutions, the GIIF plans to install new analytical software that will permit advanced and detailed analysis of financial information.

The GIIF also does on-site training and compliance monitoring investigations. In 2005, the GIIF carried out 195 compliance investigations as compared to 15 in 2004, and received several hundred follow-up reports from institutions responsible for routinely supervising covered institutions. In January 2004, the GIIF introduced a new electronic learning course designed to familiarize obliged institutions with Poland's anti-money laundering regulations. In March 2005, an updated version of the course was installed on the Ministry of Finance Website.

The Polish Code of Criminal Procedure, Article 237, allows for certain Special Investigative Measures. However, money laundering investigations are not specifically covered, although the

organized crime provisions might apply in some cases. Two main police units deal with the detection and prevention of money laundering: the General Investigative Bureau and the Unit for Combating Financial Crime. Overall, both police units cooperate well with the GIIF. The Internal Security Agency (ABW) may also investigate the most serious money laundering cases.

A recognized need exists for an improved level of coordination and information exchange between the GIIF and law enforcement entities, especially with regard to the suspicious transaction information that the GIIF forwards to the National Prosecutor's Office. To alleviate this problem the GIIF and the National Prosecutor's Office signed a cooperation agreement in 2004. The agreement calls for the creation of a computer-based system that would facilitate information exchange between the two institutions. Work on the development of this new system is currently underway. With regard to information exchange with its foreign counterparts, the GIIF remains active. In 2004, it sent official requests to foreign financial intelligence units on 102 cases concerning 224 national and foreign entities suspected of money laundering, while foreign FIUs sent 51 requests to the GIIF, concerning 163 national and foreign entities suspected of attempting to legalize proceeds from crime.

The GIIF is authorized to put a suspicious transaction on hold for 48 hours. The Public Prosecutor then has the right to suspend the transaction for an additional three months, pending a court decision. In 2004, Article 45 of the criminal code was amended to further improve the government's ability to seize assets. On the basis of the amended article, an alleged perpetrator must prove that his assets have a legal source; otherwise, the assets are presumed to be related to the crime and as such can be seized. Both the Ministry of Justice and the GIIF desire to see more aggressive asset forfeiture regulations. However, because the former communist regime employed harsh asset forfeiture techniques against political opponents, lingering political sensitivities make it difficult to approve stringent asset seizure laws. In 2003, the GIIF suspended 20 transactions worth 9 million euros and blocked nine accounts worth 5.2 million euros. During the first 11 months of 2004, the GIIF suspended five transactions worth 650,000 euros and blocked 12 accounts worth 2.1 million euros.

The GOP recently created an office of counterterrorist operations within the National Police. The office coordinates and supervises regional counterterrorism units and trains local police in counterterrorism measures. Poland has also created a terrorist watch list of entities suspected of involvement in terrorist financing. The list contains the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the names of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224, and the names designated by the EU under its relevant authorities. All covered institutions are required to verify that their customers are not included on the watch list. In the event that a covered institution discovers a possible terrorist link, the GIIF has the right to suspend suspicious transactions and accounts. Despite these efforts, Poland has not yet criminalized terrorist financing, arguing that all possible terrorist activities are already illegal and serve as predicate offenses for money laundering and terrorist financing investigations. The Ministry of Justice has completed draft amendments to the criminal code that would criminalize terrorist financing as well as elements of all terrorism-related activity. The amendments have been presented to the Minister of Justice, but have not yet been approved by Parliament.

As a member of the Council of Europe, Poland participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). It has undergone first and second round mutual evaluations by that group and is scheduled for a third in 2006. The GIIF is an active participant in the Egmont Group and in FIU.NET, the EU-sponsored information exchange network for FIUs. All information exchanged between the GIIF and its counterparts in other EU states takes place via FIU.NET.

A Mutual Legal Assistance Treaty between the United States and Poland came into force in 1999. In addition, Poland has signed bilateral mutual legal assistance treaties with Sweden, Finland, Ukraine,

Lithuania, Latvia, Estonia, Germany, Greece, and Hungary. Polish law requires the GIIF to have memoranda of understanding (MOUs) with other international competent authorities before it can participate in information exchanges. The GIIF has been diligent in executing MOUs with its counterparts in other countries, signing a total of 27 MOUs between 2002 and 2004. The GIIF-FinCEN MOU was signed in fall 2003. An additional six memoranda on exchange of financial information with Guernsey, Chile, Croatia, Indonesia, Macedonia, and Switzerland were signed in 2005. Because Poland is an EU member state, the exchange of information between the GIIF and the FIUs of other member states is regulated by the EU Council Decision of October 17, 2000.

Poland is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the European Convention on Extradition and its Protocols, the European Convention on Mutual Assistance in Criminal Matters, and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. In November 2001, Poland ratified the UN Convention against Transnational Organized Crime, which was, in part, a Polish initiative.

Over the past several years, the Government of Poland has worked diligently to implement a comprehensive anti-money laundering regime that meets international standards. Further improvements could be made by promoting additional training at the private sector level and by working to improve communication and coordination between the General Inspectorate of Financial Information and relevant law enforcement agencies. The Code of Criminal Procedure should also be amended to allow the use of Special Investigative Measures in money laundering investigations, which would help law enforcement attain a better record of prosecutions and convictions. Poland should also act on the draft amendments to the criminal code and specifically criminalize terrorist financing.

Portugal

Portugal is an entry point for narcotics transiting into Europe, and officials of the Government of Portugal (GOP) indicate that most of the money laundered in Portugal is narcotics-related. The GOP also reports that currency exchanges, wire transfers, and real estate purchases are used for laundering criminal proceeds.

Portugal has a comprehensive anti-money laundering regime that criminalizes the laundering of proceeds of serious offenses, including terrorism, arms trafficking, kidnapping, and corruption. Financial and non-financial institutions have a mandatory requirement of reporting all suspicious transactions to the Public Prosecutor regardless of threshold amount.

Money laundering is specifically defined in Penal Code Article 368-A. Act 11/2004 of 27 March, which implements the European Union's Second Money Laundering Directive, defines the legal framework for the prevention and repression of money laundering. Act 11/2004 mandates suspicious transaction reporting by credit institutions, investment companies, life insurance companies, traders in high-value goods (e.g., precious stones, aircraft), and numerous other entities. "Tipping off" is prohibited and liability protection is provided for regulated entities making disclosures in good faith. If a regulated entity has knowledge of a transaction likely to be related to a money laundering offense, it must inform the Portuguese Government. The GOP may order the entity not to complete the transaction. If stopping the transaction is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, the government also may allow the entity to proceed with the transaction but require the entity to provide it with complete details. All financial institutions, including insurance companies, must identify their customers, maintain records for a minimum of ten years, and demand written proof from customers regarding the origin and beneficiary of transactions that exceed 12,500 euros. Non-financial institutions, such as casinos, property dealers, lotteries and dealers in high-value assets, must also identify customers engaging in large transactions, maintain records, and report suspicious activities to the Office of the Public Prosecutor. Until March

2004, banking secrecy laws made it extremely difficult for investigators to obtain information about bank accounts and financial transactions of individuals or companies without their permission.

Decree-Law 295/2003 of November 21, 2003, sets out reporting requirements for the transportation across borders of cash, non-manufactured gold, and certain negotiable financial instruments, e.g., travelers' checks. When a person travels across the Portuguese border with more than 12,500 euros (U.S. $14,730) worth of such assets, a declaration must be made to Portuguese customs officials. A new EU regulation on cross-border currency reporting (EC 1889/2005), issued in November 2005, also must be implemented in Portugal.

The November 2003 law also revised and tightened the legal framework for foreign currency exchange transactions, including gold, subjecting them to the reporting requirement for transactions exceeding 12,500 euros. Beyond the requirements to report large transactions, foreign exchange bureaus are not subject to any special requirements to report suspicious transactions. The law does, however, give the GOP the authority to investigate suspicious transactions without notifying targets of the investigation.

New rules that took effect in January 2005 permit tax authorities to lift secrecy rules without authorization from the target of an investigation. The rules require companies to have at least one bank account and, for companies with more than 20 employees, to conduct their business through bank transfers, checks, and direct debits rather than cash. These rules are mainly designed to help the GOP investigate possible cases of tax evasion but may ease enforcement of other financial crimes as well.

With regard to non-banking financial institutions, namely financial intermediaries, the Portuguese Securities Market Commission set forth Regulation 7/2005 (amending Regulation 12/2000 on Financial Intermediation) requiring financial intermediaries to submit detailed annual Control and Supervision Reports to the Commission by 30 June the following year. The regulation is due to enter into force on January 1, 2006.

The three principle regulatory agencies for supervision of the financial sector in Portugal are the Central Bank of Portugal, the Portuguese Insurance Institute, and the Portuguese Securities Market Commission. The Gambling Inspectorate General, the Economic Activities Inspectorate General, the Registries and Notaries General Directorate, the National Association for Certified Public Accountants and the Association for Assistant Accountants, the Bar Association, and the Chamber of Solicitors also monitor and enforce the reporting requirements of the obliged entities.

Portugal's financial intelligence unit (FIU), known as the Financial Information Unit, or Unidade de Informação Financeira (UIF), was established through Decree-Law 304/2002 of December 13, 2002, and is operates independently as a department of the Portuguese Judicial Police (Polícia Judiciária). At the national level, UIF is responsible for gathering, centralizing, processing, and publishing information pertaining to investigations of money laundering and tax crimes. It also facilitates cooperation and coordination with other judicial and supervising authorities. At the international level, UIF coordinates with other FIUs. UIF has policing duties but no regulatory authority.

From January to September 2005, UIF received well over 40,000 reports of suspicious transactions. Portugal's General Directorate for Games was the source of 89 percent of the total number of reports, as it reports all transactions at casinos above a certain threshold. Banks submitted 237 suspicious transaction reports, and Portugal's Central Bank submitted an additional 98 reports. In this same time period, UIF sent 131 cases for further investigation to the Judicial Police and other police departments. Most of the case information originated from financial institutions and the Central Bank. Four cases resulted in proposals to suspend banking operations involving a total of approximately 3.25 million euros (U.S. $3.8 million).

Portuguese laws provide for the confiscation of property and assets connected to money laundering, and authorize the Judicial Police to trace illicitly obtained assets (including those passing through

casinos and lotteries), even if the predicate crime is committed outside of Portugal. Police may request files of individuals under investigation and, with a court order, can obtain and use audio and videotape as evidence in court. The law allows the Public Prosecutor to request that a lien be placed on the assets of individuals being prosecuted, in order to facilitate asset seizures related to narcotics and weapons trafficking, terrorism, and money laundering.

