comprehensive anti-money laundering regime that promotes respect the rule of law, willingly shares information with foreign regulatory and law enforcement agencies, is capable of thwarting money laundering and terrorist financing, and maintains compliance with all relevant international standards.

Pakistan

Pakistan is not considered a regional or offshore financial center; however, financial crimes related to narcotics trafficking, terrorism, smuggling, tax evasion and corruption are significant problems. Pakistan is a major drug-transit country. As a result of tighter controls in the financial sector, smuggling, trade-based money laundering, hawala, and physical cross-border cash transfers are the common 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. Pakistan has very little control of the border area, which allows the flow of smuggled goods to the Federally Administered Tribal Areas (FATA) and Balochistan. Goods such as foodstuffs, electronics, building materials, and other products that are primarily exported from Dubai to Karachi are falsely documented as destined for Afghanistan under the "Afghan Transit Trade Agreement," which allows goods to pass through Pakistan to Afghanistan exempt from Pakistani duties or tariffs. Through smuggling, corruption, avoidance of taxes, as well as barter deals for narcotics, many of the goods destined for Afghanistan find their way to the Pakistani black market. The proliferation of counterfeit goods and intellectual property rights violations generate substantial illicit proceeds that are laundered. A group of private, unregulated charities has also emerged as a major source of illicit funds for international terrorist networks. Another issue is the use of madrassas as training grounds for terrorists. The lack of control of madrassas, similar to the lack of control of Islamic charities, allows terrorist organizations to receive financial support under the guise of support of Islamic education.

Money laundering and terrorist financing are often accomplished in Pakistan via the alternative remittance system called hundi or hawala. This system is also widely used by the Pakistani people for informal banking and legitimate remittance purposes. Free trade zones do operate in Pakistan. The government established its first Export Processing Zone (EPZ) in Karachi in 1989 and has subsequently created additional EPZs in the Sindh and Balochistan provinces. Although no evidence has emerged of EPZs being used in money laundering, over-or under-invoicing is common in the region and could be used by entities operating out of these zones. Fraudulent invoicing is typical in hundi/hawala countervaluation schemes.

Pakistan has adopted measures to strengthen its financial regulations and enhance the reporting requirements for the banking sector, in order to reduce its susceptibility to money laundering and terrorism financing. For example, financial institutions must report within three days any funds or transactions they believe are proceeds of criminal activity. However, this is largely not observed by financial institutions because. Pakistan has not yet formally established a Financial Intelligence Unit (FIU) to which such reports of suspicious transactions can be filed. Additionally, there is no safe harbor provision for financial institutions to protect them from civil and criminal liability for filing such reports.

Pakistan has had a comprehensive anti-money laundering law under consideration by its parliament since 2005 although such legislation has not yet been enacted. As a result, the offense of money laundering cannot be prosecuted in Pakistan. Several law enforcement agencies have responsibility to enforce laws against financial crimes. The National Accountability Bureau (NAB), the Anti-Narcotics Force (ANF), the Federal Investigative Agency (FIA), and the Customs authorities all oversee Pakistan's law enforcement efforts. The major laws in these areas include: The Anti-Terrorism Act of 1997, which defines the crime of terrorist finance and establishes jurisdiction and punishments; the National Accountability Ordinance of 1999, which requires financial institutions to report corruption

related suspicious transactions to the NAB and establishes accountability courts; and The Control of Narcotics Substances Act of 1997, which also requires the reporting of narcotics related suspicious transactions to the ANF, contains provisions for the freezing and seizing of assets associated with narcotics trafficking, and establishes special courts for the offenses (including financing) involving illegal narcotics. Because Pakistan lacks a central repository for the reporting of suspicious transactions, due to confusion over which law enforcement agency should receive reports and the lack of protection from liability for reporting, suspicious transactions go largely unreported. The implementing laws for the law enforcement agencies such as NA, ANF, and FIA include provisions to allow investigators to access financial records and conduct financial investigations. However, none of these laws provides for the establishment and funding of a FIU.

Since 2002, the 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 standards. As of November 2006, draft AML legislation has been approved by the Cabinet and is currently being reviewed by the Standing Committee on Finance in the National Assembly. The draft law provides for the establishment of an FIU; however, the bill as it currently stands, does not meet international standards in several key respects. One problem is with the asset forfeiture scheme, particularly where its application is dependent upon a prosecution for the predicate offense. Another issue is with the filing of suspicious transactions reports, where the imposition of a threshold requirement—the minimum transaction amount to trigger a report—has yet to be determined. A provision for the exchange of information with the U.S. on all-source money laundering is contained in the draft AML bill.

The State Bank of Pakistan (SBP) and the Securities and Exchange Commission of Pakistan (SECP) are Pakistan's 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 nonbank financial institutions, has applied "know your customer" regulations to stock exchanges, trusts, and other nonbank 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 hawaladars 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 hawaladars 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 countries' increased awareness and regulation of hawala, post-September 11 changes in the behavior patterns of overseas Pakistanis, and a substantial increase in credit available in the formal financial sector.

Pakistan has criminalized the financing of terrorism under its Anti-Terrorism Act of 1997. It includes the provision that it is a crime to enter into or become part of an arrangement that facilitates retention or control of terrorist property by or on behalf of another person, by concealment, removal from the jurisdiction, transfer to nominees, or in any other way. Pakistan, through the SBP, circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list as being linked with Usama Bin Laden, members of the al-Qaida organization or the Taliban. SBP has the ability to freeze bank accounts and property held by these individuals and entities. However, there have been some deficiencies concerning the timeliness and thoroughness of the asset freezing.

The Ministry of Social Welfare is drafting a Charities Registration Act bill. Under this bill, charities would have to prove the identity of their directors and open their financial statements to government scrutiny. Currently, charities can register under one of a dozen different acts, some dating back to the middle of the nineteenth century. The Ministry hopes that when the new legislation is enacted, it will be better able to monitor suspicious charities and ensure that they have no links to designated terrorists or terrorist organizations. The Act is not expected to be passed during the next year

Reportedly, bulk cash couriers are the major source of funding for terrorist activities. According to the Pakistan Central Board of Revenue, cash smuggling is an offense punishable by up to five years in prison. It is illegal for passengers to carry more than $10,000 per person. It is illegal to bring money into Pakistan except through legal banking channels; however, there are no reporting requirements upon entering the country. There are joint counters at international airports staffed by the SBP and Customs to monitor the transportation of foreign currency. However, enforcement is spotty and corruption rampant.

Pakistan enforces existing drug related asset seizure and forfeiture laws. Pakistan's Anti Narcotics Force shares information about seized narcotics assets and the number of arrests with the USG. Section 12 of the Control of Narcotic Substances Act of 1997 criminalizes the acquisition and possession of assets derived from drug money. The Act also makes it an offense to conceal or disguise the true nature, source, location, disposition, movement or ownership of such assets through false declaration. The suspected assets and properties shall also be liable to forfeiture. The SBP has the ability to freeze assets while the NAB, FIA, and ANF have the ability to seize assets.

Pakistan is an active member of the Asia/Pacific Group on Money Laundering (APG), although its failure to enact an AML law has called into question its commitment to membership, since the terms of reference of APG membership require a country to develop, pass and implement anti-