Act 5/2002 shifted the burden of proof in cases of criminal asset forfeiture from the government to the defendant; an individual must prove that his assets were not obtained as a result of his illegal activities. The law defines criminal assets as those owned by an individual at the time of indictment and thereafter. The law also presumes that assets transferred by an individual to a third party within the previous five years still belong to the individual in question, unless proven otherwise. GOP law enforcement agencies seized a total of 2.4 million euros in cash and accounts in 2003 and 5.1 million euros in 2004 in association with drug and money laundering investigations. Portugal has comprehensive legal procedures that enable it to cooperate with foreign jurisdictions and share seized assets.

In August 2003, Portugal passed Act 52/2003, which specifically defines terrorist acts and organizations and criminalizes the transfer of funds related to the commission of terrorist acts. Portugal has created a Terrorist Financing Task Force that includes the Ministries of Finance and Justice, the Judicial Police, the Security and Intelligence Service, the Bank of Portugal, and the Portuguese Insurance Institution. Portugal has applied all of the Financial Action task Force (FATF) Special Recommendations on Terrorist Financing. Names of individuals and entities included on the UNSCR 1267 Committee's consolidated list, or that the United States and EU have linked to terrorism, are passed to private sector organizations through the Bank of Portugal, the Stock Exchange Commission, and the Portuguese Insurance Institution. In practice, the actual seizure of assets would only occur once the EU's clearinghouse process agrees to the EU-wide seizure of assets of terrorists and terrorist-linked groups. Portugal is actively cooperating in the search and identification of assets used for terrorist financing. To date, no significant assets have been identified or seized.

The Portuguese Madeira Islands International Business Center (MIBC) has a free trade zone, an international shipping register, offshore banking, trusts, holding companies, stock corporations, and private limited companies. The latter two business groups, of which there are approximately 6,500 companies registered in Madeira, are similar to international business corporations. All entities established in the MIBC will remain tax exempt until 2011. Twenty-seven offshore banks are currently licensed to operate within the MIBC. The Madeira Development Company supervises offshore banks.

Companies can also take advantage of Portugal's double taxation agreements. Decree-Law 10/94 permits existing banks and insurance companies to establish offshore branches. Applications are submitted to the Central Bank of Portugal for notification, in the case of EU institutions, or authorization, in the case of non-EU or new entities. The law allows establishment of "external branches" that conduct operations exclusively with nonresidents or other Madeiran offshore entities, and "international branches" that conduct both offshore and domestic business. Although Madeira has some local autonomy, Portuguese and EU legislative rules regulate its offshore sector, and the competent oversight authorities supervise it. Exchange of information agreements contained in double taxation treaties allow for the disclosure of information relating to narcotics or weapons trafficking. Bearer shares are not permitted.

Portugal is a member of the Council of Europe, the European Union, and the FATF. Portugal is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Portugal is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and became a party to the UN International Convention for

the Suppression of the Financing of Terrorism on October 18, 2002. The Money Laundering Investigation Unit of Portugal's Judicial Police is a member of the Egmont Group.

The Government of Portugal has put into place a comprehensive and effective regime to combat money laundering. Laws passed in 2002 strengthen its ability to investigate and prosecute; steps taken in 2003 extended the regime's reach to terrorist financing; and legislative measures adopted in 2004 have consolidated the anti-money laundering legal framework, imposing on financial and non-financial institutions obligations to prevent and repress the use of the financial system for the purpose of money laundering.

Qatar

Qatar has a relatively small population (approximately 850,000 residents), with a low rate of general and financial crime. The financial sector, though modern, is limited in size and subject to strict regulation by the Qatar Central Bank (QCB). There are 15 licensed banks, including two Islamic banks and a Qatar Industrial Development Bank. Qatar has 19 exchange houses, three investment companies and one commercial finance company. Although Qatar is a cash-intensive economy, cash placement by money launderers is believed by authorities to be a negligible risk due to the close-knit nature of the society in Qatar and the rigorous "know your customer" procedures required by Qatari law.

On September 11, 2002, the Emir of the State of Qatar signed the Anti-Money Laundering Law. According to Article 28 of the law, money laundering offenses involve the acquisition, holding, disposing of, managing, keeping, exchanging, depositing, investing, transferring, or converting of funds from illegal proceeds. The law imposes penalties of imprisonment of five to seven years, in addition to fines. The law expanded the powers of confiscation of proceeds gained from the commission of a crime, and instrumentalities used to commit a crime, to include the identification and freezing of assets as well as the ultimate confiscation of the illegal proceeds upon conviction of the defendant for money laundering.

The law requires all financial institutions to report suspicious transactions to the QCB and retain records for up to 15 years. The law also gives the QCB greater powers to inspect suspicious bank accounts, and grants the authorities the right to confiscate money in illegal transactions. Article 17 permits Qatar to extradite convicted criminals in accordance with international or bilateral treaties.

The Anti-Money Laundering Law established the National Anti-Money Laundering Committee (NAMLC) to oversee and coordinate money laundering combating efforts. It is chaired by the Deputy Governor of the Qatar Central Bank, in addition to ten other members from the Ministries of Interior, Civil Service Affairs and Housing, Economy and Commerce, Finance, Justice, QCB, Customs and Ports Authority, and the State Security Bureau.

In February 2004, the Government of Qatar passed the Combating Terrorism Law. According to Article Four of the law, any individual or entity that provides financial or logistical support, or raises money for activities considered terrorist crimes, is subject to punishment. The punishments are listed in Article Two of the law, which include the death penalty, life imprisonment, and 10 or 15 year jail sentences, depending on the nature of the crime.

The Qatari Financial Intelligence Unit (FIU) was established in October 2004. The FIU is responsible for reviewing all financial transaction reports, identifying suspicious transactions and financial activities of concern, ensuring that all government ministries and agencies have procedures and standards to ensure proper oversight of financial transactions, and recommending actions to be taken by the NAMLC if suspicious transactions or financial activities of concern are identified. The FIU is coordinating closely with the Doha Securities Market (DSM) to establish procedures and standards to monitor all financial activities that occur in Qatar's stock market. In November 2004, the FIU

established monitoring standards in coordination with the National Post Office to ensure that post offices throughout the country monitor carefully all cash transfers. The FIU is also taking steps to monitor financial activities that take place in the Ministry of Justice's Registration Department and Qatar's camel market. Qatar's FIU became a full member of the Egmont Group in June 2005.

In addition to reporting suspicious transactions, all financial institutions (including businesses conducting hawala transactions) must report transactions of Qatari riyals (QR) 100,000 (approximately $33,000) or above to the QCB. Any repeated cash transactions of QR 30,000 (approximately $10,000) or higher made by an individual or entity must be reported. Any transaction of QR 100,000 or higher and repeated transactions of QR 30,000 or higher will be investigated by the FIU in coordination with the Ministries of Justice and Interior. Exchange houses must report any transaction of QR 40,000 (approximately $13,330) or higher. All financial institutions also must identify the person entering into a business relationship or conducting a transaction. In December 2004, QCB installed a central reporting system to assist the FIU in monitoring all financial transactions made by banks.

Only Qatari citizens, legal foreign residents, and citizens of other Gulf Cooperation Council (GCC) states are permitted to open bank accounts. All accounts must be opened in person. In January 2002, QCB issued Circular Number 9 regarding the Combat of Money Laundering and Financing of Terrorism. This circular was designed to increase the awareness of all banks operating in Qatar with respect to anti-money laundering and counterterrorist financing, by explaining money laundering and terrorist finance schemes and monitoring suspicious activities.

In addition to Circular Number 9, Qatar has taken other steps to combat the financing of terrorism, including requiring banks to freeze the assets of suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list. In 2002, the GOQ established a national committee to review the UN 1267 Sanctions Committee's consolidated list and recommend any necessary actions against individuals or entities found in Qatar. On August 24, 2003, the Anti-Money Laundering law was amended (Amendment 21/2003) and published in the official gazette. Amendment 21 revised three articles in the anti-money laundering law. Article 2 was amended to broaden the definition for money laundering to include any activities related to terrorist financing. Article 8 added the customs and ports authority to the NAMLC. Article 12 authorized the Central Bank governor to freeze suspicious accounts up to ten days and to inform the attorney general within three days of any action taken. The Attorney General may renew or nullify the freeze order for a period of up to three months. After this process, a freeze order may not be renewed unless authorized by court order.

The QCB, Public Prosecutor, and the Criminal Investigation Division (CID) of the Ministry of Interior are the principal entities that have responsibility for investigating and prosecuting money laundering cases. The FIU receives all suspicious transaction reports and conducts an initial analysis. The FIU also obtains additional information from the banks and other government ministries before determining whether to forward the suspicious transaction report to the Ministry of Interior. The Public Prosecutor and CID work closely on all criminal cases, although in financial cases they often seek the assistance of the QCB. There are no specialized units within the Public Prosecutor or CID's offices that initiate or investigate financial crimes.

On January 12, 2005, the Government of Qatar announced plans for the establishment of the Qatar Financial Centre (QFC), an international financial center to lure major international financial institutions and corporations to set up their offices in the country. The center began operating on May 1, 2005. The QFC is a totally independent body, managed by the QFC authority. The authority oversees business conduct and grants licenses to operate in the center. All companies setting up their offices at QFC are entitled to a three-year tax exemption, full repatriation of profits and 100 percent foreign ownership. At the end of three years they will be subject to a relatively low tax rate on profits.

In March 2004, the Government of Qatar passed a law to establish the Qatar Authority for Charitable Works, which monitors all charitable activity in and outside of Qatar. This law incorporates the

Charitable Societies Law (Law No. 8/1998), which details the monitoring and supervision of Qatar's charities. The Secretary General of the Authority approves all international fund transfers by the charities. The Authority has primary responsibility for monitoring overseas charitable, development, and humanitarian projects that were previously under the oversight of several government agencies such as the Ministry of Foreign Affairs, the Ministry of Finance and the Ministry of Economy and Commerce. Overseas activities must be undertaken in collaboration with a non-governmental organization (NGO) that is legally registered in the receiving country. The Authority prepares an annual report on the status of all projects and submits the report to relevant ministries. The Authority is in the process of developing concrete measures to exert more control over domestic charity collection.

Article 37 of Law Number 8 of 1998, concerning the establishment and governance of private associations and institutions, stipulates that the Ministry of Awqaf (Endowments) and Islamic Affairs shall oversee and monitor all the activities of private institutions within the boundaries that are regulated by executive provisions. The Ministry may examine the institution's books, records, and documents that are related to its activities and it may amend its bylaws. The institution shall provide the Ministry with any information, documents, or other data it requests. According to Article 1 of Law 15 of 1993, banks with offshore business shall be formed either as joint stock companies having their head offices in the State of Qatar or as branches of Qatari or foreign banks.

Qatar does not yet have any cross-border reporting requirements for financial transactions. Immigration and customs authorities are reviewing this policy and are increasingly interested in expanding their ability to detect trade-based money laundering. The Government of Qatar has established a subcommittee under the NAMLC to implement cross-border reporting requirements. The subcommittee is composed of the QCB, Customs Authority, FIU, and members of the NAMLC.

Qatar is a party to the 1988 UN Drug Convention but not the UN Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime. Qatar is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body that promotes best practices to combat money laundering and terrorist financing in the region that was established in November 2004.

Qatar has demonstrated a willingness to fight financial crimes, including terrorist financing, and to work cooperatively with other countries in doing so. Implementation and enforcement of the new law and regulations are essential to the success of Qatar's efforts. Qatar should continue to work to ensure that law enforcement, prosecutors, and customs authorities receive the necessary training to improve their capabilities in recognizing and pursuing various forms of terrorist financing, money laundering and other financial crimes. Qatar should institute cross-border cash reporting requirements. Qatar 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.

Romania

Romania's geographic location makes it a natural transit country for trafficking in narcotics, arms, stolen vehicles, and persons. As such, the nation is vulnerable to financial crimes. Romania's National Bank estimates the dollar amount of financial crimes to range from $1 billion to $1.5 billion per year. Tax evasion and value-added tax (VAT) fraud constitute approximately 45 percent ($500-$600 million per year) of this total. Financial sector fraud, fraudulent bankruptcy claims, and smuggling of illicit goods are additional types of financial crimes prevalent in the country. Romania also has one of the highest occurrences of online credit card fraud in the world.

Laundered money comes primarily from domestic criminal activity carried out by international crime syndicates, which often launder money through limited liability companies set up for this purpose. The

U.S. dollar is the preferred currency. Endemic corruption in Romania and its neighboring countries abets money laundering. The proceeds from the smuggling of cigarettes, alcohol, coffee, and other dutiable commodities are also laundered in Romania. From Romania, most of the laundered funds go to offshore financial shelters in the Caribbean.

Romania first criminalized money laundering with the adoption in January 1999 of Law No. 21/99, On the Prevention and Punishment of Money Laundering. The law became effective in April 1999 and required customer identification, record keeping, reporting transactions of a suspicious or unusual nature, and currency transaction reporting for transactions over 10,000 euros.

The law also established a financial intelligence unit (FIU), known as the National Office for the Prevention and Control of Money Laundering (NOPCML), and mandated that the NOPCML oversee the implementation of internal anti-money laundering procedures and training for all domestic financial institutions covered by the law. The list of entities subjected to money laundering controls included banks, non-bank financial institutions, attorneys, accountants, and notaries. However, in practice, the controls on non-bank financial institutions have not been as rigorous as those imposed on banks.

In December 2002, the Law on the Prevention and Sanctioning of Money Laundering (Law 656/2002) went into effect, changing the list of predicate offenses to the all-crimes approach. Every cash operation and every external wire transfer involving a sum exceeding 10,000 euros must be reported to the NOPCML and be monitored. NOPCML is authorized to participate in inspections and controls in conjunction with supervisory authorities.

In addition, the new law expands the number and types of entities required to report to the NOPCML. Some of these new entities include art dealers, travel agents, privatization agents, postal officials, money transferors, and real estate agents. Training for these entities is necessary to ensure compliance with reporting, record keeping, recognition of suspicious transactions, and development of internal controls. The new law also provides for both suspicious transaction reports (STRs) and currency transaction reports (CTRs) to be forwarded to the NOPCML, with the CTR amounts conforming to European Union (EU) standards.

In keeping with new international standards, the National Bank of Romania (BNR) introduced Norm No. 3, Know Your Customer, in December 2003, to strengthen information disclosure for external wire transfers and correspondent banking. When sending out wire transfers, banks must include information about the originator's name, address, and account. The same information is required for incoming wires as well. Banks are further required to undertake proper due diligence before entering into international correspondent relations, and are prohibited from opening correspondent accounts with shell banks. The BNR is currently working on a project to strengthen its anti-money laundering (AML) and counterterrorist financing (CTF) regulations through the introduction of improved bank examination procedures. Plans are also underway to replicate the project in the insurance industry. In 2005, the Insurance Supervision Commission has instituted similar regulations for the insurance industry

The know-your-customer identification requirements have also been honed, so that identification of the client becomes necessary upon account opening and when single or multiple transactions meet or approach 10,000 euros. In accordance with a new national strategy on money laundering, lawyers are now obligated to report to the NOPCML. In addition, and in line with the Second EU Directive, tipping off has been prohibited. Romanian law permits the disclosure of client and ownership information to bank supervisors and law enforcement authorities, and protects banking officials with respect to their cooperation with law enforcement.

During the first ten months of 2005, the number of files sent to the General Prosecutor's Office on suspicion of money laundering reached 411, compared to 501 in 2004. The number of files sent to the

National Anti-Corruption Department on suspicion of money laundering connected with corruption reached 41 notifications in the first ten months of 2005, compared to 22 in 2004. The approximate amount associated with the above cases was $349.1 million during the first ten months of 2005, compared to $594.9 million in 2004. The number of files sent to the General Prosecutor's Office for suspicion of money laundering connected to terrorism financing was three in the first ten months of 2005, involving approximately $3.3 million, compared to one case involving $3.1 million in 2004. According to NOPCML estimates, the annual amounts of money laundered reached $651.7 million in 2003, $604.5 million in 2004, and $349.1 million in the first ten months of 2005.

Despite these improvements, the NOPCML is still hampered by a lack of sufficient resources (outdated IT systems) and personnel who are in need of comprehensive training regarding AML/CTF issues, as well as training in advanced analytical research methodologies. The Law on the Prevention and Sanctioning of Money Laundering increased the powers of NOPCML, but it did not provide for an increase in administrative capacity. The NOPCML has begun a process of international cooperation to exchange information with other FIUs. The NOPCML has also worked closely with Italy to improve its efficiency and effectiveness through an EU Project, which was completed in July 2005.

The total number of suspicious transactions reported to the NOPCML rose from 2,053 in 2004 to 2,826 in the first ten months of 2005. Of this figure, reporting by banks and other credit institutions rose from 1,417 in 2004 to 1,993 in the first ten months of 2005. Reporting entities have requested improved feedback from the NOPCML.

Efforts to prosecute these cases have been hampered by delays in reporting suspicious transactions (though somewhat improved in 2005) and by a lack of resources in some regions. The Directorate of Economic and Financial Crimes of the national police also has a mandate to pursue money laundering. However, despite hundreds of money laundering cases investigated since 2001, the interface with the justice system remains inadequate. In 2004, only one individual received a final conviction for money laundering under Law 656/2002, bringing the total to five between January 2002 and October 2005. At the end of the first nine months of 2005, the General Prosecutor's Office closed 133 criminal files related to money laundering, resulting in six indictments and 127 non-indictments since January 2005. There are 1,114 money laundering files pending. The National Anti-Corruption Department has opened 59 cases since 2004, of which four have resulted in an indictment and 34 in non indictments. Eleven cases are still pending.

Romania's 2002 anti-money laundering law was amended in July 2005 as Law 230/2005. The new law provides for a uniform approach to combating and preventing money laundering and terrorist financing. The purpose of the law is to meet the requirements of EU Directive 2001/97/EC and EU Directive 91/308/EEC on Preventing Use of the Financial System for Money Laundering, as well as the requirements of the European Council's Framework Decision of June 2001 on Identification, Search, Seizure, and Confiscation of the Means and Goods Obtained from Such Offenses. The law also responds to the Recommendations of the Financial Action Task Force (FATF). Law 230/2005 also provides that transactions suspected of connection to terrorism financing must be reported to the NOPCML and are subject to obligations regarding customer identification and the collection, preservation and disclosure of information.

The GOR announced a national anticorruption plan in early 2003 and passed a law against organized crime in April 2003. A new Criminal Procedure Code was passed and became effective on July 1, 2003. The new Code contains provisions for authorizing wiretapping and intercepting and recording telephone calls for up to 30 days, in certain circumstances. These circumstances, as provided for within the Code, include terrorist acts and money laundering.

In response to the events of September 11, 2001, Romania passed a number of legislative measures designed to sanction acts contributing to terrorism. Emergency Ordinance 141, passed in October 2001, provides that the taking of measures, or the production or acquisition of means or instruments,

with intent to commit terrorist acts, are offenses of exactly the same level as terrorist acts themselves. These offenses are punishable with imprisonment ranging from five to 20 years.

In April 2002, the Supreme Defense Council of the Country (CSAT) adopted a National Security Strategy, which includes a General Protocol on the Organization and Functioning of the National System on Preventing and Combating of Terrorist Acts. This system, effective July 2002 and coordinated through the Intelligence Service, brings together and coordinates a multitude of agencies, including 14 ministries, the General Prosecutor's Office, the National Bank, and the NOPCML. The Government of Romania (GOR) has also set up an inter-ministerial committee to investigate the potential use of the Romanian financial system by terrorist organizations.

Romanian law has some limited provisions for asset forfeiture in the Law on Combating Corruption, No. 78/2000, and the Law on Prevention and Combat of Tax Evasion, No. 241, introduced in July 2005. The Romanian Government, particularly the BNR, has been cooperative in seeking to identify and freeze terrorist assets. Emergency Ordinance 159, passed in late 2001, includes provisions for preventing the use of the financial and banking system to finance terrorist attacks, and sets forth the parameters for the government to combat such use. The BNR, which oversees all banking operations in the country, issued Norm No. 5 in support of Emergency Ordinance 159. Emergency Ordinance 153 was passed to strengthen the government's ability to carry out the obligations under UNSCR 1373, including the identification, freezing, and seizure of terrorist funds or assets. Legislative changes in 2005 extended the length of time a suspect account may be suspended. The NOPCML is now allowed to suspend accounts suspected of money laundering activity for three working days, as opposed to the previous two day limit. In addition, once the case is sent to the General Prosecutor's Office, it may further extend the period by four working days instead of the previously allowed three days.

In November 2004, the Parliament adopted law 535/2004 on preventing and combating terrorism, which abrogates some of the previous government ordinances and incorporates many of their provisions. The law includes a chapter on combating the financing of terrorism by prohibiting financial and banking transactions with persons included on international terrorist lists, and requiring authorization for transactions conducted with entities suspected of terrorist activities in Romania.

The BNR receives lists of individuals and terrorist organizations provided by the United States, the UNSCR 1267 Sanctions Committee, and the EU, and it circulates these to banks and financial institutions. The new law on terrorism provides that the assets used or provided to terrorist entities will be forfeited, together with finances resulting from terrorist activity. To date, in regard to terrorist financing, no arrests, seizures, or prosecutions have been carried out.

The EU's Europe Agreement with Romania provides for cooperation in the fight against drug abuse and money laundering. Romania is a member of the Council of Europe (COE) and participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). A mutual evaluation in April 1999 by that Committee uncovered a number of areas of concern, including the high evidence standard required for reporting suspicious transactions, a potential conflict with the bank secrecy legislation, and the lack of provisions for cases in which the reporting provisions are intentionally ignored. Romania has been working to address these concerns, bringing in legal experts from the EU to consult. In late 2003, Romania also underwent a Financial Sector Assessment Program (FSAP) by the World Bank as part of that organization's pilot program.

The GOR recognizes the link between organized crime and terrorism. Bucharest is the site of the Southeast European Cooperative Initiative's Center for Combating Transborder Crime, a regional center that focuses on intelligence sharing related to criminal activities, including terrorism. Romania also participates in a number of regional initiatives to combat terrorism. Romania has worked within SEEGROUP (a working body of the NATO initiative for Southeast Europe) to coordinate counterterrorist measures undertaken by the states of Southeastern Europe. The Romanian and

Bulgarian interior ministers signed an inter-governmental agreement in July 2002 to cooperate in the fight against organized crime, drug smuggling, and terrorism.

The NOPCML is a member of the Egmont Group. A Mutual Legal Assistance Treaty signed in 2001 between the United States and Romania entered into force in October 2001. The GOR has demonstrated its commitment to international anticrime initiatives by participating in regional and global anticrime efforts. Romania is a party to the 1988 UN Drug Convention, the Agreement on Cooperation to Prevent and Combat Transborder Crime, and the UN Convention against Transnational Organized Crime. Romania also is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the Council of Europe's Criminal Law Convention on Corruption; and the UN International Convention for the Suppression of the Financing of Terrorism. On November 2, 2004, Romania became a party to the UN Convention against Corruption.

Although legislation and regulations designed to combat financial crime are fairly new, they are quite comprehensive in scope. Nevertheless, implementation lags. The FIU has improved in its ability to report and investigate cases in a timely fashion. However, these investigations have resulted in only a handful of successful prosecutions to date. Romania should ensure that non-bank entities are fully aware of their reporting and record-keeping responsibilities and are adequately supervised. Romania should improve communications between reporting and monitoring entities, as well as between prosecutors and monitors. The General Prosecutor's Office should place a higher priority on money laundering cases. Romania should further implement existing procedures for the timely freezing, seizure, and forfeiture of criminal or terrorist-related assets.

Russia

Russia has enjoyed rapid economic growth in recent years, mainly driven by high world energy prices. However, Russia has been slow to complete structural reforms of the banking sector, and overall public confidence in Russian banks remains low. Russia's financial system does not attract a significant portion of legal or illegal depositors, and therefore Russia is not considered an important regional financial center. Over the past several years, however, Russia has committed significant resources to improve its ability to combat the laundering of criminal financial proceeds domestically and internationally. Through aggressive enactment and implementation of comprehensive money laundering and counterterrorism financing legislation, Russia now has well-established legal and enforcement frameworks to deal with money laundering and terrorism financing.

Despite having the political will to combat financial crime and making noticeable progress in doing so, Russia remains vulnerable to such activity because of its vast natural resource wealth, the pervasiveness of organized crime, and a high level of corruption. Other factors include porous borders, Russia's role as a geographic gateway to Europe and Asia, a weak banking system, and under-funding of regulatory and law enforcement agencies. Criminal elements from Russia and neighboring countries continue to use Russia's financial system to launder money because of familiarity with the language, culture, and economic system. The majority of laundered funds do not appear to be from activities related to narcotics production or trafficking, although these activities likely occur. Experts believe that most of the dirty money flowing through Russia derives from domestic criminal or quasi-criminal activity, including evasion of tax and customs duties and smuggling operations.

Net private capital inflows for 2005 were $0.3 billion, according to the Russian Ministry of Finance, marking a reversal from the $9.3 billion in outflows in 2004. In contrast to the capital flight that occurred during the 1990s, the majority of more recent outflows involve the legitimate movement of money to more secure and profitable investments abroad, which reflects the maturing of the Russian business sector. However, at least a portion of this money undoubtedly involves the proceeds of criminal activity.

Russia has the legislative and regulatory framework in place to pursue and prosecute financial crimes, including money laundering and terrorism finance. The Russian Federation's Federal Law No. 115-FZ "On Combating Legalization (Laundering) of Criminally Gained Income and Financing of Terrorism" became effective on February 1, 2002, with subsequent amendments to the laws on banking, the securities markets, and the criminal code taking effect in October 2002, January 2003, December 2003, and July 2004. Law RF 115-FZ obligates banking and non-banking financial institutions to monitor and report certain types of transactions, keep records, and identify their customers.

According to the original language of RF 115-FZ, those institutions legally required to report included: banks, credit organizations, securities market professionals, insurance and leasing companies, federal postal service, jewelry and precious metals merchants, betting shops, and companies managing investment and non-state pension funds. Amendments to the law that came into force on August 31, 2004, extend the reporting duty to real estate agents, lawyers and notaries, and persons rendering legal or accounting services that involve certain transactions (e.g., managing money, securities, or other property; managing bank accounts or securities accounts; attracting or managing money for organizations; or incorporating, managing, and buying or selling organizations).

Article 8 of Law 115-FZ provides for the establishment of Russia's financial intelligence unit as an independent executive agency administratively subordinated to the Ministry of Finance. In March 2004, President Putin issued a decree to upgrade the unit, formerly called the Financial Monitoring Committee, to a service, now called the Federal Service for Financial Monitoring (FSFM). All financial institutions with an obligation to report certain transactions must send this information to the FSFM. The FSFM's mission is to implement a unified state policy to combat money laundering and terrorism finance, yet it has no law enforcement investigative powers. In June 2005, President Putin approved a national strategy for combating money laundering and terrorism finance, part of which called for the creation of a new interagency commission on money laundering. The Ministry of Justice established the commission in November 2005, which is comprised of 12 ministries and government departments. The new commission will be chaired by the head of the FSFM and will be responsible for monitoring and coordinating the government's activity on money laundering and terrorism financing.

Various regulatory bodies ensure compliance with Russia's anti-money laundering and counterterrorism finance laws. The FSFM is specifically responsible for regulating real estate and leasing companies, pawnshops, and gambling services. The Central Bank of Russia (CBR) supervises credit institutions; the Federal Insurance Supervision Service oversees insurance companies; the Federal Service for Financial Markets regulates entities managing non-governmental pension and investment funds, as well as professional participants in the securities sector; and the Assay Chamber (under the Ministry of Finance) supervises entities buying and selling precious metals or stones.

The CBR has issued guidelines regarding anti-money laundering practices within credit institutions, including "know your customer" (KYC) and bank due diligence programs. Banks are required to obtain and retain for five years information regarding individuals and legal entities and beneficial owners of corporate entities. Further, banks must adopt internal compliance rules and procedures and appoint compliance officers. Since July 2004, the amendment to Law 115-FZ now requires banks to identify the original source of funds and to report to the FSFM all suspicious transactions. Institutions that fail to meet mandatory reporting requirements face revocation of their licenses to carry out relevant activity, limits on certain banking operations, and possible criminal or administrative penalties. An administrative fine of up to $16,700 can be levied against an institution, with a fine of up to $700 on an officer of an institution. The maximum criminal penalty is 10 years in prison with applicable fines.

Since the CBR issued Order 1317-U in August 2003, Russian financial institutions must now report all transactions with their counterparts in offshore zones. In some cases, offshore banks are also subject to

enhanced due diligence and maintenance of additional mandatory reserves to offset potential risks undertaken by the Russian institution for specific transactions. The CBR has also raised the standards for "eligible" offshore financial institutions, thereby reducing their number. Overall wire transfers from Russian banks to offshore financial centers have dropped significantly as a result of such regulatory measures.

Foreign financial entities, including those from known offshore havens, are not permitted to operate directly in Russia; they must do so solely through subsidiaries incorporated in Russia, which are subject to domestic supervisory authorities. During the process of incorporating and licensing these subsidiaries, Russian authorities must identify and investigate each director of the Russian unit; therefore nominee or anonymous directors are, as a practical matter, not permitted under Russian law and regulation. In September 2005, the CBR completed its review of all banks that sought admission to the recently established Deposit Insurance System (DIS). To gain admission to the DIS, a bank had to verifiably demonstrate to the CBR that it complies with Russian identification and transparency requirements. Currently, 927 of Russia's estimated 1200 banks have been admitted to the DIS, effectively weeding out over 200 banks from Russia's banking system.

By law, Russian businesses must obtain government permission before opening operations abroad, including in offshore zones. A department within the Ministry of Economic Development and Trade (MEDT) reviews such requests from Russian firms, and once the MEDT approves, the CBR must then approve the overseas currency transfer. In either case, the regulatory body responsible for the offshore activity is the same as for domestic activity, i.e., the Federal Service for Financial Markets regulates brokerage and securities firms, while the CBR regulates banking activity.

All obligated financial institutions must monitor and report to the government: any transaction that equals or exceeds 600,000 rubles (approximately $20,000) and involves or relates to: cash payments, individuals or legal entities domiciled in states that do not participate in the international fight against money laundering, bank deposits, precious stones and metals, payments under life insurance policies, or gambling; all transactions of "extremist organizations" or individuals included on Russia's domestic list of such entities and individuals; and suspicious transactions.

Each of the FSFM's seven territorial offices corresponds with one of the federal districts that comprise the Russian Federation. The Central Federal District office is headquartered in Moscow; the remaining six are located in the major financial and industrial regions throughout Russia. The primary functions of the territorial offices are to coordinate with regional law enforcement and other authorities to enhance the incoming information flow into the FSFM, and to supervise compliance with anti-money laundering and counterterrorism financing legislation by institutions under FSFM supervision. Additionally, the satellite offices must identify and register at the regional level all pawnshops, leasing and real estate firms, and gaming entities under their jurisdiction. The regional offices also are charged with coordinating the efforts of the CBR and other supervisory agencies to implement anti-money laundering and counterterrorist financing regulations.

Russia's anti-money laundering law, as amended, provides the FSFM with the appropriate authority to gather information regarding the activities of investment foundations, non-state pension funds, gambling businesses, real estate agents, lawyers and notaries, persons rendering legal/accountancy services, and sales of precious metals and jewelry. Virtually all financial institutions submit reports to the FSFM via encrypted software provided by the FSFM. According to press reports, Russia's national database contains over four million reports involving operations and deals worth over $877 billion. The FSFM estimates that Russian citizens may have laundered as much as $7 billion in 2005. The FSFM receives approximately 10,000 transaction reports daily. Of these daily reports, 75 percent result from mandatory (currency) transaction reports, and the remaining 25 percent relate to suspicious transactions.

During the first ten months of 2005, the FSFM carried out 3,803 financial investigations, referring 2,026 of them to law enforcement agencies for possible criminal investigations. According to the Economic Crimes Unit of the Ministry of Interior (MVD), in 2005 Russian law enforcement investigated 7,269 cases of money laundering, sent 6,186 of the cases to court, and convicted 216 individuals on money laundering charges. Both the FSFM and MVD estimate that the number of suspicious transaction reports in 2005 has grown five-fold over the previous year, an increase which both agencies attribute to a greater focus government-wide on financial crimes and terrorism financing.

On terrorism finance, the FSFM reports that it has compiled a list of 1,300 organizations and individuals suspected of financing terrorism, 400 of which were foreign. To date, the FSFM has uncovered 113 bank accounts related to organizations and individuals included on Russia's terrorism list. Depending on the nature of the activity, the FSFM provides information to the appropriate law enforcement authorities for further investigation, i.e., the MVD for criminal matters, the Federal Drug Control Service (FSKN) for narcotics-related activity, or the Federal Security Service (FSB) for terrorism-related cases.

As part of administrative reforms enacted in 2004, the FSKN now has a full division committed to money laundering, staffed by agents with experience in counternarcotics and economic crimes. This division cooperates closely with the FSFM in pursuing narcotics-related money laundering cases. In 2005, the FSKN reportedly initiated approximately 1,550 money laundering cases and referred over 400 of these cases to the General Procuracy for prosecution. In July 2005, the FSKN announced that it had uncovered a major money laundering ring that was using an alternative remittance system to conduct illegal transactions involving money gained from drug smuggling. According to the FSKN's press service, the FSKN uncovered monthly transactions of up to $14 million that were linked to this criminal ring. The FSKN arrested four individuals, and opened criminal cases under Article 172 (illegal banking activities) and Article 174.1 (money laundering) of Russia's criminal code. Consistent with Financial Action Task Force (FATF) recommendations, the criminal code was amended in December 2003 to remove a specific monetary threshold for crimes connected with money laundering, thus paving the way for prosecution of criminal offenses regardless of the sum involved.

With its legislative and enforcement mechanisms in place, Russia has begun to prosecute high-level money laundering cases. In 2005, the CBR revoked the licenses of 37 banks for failing to observe banking regulations. Of these, 14 banks lost their licenses for violating Russia's anti-money laundering laws. In early 2005, the FSFM announced that it suspected ten unnamed banks of involvement in money laundering activities. Subsequently, the CBR announced that it was considering revoking the licenses of two banks for suspicion of money laundering. According to press reports, Russian law enforcement agencies conducted several raids and launched criminal investigations into banks suspected of money laundering. This increased targeting of suspect credit and non-credit institutions demonstrates Russia's broad-based commitment to enforcing its anti-money laundering and counterterrorism financing legislation and an improvement in compliance levels as a result of its actions.

Russia has a legislative and financial monitoring scheme that permits the tracking, seizure and forfeiture of criminal proceeds. None of this legislation is specifically tied to narcotics proceeds. Russian legislation provides for investigative techniques such as search, seizure, and compelling the production of documents, as well as the identification, freezing, seizing, and confiscation of funds or other assets. Where sufficient grounds exist to suppose that property was obtained as the result of a crime, investigators and prosecutors can apply to the court to have the property frozen or seized. Law enforcement agencies have the power to identify and trace property that is, or may become, subject to confiscation or is suspected of being the proceeds of crime or terrorist financing. Moreover, the law allows the FSFM, in concert with banks, to freeze possible terrorist-related financial transactions up to

one week. Banks may freeze transactions for two days, and the FSFM may follow up with freezing for an additional five days.

In accordance with its international agreements, Russia recognizes rulings of foreign courts relating to the confiscation of proceeds from crime within its territory and can fully or partially transfer confiscated proceeds of crime to the foreign state whose court issued the confiscation order. However, Russian law still does not provide for the seizure of instruments of crime. Businesses can be seized only if it can be shown that they were acquired with criminal proceeds. Legitimate businesses cannot be seized solely on the basis that they were used as "instruments" to facilitate the commission of a crime. The Presidential Administration as well as Russian law enforcement agencies have expressed concern about the ineffective implementation of Russia's confiscation laws. The government has proposed amendments that are currently under review by the Duma which would make it easier to identify and seize criminal instrumentalities and proceeds. While Russian law enforcement has adequate police powers to trace assets, and the law permits confiscation of assets, most Russian law enforcement personnel lack experience and expertise in these areas.

The Russian Federation has enacted several pieces of legislation and issued executive orders to strengthen its ability to fight terrorism. On January 11, 2002, President Putin signed a decree entitled "On Measures to Implement the UN Security Council Resolution (UNSCR) No. 1373 of September 28, 2001." Noteworthy among this decree's provisions are the introduction of criminal liability for intentionally providing or collecting assets for terrorist use, and the instructions to relevant agencies to seize assets of terrorist groups. This latter clause, however, conflicted with existing domestic legislation. Accordingly, on September 24, 2002, the Duma approved an amendment to the anti-money laundering law, resolving the conflict and allowing banks to freeze assets immediately, pursuant to UNSCR 1373. This law came into force on January 2, 2003. Further, Article 205.1 of the criminal code, which was enacted in October 2002, criminalizes terrorist financing. On October 31, 2002, the Federation Council, Russia's upper house, approved a supplemental article to the 2003 federal budget, allocating from surplus government revenues an additional 3 billion rubles ($100 million) in support of federal counterterrorism programs and improvement of national security.

In February 2003, at the request of the General Procuracy, the Russian Supreme Court issued an official list of 15 terrorist organizations. According to press reports, the financial assets of these organizations were immediately frozen. In addition, Russia has assisted the United States in investigating high profile cases involving terrorist financing. In 2003, Russia provided vital financial documentation and other evidence that helped establish the criminal activities of the Benevolence International Foundation (BIF). In April 2005, a U.S. Federal Court convicted a British national for attempting to smuggle shoulder-held missiles into the U.S. with the intent to sell the weapons to a presumed terrorist group. The subject was arrested in a sting operation that involved 18 months of collaboration among U.S., Russian, and British authorities. He was found guilty on five counts, including material support to terrorists, unlawful arms sale, smuggling, and two counts of money laundering. However, Russia and the U.S. continue to differ about the purpose of the UN 1267 Sanctions Committee's designation process, and such political differences have hampered bilateral cooperation in this forum.

Russia became a full member of the FATF in June 2003 and was the driving force behind the creation of the Eurasian Group on Combating Legalization of Proceeds from Crime and Terrorist Financing (EAG), which also includes Belarus, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan as members, and several other nations and multilateral organizations as observers, including the United States. The EAG Secretariat is located in Moscow. Since its inception, the EAG has held three plenary sessions (two in Moscow and one in Shanghai) in addition to several working group and typologies meetings. Russia, in its current role as President of the EAG, continues to play a strong leadership role in bringing the region up to international standards in its capacity to fight money laundering and terrorism financing.

The United States and Russia signed a Mutual Legal Assistance Treaty in 1999, which entered into force on January 31, 2002. The FSFM has signed cooperation agreements with the Financial Intelligence Units (FIUs) of 24 countries, including Belgium, Columbia, Cyprus, Czech Republic, Estonia, Finland, France, Israel, Italy, Korea, Latvia, Liechtenstein, Luxembourg, Monaco, Panama, Peru, Poland, Portugal, Slovenia, Sweden, Ukraine, the United Kingdom, the United States, and Venezuela. Additionally, the FSFM is an active member of the Egmont Group, having sponsored several candidate countries for membership in 2004. U.S. law enforcement agencies exchange operational information with their Russian counterparts on a regular basis. In 2005, Russian law enforcement agencies cooperated with the U.S. in a high- profile case that led to the conviction of a Russian national in a U.S. District Court on charges that he laundered over $130 million through a Moscow bank. The individual was sentenced to 51 months imprisonment and ordered to pay $17.4 million in restitution to the Russian government.

In addition to membership in the FATF, Russia holds membership in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). Russia ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime in January 2001. Russia is a party to the 1988 UN Drug Convention and on May 26, 2004, became a party to the UN Convention against Transnational Organized Crime. In November 2002, Russia ratified the UN International Convention for the Suppression of the Financing of Terrorism. Russia also became a signatory to, but has not yet ratified, the UN Convention against Corruption.

Russia has developed a solid legislative and regulatory foundation for combating money laundering and terrorism financing. Given its role in spearheading the creation of the EAG, Russia has demonstrated both the political will and a capability to improve the region's capacity for countering money laundering and terrorism financing. President Putin also sent a clear signal of support when he approved a national money laundering strategy in June 2005 and charged an inter-agency commission to implement the strategy in the short term.

Nevertheless, some vulnerabilities remain. To meet President Putin's stated goal of combating money laundering and corruption, Russia needs to follow through on its commitment to improve CBR oversight of shell companies and scrutinize more closely those banks that do not carry out traditional banking activities. To prevent endemic corruption and deficiencies in the business environment from undermining Russia's efforts to establish a well functioning anti-money laundering and counterterrorism finance regime, Russia should strive to stamp out official corruption, particularly at high levels, and to increase transparency in the financial sector and the corporate environment. Russia should also commit adequate resources to its regulatory and law enforcement entities in order to help them fulfill their responsibilities, and enact legislation that would provide for the seizure of instruments, as opposed to merely the proceeds, of criminal activity. Finally, Russia should continue to play a leadership role in the region with regard to anti-money laundering and counterterrorist finance regime implementation.

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 Samoa 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. At the 2005 Asia/Pacific Group Plenary, Samoa reported that these bills and an Insurance Act would be tabled for Parliament's approval in December, 2005. The Attorney General's stated that enactment of the relevant amendments to these bills would be enacted in the first quarter of 2006.. Samoa also reported that in 2004, the MLPA received 23 suspicious transaction reports in 2004. 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.

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 eleven 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 2005, although a definitive determination is hard to make because of the absence of official criminal statistics, 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 (GOSA) 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 Recommendations of the Financial Action Task Force (FATF). 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 ($26,667); 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 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 GOSA provides anti-money laundering training for bank employees, prosecutors, judges, customs officers and other government officials.

In 2003, the GOSA established an anti-money laundering unit in SAMA and in 2005 the GOSA opened a Financial Investigation Unit (FIU) under the auspices of the Ministry of Interior. Saudi banks are required to have their own anti-money laundering units with specialized staff to work with SAMA,

the FIU and law enforcement authorities. All banks are also required to report any suspicious transactions to the FIU. The Saudi FIU collects and analyzes suspicious transaction reports and other available information and decides whether to make referrals to the Ministry of Interior's Bureau of Investigation and Prosecution or other entities for further investigation and prosecution. The FIU is staffed by officers from the Mabahith and SAMA. The FIU is committed to obtaining membership in the Egmont Group within the next two years.

Hawala transactions outside banks and licensed money changers 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. In 2005, in an effort to further regulate the over $16 billion in remittances that leave Saudi Arabia every year, in 2005 SAMA consolidated the eight largest money changers into a single bank, Bank Al-Bilad.

In late 2005, the GOSA enacted stricter regulations on the cross-border movement of money and precious metals. Money and gold in excess of $16,000 must be declared upon entry and exit from the country. While the regulations were effective immediately, Customs staff training and public education probably will not be completed until early-to-mid 2006.

Contributions to charities in Saudi Arabia are usually in the form of Zakat, which refers to an Islamic religious duty with specified humanitarian purposes. The 9/11 Commission Report noted that the GOSA failed to adequately supervise 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 GOSA issued guidelines for the National Commission for Relief and Charitable Work Abroad. However, as of the end of 2005, there has been no further announcement on the Charities Commission structure, leadership or staffing. The U.S. government is working with the Saudi authorities to clarify the status of the international charities with headquarters in Saudi Arabia and the role of the Charities Commission.

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 all charities include stipulations that accounts can be only 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; and there will be no money transfers outside of Saudi Arabia. According to GOSA officials, these regulations apply to international charities as well and are being actively enforced.

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 for 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 GOSA was one of the original charter signatories. The MENAFATF is a FATF-style regional body.

The success of the MENAFATF is 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 names of suspected terrorists and terrorist organizations on 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 GOSA and U.S. continue to work bilaterally to investigate terrorist financing. 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 is moving to monitor and enforce its anti-money laundering and terrorist finance laws, regulations and guidelines. However, it needs to establish the High Commission for Charities. As in many countries in this 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. Donations in the form of gold and other gifts need to be scrutinized. International charities need to be made subject to the same government oversight as domestic charities, including the rules of both SAMA and the Charities Commission. The GOSA should become a party to the UN International Convention for 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). Serbia and Montenegro is located in Southeastern Europe (the Balkans), bordering the Adriatic Sea to the west and Romania and Bulgaria to the east. SAM is a state union consisting of two republics, the Republic of Serbia and the Republic of Montenegro. In the Republic of Serbia is the nominally autonomous province of Vojvodina. Kosovo, recognized by the UN as part of SAM, has been administered by the United Nations Mission in Kosovo since 1999. (Since Serbia no longer exercises effective control over Kosovo, this report does not address Kosovo.) 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 continues to have a significant black market for smuggled goods. Illegal proceeds are generated from drug trafficking, official corruption, tax evasion, organized crime and other types of financial crimes. Proceeds from illegal activities are being heavily invested in all forms of real estate. The construction and renovation of commercial buildings such as offices, apartments, high-end retail businesses as well as personal residences is evident in the capitals of Belgrade and Podgorica as well as other major cities. Investment by foreign individuals and businesses in expensive real estate along the Montenegro coast has raised prices and generated concerns about the source of funds used for these investments.

Tax evasion, which is a predicate crime for money laundering, and trade-based money laundering in the form of over- and under-invoicing, are common methods used to launder money. Serbia introduced a VAT tax in 2005 and the full impact of refund fraud associated with the administration of the VAT

is still not clear. Serbia's Tax Administration does not have the capacity or resources to investigate the large number of suspicious transactions that are forwarded by Serbia's Financial Intelligence Unit (FIU). This creates a situation where criminals can spend and invest criminal proceeds freely with little fear of challenge by the tax authorities or other law enforcement agencies. In both Serbia and Montenegro, the difficulty of convicting a suspect of money laundering without a conviction for the original criminal act and the unwillingness of the courts to accept circumstantial evidence to support money laundering or tax evasion charges is hampering law enforcement and prosecutors in following the movement and investment of illegal proceeds and effectively using the anti-money laundering laws.

Some Serbian officials also estimate that up to half of all significant financial transactions in SAM may be connected in some way to money laundering. Neither republic has identified any activities relating to the financing of terrorism. Both Montenegro and Serbia (2005) have criminalized the financing of terrorism.

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 invested in federal Yugoslav authorities devolved to the individual republics. As a result, responsibility for the laws and institutions that determine policies shifted. Subsequently, 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 in its own way. Banks in both republics have demonstrated substantial compliance with the laws in their respective jurisdictions.

Serbia and Montenegro 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 does not have a mutual legal assistance arrangement with the United States. SAM has signed 34 bilateral agreements on mutual legal assistance with 21 countries: Algeria, Austria, Belgium, Bulgaria, the Czech Republic, France, Greece, Croatia, Iraq, Italy, Cyprus, Germany, Poland, Romania, Hungary, Macedonia, Mongolia, Russian Federation, Spain, Turkey, the United Kingdom. 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; a sub-office for liaison with Interpol exists in the Montenegrin Interior Ministry.

Ratification of international Conventions and treaties currently lies at the State Union level. 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 is a party to 11 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 Serbia. Both Serbia and Montenegro have criminalized the financing of terrorism, but the freezing, seizing and confiscation of assets of terrorists in accordance with UN Security Council resolutions still lacks a legal basis in Serbia; Montenegro can since 2005 take action on the basis of such decisions. In December 2003, SAM

signed, and recently 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. The report urged both republics to improve the provisions on provisional measures and confiscation, as well as to adopt specific provisions on the countering of the financing of terrorism, both the criminalization and the obligation to report in case of a suspicion of financing of terrorism.

Serbia. The Yugoslav Federal Assembly adopted an Anti-Money Laundering Law (AML Law) in September 2001; it came into effect in July 2002. This law effectively created Serbia's Financial Intelligence Unit (FIU), the Administration for the Prevention of Money Laundering. In July 2003, the FIU became a member of the Egmont Group, and has since begun active participation in information exchanges with counterpart FIUs.

In September 2005, Serbia criminalized terrorist financing and codified an expanded definition of money laundering into the Penal Code. This gives police and prosecutors more flexibility to pursue money laundering charges since the money laundering conduct is broader under the new law and in conformity with international standards. The penalty for money laundering is up to 10 years imprisonment. This is significant in that under Serbian law and procedure, it falls into the serious crime category and permits the use of Mutual Legal Assistance (MLAT) procedures to obtain information from abroad. Previous penalties for money laundering kept money laundering out of the serious crime category, and use of the MLAT or letters rogatory were not an option in cases where a serious crime could not be identified as the source of the suspected illegal proceeds.

On November 28, 2005, Serbia adopted a revised money laundering law that elevates the status of the FIU to that of an administrative body under the Ministry of Finance from its previous position of "sector" in that Ministry. This will provide more autonomy for the agency to carry out its mandate and provide additional resources. One important change is that the Administration will have its own line item operating budget. The law also expands the number of entities required to collect certain information on all transactions over 15,000 Euros, or the dinar equivalent, and to report all cash transactions exceeding this threshold to the FIU. Suspicious transactions in any amount must be reported to the FIU. The law also requires attorneys and accountants to report suspicious transactions. Other significant changes include the authority of the FIU to freeze transactions for up to 72 hours and to require covered entities and individuals to monitor customers' accounts where money laundering is suspected. Under Serbian law, assets derived from criminal activity or suspected of involvement in the financing of terrorism can be confiscated upon conviction for an offense.

Serbia signed a memorandum of understanding (MOU) on the exchange of information with the National Bank of Serbia in 2004 and is negotiating MOUs with the Customs and Tax Administrations. The Government of Serbia has established an interagency working group tasked with developing an implementation plan for the recommendations from MONEYVAL's review in October 2003. It is also tasked with drafting a new law to address the procedures needed to comply with UN Security Council resolutions regarding the freezing, seizing and confiscation of suspected terrorist assets and to require suspicions of terrorist financing to be reported to the FIU.

The FIU 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.

The government still needs better interagency coordination to improve information sharing, record keeping and statistics, and thereby introduce a more effective regime and permit a meaningful assessment of its AML/CFT efforts at all levels of government.

Montenegro. 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 to detect money laundering. The CBCG dissolved all offshore banks for failure to re-register and reestablish themselves as regular banks. 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 was criminalized in 2002, and the Criminal Code was amended in June 2003 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 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 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 became operational in November 2003 and began receiving reports of transactions in July 2004. All reporting by banking institutions is received electronically. The Montenegro FIU became an Egmont member in June 2005. It has executed a number of Memorandums of Understanding to exchange information with most established FIUs in the region.

Montenegro can seize and forfeit assets. In September 2004, the Government of Montenegro seized over one million euros in undeclared currency in connection with the arrest of two Chinese nationals attempting to enter Montenegro. Further investigation revealed that these individuals had moved over four million euros through bank accounts in Montenegro. The criminal charges were dismissed by the court of first instance which said that the Prosecutor's office had not provided proof that the funds were from an illegal source. This case has been appealed.

Amendments to Montenegro's laws on terrorism and terrorist financing were initiated in November 2004 and adopted in March 2005. These amendments were 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 circulates to banks and other financial institutions the names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanction Committee's consolidated list. No terrorist financing or use of alternative remittance systems have been detected within Montenegro.

It would be beneficial for the U.S. to have an updated extradition treaty with SAM as well as a bilateral mutual legal assistance agreement. 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 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. They should both implement a comprehensive framework to support a

counterterrorism regime that complies with international standards. Serbia should adopt the new law to address the procedures needed to comply with UN Security Council resolutions regarding the freezing, seizing and confiscation of suspected terrorist assets and to require suspicions of terrorist financing to be reported to the FIU.

Seychelles

Seychelles is a not a major financial center, but it does have a developed offshore financial sector that 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 25,461 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, one for Captive Insurance and two for General Insurance). 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.

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. The transactions of charitable and non-profit entities are scrutinized by the authorities to prevent their misuse, and such alternative remittance systems as hawala are regulated. 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 is no cross-border currency reporting requirement.

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. While there have been about thirty investigations, there have been no arrests or prosecutions for money laundering or terrorist financing since January 1, 2003.

In 1998, the Central Bank of Seychelles issued a comprehensive set of guidance notes that clarified 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 of 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 provision 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 of 2004. The legislation specifically recognizes the government's authority to identify, freeze, and seize terrorist finance-related assets. Under the new law, 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.

The Mutual Assistance in Criminal Matters Act of 1995 empowers the Seychelles Central Authority to provide assistance in connection with a request to conduct searches and seizures relating to serious offenses under the law of the requesting state. Previously, the Seychelles authorities could work only with states that were members of the Commonwealth or that had a treaty for bilateral mutual legal assistance with the Seychelles regarding criminal matters. The Prevention of Terrorism Bill of 2004 extends the authority of the GOS to include the freezing and seizing of terrorism-related assets, upon the request of a foreign state. To date, no such assets have been identified, frozen, or seized.

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. Seychelles signed and ratified the UN International Convention for the Suppression of the Financing of Terrorism on March 30, 2004. The Seychelles circulates to relevant authorities the updated lists of names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224. Seychelles should expand its anti-money laundering efforts by moving to prohibit bearer shares and requiring the 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 criminalize the financing of terrorism and continue to 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, widespread corruption, and a prevalent informal money-exchange system create an atmosphere that is 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.

The President signed the Anti-Money Laundering Act in July 2005. The new law requires that international financial transfers over $10,000 go through formal financial institution channels. The law designates the Governor of the Bank of Sierra Leone as the Anti-Money Laundering Authority and also establishes a financial intelligence unit to oversee financial institution operations. Sierra Leone is

still a cash economy, and the new anti-money laundering law has not been widely publicized. There have been a few arrests under the law but no convictions to date.

In July 1996, the Central Banks of The Gambia, Ghana, Liberia, Nigeria and Sierra Leone established the West African Institute for Financial and Economic Management (WAIFEM) (www.waifem.org). The Institute's principal mandate is to build sustainable capacity for macroeconomic management in the five countries. It also conducts research and consultancy services in the area of macro policy management. In September 2005, the Bank of Sierra Leone hosted a WAIFEM-sponsored regional anti-money laundering workshop.

Sierra Leone is a party to the 1988 UN Drug Convention, the UN Convention Against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime.

Now that Sierra Leone has the Anti-Money Laundering Act in place, the challenges will be increasing awareness and enforcement. The country should implement the law as soon as possible. It should ratify the UN Convention against Transnational Organized Crime.

Singapore

As a significant international financial and investment center, and in particular as a major offshore financial center, Singapore is vulnerable to potential money launderers. Bank secrecy laws and the lack of routine currency reporting requirements make Singapore an attractive destination for drug traffickers, criminals, terrorist organizations and their supporters seeking to launder 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.

Some structural gaps remain in financial regulation that may hamper efforts to control these crimes. The Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act of 1999 (CDSA) criminalizes the laundering of proceeds from narcotics and 184 other categories of serious offenses, including ones committed overseas, which would be serious offenses if they had been committed in Singapore. As part of amendments to the CDSA that came into effect in September 2005, Singapore added two more categories of offenses. Despite these changes, Singapore's current list of designated predicate offenses for money laundering does not include many of those in line with the Financial Action Task Force's (FATF's) Recommendations.

Singapore has a sizeable offshore financial sector. In 2005, there were 110 commercial banks in operation, including five local and 24 foreign-owned full banks, 46 offshore banks, and 35 wholesale banks. All offshore and wholesale banks are also foreign-owned. Singapore does not permit shell banks, in either 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, particularly with respect to Singapore's anti-money laundering and countering the financing of terrorism efforts (AML/CFT). MAS performs extensive prudential and regulatory checks on all applicants for banking licenses, including whether banks are under adequate home country banking supervision. Banks must have clearly identified directors. Unlicensed banking transactions are illegal.

Beginning in 2000, MAS began issuing 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. 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 to verify names, permanent contact addresses, dates of birth, and nationalities, and to check 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. They 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.

In January 2005, as part of a draft revision of its overall AML/CFT regulations for banks, MAS commenced a review of Notice 626, which proscribes banks from entering into, or continuing, correspondent banking relationships with shell banks, in line with the Revised FATF Forty Recommendations adopted in June 2003. Draft Notice 626, which is still under review, also mandates originator information on cross-border wire transfers, in line with 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, and mandates enhanced customer due diligence for foreign politically exposed persons. It furthermore extends coverage of the regulations to include terrorist financing activities. In addition to the revised Notice 626, Singapore is reviewing regulations governing other financial institutions and designated non-financial businesses and professions to bring them into conformity with FATF recommendations.

In addition to banks offering trust, nominee, and fiduciary accounts, Singapore has 16 trust companies. All banks and trust companies, whether domestic or offshore, are subject to the same regulation, record keeping, and reporting requirements, including regarding money laundering and suspicious transactions. In August 2005, Singapore introduced regulations under the new Trust Companies Act (enacted in January 2005 to replace the Singapore Trustees Act) that mandated licensing of trust companies and MAS approval for appointments of managers and directors.

In April 2005, Singapore lifted its ban on casinos, paving the way for the development of integrated resorts with casinos. Total investment in the two resorts, both of which are expected to open in 2009, is estimated to exceed $4 billion. In October 2005, Singapore released for public comment draft legislation for the Casino Control Act. The Act calls for creation of a Casino Regulatory Authority and mandates certain cash reporting requirements. Internet gaming sites are illegal in Singapore.

Any person who wishes to engage in for-profit business in Singapore, whether local or foreign, must register under the Companies Act. Every Singapore-incorporated company is required to 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.

Financial institutions must report suspicious transactions and positively identify customers engaging in large currency transactions, and are required to maintain adequate records. However, there is no systematic reporting of large currency transactions. There are no reporting requirements on amounts of currency brought into or taken out of Singapore. Singapore is considering implementation of FATF Special Recommendation Nine, which requires either a declaration or disclosure system for monitoring cross-border movement of currency and bearer negotiable instruments.

The Singapore Police's Suspicious Transaction Reporting Office (STRO) has served as the country's Financial Intelligence Unit (FIU) since January 2000. In December 2004, STRO concluded a Memorandum of Understanding (MOU) concerning the exchange of financial intelligence with its U.S. counterpart, FinCEN. STRO has also signed MOUs with counterparts in Australia, Belgium and Japan, and continues to actively seek MOUs with additional FIUs. To improve its suspicious transaction reporting, STRO is developing a computerized 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. Procedural regulations and bank secrecy laws limit STRO's ability to provide information relating to financial crimes.

Singapore is an important participant in the regional effort to stop terrorist financing in Southeast Asia. The Terrorism (Suppression of Financing) Act that took effect January 29, 2003, 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.

Based on an assessment of Singapore's financial sector published in April 2004, the International Monetary Fund and World Bank concluded that the country imposes few restrictions on intergovernmental terrorist financing-related mutual legal assistance, even in the absence of a Mutual Legal Assistance Treaty, because it is a party to the UN International Convention for the Suppression of the Financing of Terrorism. The IMF, however, urged Singapore to improve its mutual legal assistance for other offenses, noting serious limitations on assistance with the provision of bank records, search and seizure of evidence, restraining proceeds of crime, and the enforcement of foreign confiscation orders.

MAS has broad powers to direct financial institutions to comply with international terrorist financing obligations. 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 that will benefit terrorists or terrorist financing. Financial institutions must notify the MAS immediately if they have in their possession, custody or control any property belonging to designated 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 located in Singapore. The regulations include periodically updated names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

Singapore's approximately 600,000 foreign guest workers are the main users of alternative remittance systems. As of June 2005, there were 406 money-changers and 102 remittance agents. All must be licensed and are subject to the Money-Changing and Remittance Businesses Act (MCRBA), which includes requirements for record-keeping and the filing of suspicious transaction reports. Firms must submit a financial statement every three months and report the largest amount transmitted on a single day. They must also answer questions about their business and overseas partners. Unlicensed informal networks, such as hawala, are illegal. In August 2005, Singapore amended the MCRBA to apply certain AML/CFT regulations to remittance licensees and money-changers engaged in inward remittance transactions. The Act eliminated sole proprietorships and required all remittance agents to incorporate under the Companies Act with a minimum paid-up capital of S$100,000 (approximately $60,000).

Singapore has eight free trade zones (FTZs) for sea borne cargo and two for airfreight regulated under the Free Trade Zone Act. The FTZs may be used for storage, repackaging of import an export cargo, assembly and other manufacturing activities approved by the Director General of Customs in conjunction with the Ministry of Finance.

Charities in Singapore are subject to extensive government regulation, including close oversight and reporting requirements, and restrictions that limit the amount of funding that can be transferred out of Singapore. Singapore had a total of 1,747 registered charities as of December 2004. All charities must register with the Commissioner of Charities and submit governing documents outlining the charity's objectives and particulars on all trustees. The Commissioner of Charities has the power to investigate

charities, search and seize records, 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.

Singapore will implement tighter regulations under the Income Tax Act governing public fund-raising by charities beginning January 1, 2007. Charities authorized to receive tax-deductible donations will be required to disclose the amount of funds raised in excess of S$1 million (approximately $600,000), expenses incurred, and planned use of funds. 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 must demonstrate that at least 80 percent of the funds raised will be used in Singapore, although the Commissioner of Charities has discretion to allow for a lower percentage. 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 names of recipients. The government issued 34 permits in 2004 related to fund raising for foreign charitable purposes. There are no restrictions or direct reporting requirements on foreign donations to charities in Singapore.

To regulate 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 184 predicate "serious offenses" listed under the CDSA. The provisions of the MACMA apply to countries whether or not they have concluded treaties, MOUs 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.

In May 2003, Singapore issued a regulation pursuant to the MACMA and the Terrorism Act and 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, it 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. As of December 2005, Singapore, Malaysia, and Vietnam have ratified the treaty. In 2005, Singapore and India signed a similar treaty.

In addition to the UN International Convention for the Suppression of the Financing of Terrorism, Singapore is also party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. In addition to FATF, Singapore is a member of the Asia/Pacific Group on Money Laundering, the Egmont Group, and the Offshore Group of Banking Supervisors. Singapore hosted the June 2005 Plenary meeting of the FATF, the first time a FATF Plenary was held in Southeast Asia. FATF is slated to review Singapore's AML/CFT regime, most likely in 2007.

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 Financial Action Task Force's (FATF) Special Recommendation Nine, adopted in October 2004, that mandates 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. In order to conform to international standards, Singapore should lift its rigid bank secrecy restrictions and significantly increase its list of predicated crimes for money laundering.

Slovakia

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 a suspicious transaction and "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 existing 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 for 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 also 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. Act No. 367/2000 also 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.

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."

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 2004, the BFP (through the FIU) filed 818 reports alleging suspicious business operations totaling $632 million. The BFP submitted 82 proposals for the action of tax authorities and 20 proposals to launch criminal prosecutions worth an estimated value of $1.5 million. During the same period, the Financial Police conducted and/or started 70 on-site inspections of obliged entities, and in 23 cases inspectors levied fines amounting to $75,313. A total of 29 inspections have been completed; of those, no penalties were levied in 22 of the cases. Penalties worth a total value of $21,875 were paid in 6 cases.

During the first eleven months of 2005, the FIU of the OFOC received 1,094 reports alleging unusual financial transactions worth $319.1 million. It submitted eight proposals for criminal prosecution with a value of $455 million and 179 proposals for tax prosecution worth $36.5 million. In addition, the Financial Police regional units submitted 134 proposals for criminal prosecutions. The OFOC conducted or started 93 on-site inspections of "obliged persons" and levied penalties in 33 cases with a total value of $129,063.

In 2003, a law amending and supplementing the Criminal Procedure Code and Criminal Code entered into force. The amendment strengthens the competencies of law enforcement by granting investigators the authority to conduct sting operations and introduces provisions regarding corporate criminal liability. In addition, crown witnesses (a criminal who voluntarily opts to cooperate with law enforcement bodies) are now protected by the law and can 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 draft 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 an amount 200 times the minimum monthly wage 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. Due to widespread public opposition, the Ministry of Justice withdrew the draft law from Parliament in January 2004. However, on June 23, 2005, Parliament nevertheless approved it, and it came into force on September 1, 2005. Despite its approval, the new law was still controversial, and its implementation was frozen by the Constitutional Courts on October 6, 2005.

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 consistent with UNSCR 1373. According to Act No. 367/2000 and its later amendments, financial institutions are required to report to the regional financial police when they freeze or identify suspected terrorist-linked assets. The Government of Slovakia (GOS) has agreed to freeze immediately all accounts owned by entities on the UNSCR 1267 Sanctions Committee's and EU's consolidated lists, but not those of the United States. No terrorist finance-related accounts have been frozen or seized in Slovakia, but were a terrorism-related account to be identified, the Financial Police could 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 a party to all 12 of the UN Conventions concerning the fight against terrorism. However, as reported in its 2004 self-assessment questionnaire on anti-money laundering efforts for the Council of Europe (COE), Slovakia is still not fully compliant with the Financial Action Task Force's (FATF's) Special Recommendations on Terrorist Financing. The COE's Committee of Experts gave Slovakia a rating of "partial compliance" in 2004, with regard to Special Recommendation I (Implementation of UNSCR 1373) and Special Recommendation VII (enhanced scrutiny of transfers lacking originator information).

In late 2005, following its official release, Slovak authorities started to prepare for implementation of the Third EU Money Laundering Directive. The Finance Ministry, the National Bank of Slovakia, and the Ministry of Interior plan to establish an interdepartmental committee in early 2006 to coordinate the modification of Slovak legislation to conform to the new Directive.

In 2002, the GOS ratified 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 is a member of the Egmont Group and has signed 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 2006. 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 in Criminal Matters, 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 Group of States Against Corruption (GRECO), a platform of the Council of Europe to fight against corruption. GRECO reviewed Slovakia for the first time in 2000. The first round evaluation report on Slovakia contained 19 recommendations, of which 15 were satisfactorily addressed by 2003. GRECO evaluated the last four recommendations as "implemented" in October 2005. In late 2003, Slovakia faced additional examination by GRECO. With regards to money laundering, GRECO recommended that "the Slovak authorities undertake a comprehensive and sustained program of specialized professional training for judges, prosecutors and police regarding the effective and appropriate use of criminal and administrative laws relating to money laundering, accounting offenses, and the use of legal persons to shield corrupt activity."

Slovakia is a member of the Council of Europe and has actively participated in MONEYVAL, the Council of Europe's FATF-style regional body, since 1997. Slovakia sends experts to conduct mutual evaluations on fellow member countries; it also underwent mutual evaluations by this group in 1998 and 2001. Slovakia has since implemented changes to its money laundering regime based on the results of these evaluations. In 2005, Slovakia faced a third round of evaluations, which was aimed at assessing its level of compliance with the FATF's Recommendations and the EU's Second Money Laundering Directive. The MONEYVAL report should be released in the first half of 2006.

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 of its non-financial sectors to ensure that 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.

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, nor does it have free trade zones. It does, however, operate Industrial Development Zones (IDZs). The South African revenue service monitors the customs control of these zones. Imports and exports that are involved in manufacturing or processing in the zone are duty-free, provided that the finished product is exported. South Africa maintains IDZs in Port Elizabeth, East London, Richards Bay, and Johannesburg International Airport. The South African Government (SAG) 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) criminalizes 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 May 20, 2005, the Protection of Constitutional Democracy Against Terrorist and Related Activities Act (POCDATARA) came into effect. The Act criminalized terrorist activity and terrorist financing and gave the government investigative and asset seizure powers in cases of suspected terrorist activity. The Act is applicable to charitable and non-profit organizations operating in South Africa. The Act requires financial institutions to report suspected terrorist activity to the South African financial intelligence unit (FIU), the Financial Intelligence Centre (FIC).

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. In addition to the FIC, South Africa has a Money Laundering Advisory Council (MLAC) to advise the Minister of Finance on policies and measures to combat money laundering.

The Financial Intelligence Centre Act (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. Regulated 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, it forwards 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.

During the FIC's first full year of operation, it received 105 information requests from local law enforcement and 56 from international law enforcement agencies. The FIC continued to make progress in 2005 in building its capabilities and in establishing its credibility with the South African law enforcement community. During its most recent fiscal year, it received 92 information requests from local law enforcement and 107 from international law enforcement agencies. The FIC continued to grow significantly during the year and maintained its focus on further analytical training for its staff and the banking community in order to increase the quality of suspicious transaction reports.

From March 2004 through March 2005, the FIC received 15,757 suspicious transaction reports (STRs), more than a 110 percent increase from the previous year's 7,480 STRs. The FIC reports that this increase is due to the development and distribution of its batch-reporting tool. Precise information is not 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 remains uneven, as the FIC and South Africa's banks continue to work to provide effective and comprehensive 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. Certain KYC requirements were waived for low-cost bank account holders when South Africa's banks introduced these accounts in 2004. Reporting requirements were also specifically

waived for brokers assisting clients with a one-time amnesty offer according to the Exchange Control and Amnesty and Amendment of Taxation Laws Act of 2003.

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 within the country; however, the South African Revenue Service (SARS) requires large cash amounts to be declared at entry and exit points.

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. While legislation has been adopted in response to the recommendations, full implementation has not taken place.

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 (FATF), and it holds the FATF Presidency for the period June 2005-June 2006. South Africa is also an active member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body, having signed the memorandum of understanding in 2003.

The SAG is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

The South African Government should implement the FATF Special Recommendation Nine 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 publicly available the number of criminal investigations resulting from STRs, and it should increase the number of actual money laundering prosecutions. It should fully implement the new law (Protection of Constitutional Democracy Against Terrorist and Related Activities Act—POCDATARA) against terrorist activity and terrorist financing.

Spain

Spain is an important money laundering destination for Latin American drug runners and Eastern European criminal syndicates. Criminals of all types launder money by investing in the strong real estate market, particularly in Spain's coastal regions. Moreover, during 2005, Spanish police arrested several individuals reportedly engaged in terrorist financing activities.

Money laundered in Spain is primarily a product of the Colombian cocaine trade, although money from other Latin American countries is also laundered there. Using narcotics proceeds, Colombian companies purchase goods in Asia and sell them legally at cartel-run stores in Spain and other European countries. Drug proceeds from Morocco, Turkey, and other regions also enter Spain. Cash is smuggled in and out of Spain via couriers, luggage, shipping containers, and by small craft operating along Spain's long coastline. Informal non-bank outlets such as "locutorios" make small international transfers for the immigrant community, continually moving money in and out of Spain. Regulators also suspect the presence of hawala-like networks in the Islamic community. Other sources of illicit funds in Spain are tax evasion and smuggling. The smuggling of electronics and tobacco from Gibraltar remains an ongoing issue.

The Government of Spain (GOS) remains committed to combating narcotics trafficking, terrorism, and financial crimes, and continues to work 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 require a prison sentence greater than three years. Amendments to the code on November 25, 2003, made all forms of money laundering financial crimes 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.

In December 1993, specific measures to prevent money laundering were adopted to regulate the legal entities in the financial sector and individuals moving large sums of cash (Law 19/1993). 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 most recently in January 2005 by Royal Decree 54/2005. Pursuant to these laws and regulations, 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 added 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 and under the supervision of appropriate regulators.

Law 19/2003 regulates the movements of capital and foreign transactions and implements parts of Council Directive 2001/97/EC on prevention of the use of the financial system for money laundering (2nd 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 (approximately $35,355). The law also requires the declaration and reporting of internal transfers of funds greater than 80,500 euros (approximately $94,870). Individuals traveling internationally are required to report the importation or exportation of currency greater than 6,000 euros (approximately $7,070). 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. Agencies represented include the National Drug Plan Office, the Ministry of Economy, the Public Prosecutor's Office (Fiscalia), Customs, the Spanish National Police, the Guardia Civil, the National Stock Market Committee, the Treasury, the Bank of Spain, and the Director General of Insurance and Pension Funds. Any member of the Commission may request an investigation.

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 CPBC also delegates responsibility to 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 national government 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 334,452 CTRs in 2004. SEPBLAC has noted an increase in both quantity and quality of suspicious transaction reporting in 2004. The Fund of Seized Goods of Narcotics Traffickers receives seized assets.

Terrorist financing issues are governed by a separate code of law and commission, the Commission of Vigilance against 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 Public Prosecutor's Office and Ministries of Justice and Economy. SEPBLAC serves 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 based on 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 yet been submitted to Spain's Council of Ministers for approval. Once in full effect, this law will allow administrative freezing of suspect assets without a judge's order. Nonetheless, Spain has thus far frozen an estimated 500,000 euro (approximately $590,000) in al-Qaida funds.

Although the sums involved in terrorist financing are low in comparison with the overall money-laundering problem in Spain, it is clear from arrests in 2005 and 2006 that Spain is an important logistical base for global Islamic terrorists. At the same time, 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.

Spanish police and intelligence services are very active in the area of terrorist financing; as of November 2005, Spanish law enforcement officials were engaged in 85 different terrorist financing investigations. In a well-publicized 2005 operation, two Pakistani hawaladars were arrested on terrorism-finance related charges. Other arrests in December 2005 involved 16 suspected Islamic militants in Seville, Malaga, Granada, and Lerida, several of whom allegedly belonged to a "recruitment and financing group."

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

Spain is a member of the FATF, and its head of delegation 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. SEPBLAC is a member of the Egmont Group and is currently chairing the Egmont Group's Outreach Working Group.

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. Spain and its FIU, SEPBLAC, have entered into bilateral agreements for cooperation and information exchange on money laundering issues with a number of countries, including Bolivia, Colombia, Chile, El Salvador, France, Israel, Mexico, Panama, Russia, Turkey, 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 officials work closely with the Spanish customs service, Spanish prosecutors, the national police corps, and the Civil Guard. The U.S. Drug Enforcement Administration works closely with SEPBLAC, the national police, and the Civil Guard. These organizations regularly share information.

The scale and sophistication of money laundering activities in Spain create a very large law enforcement problem. 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.

St. Kitts and Nevis

The Government of St. Kitts and Nevis (GOSKN) is a federation composed of two islands in the Eastern Caribbean; 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.

GOSKN officials were unable to disclose 2005 statistics or information on its financial sector because Parliament has yet to approve the Financial Intelligence Unit's (FIU) Annual Report. The GOSKN did not publicly release statistics for 2004 until mid-year 2005. 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). Figures from 2003 reported that the Nevis domestic financial market consists of five domestic banks, four domestic insurance companies (all of which are subsidiaries of St. Kitts companies), and two money remitters. There are approximately 15,000 international business companies (IBCs) and 950 trusts, with 50 trust and company service providers. 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, 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's 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 the 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. However, an official GOSKN website for offshore finance contends that Nevis-registered companies are not required to divulge beneficial ownership.

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 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. In 2004, the FIU had received 104 SARs. No SAR figures were released for 2005. In 2005, U.S. law enforcement worked with the GOSKN on an investigation which resulted in a seizure of $338,000 from the offshore bank of Nevis.

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.

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.

A mutual legal assistance treaty between SKN 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.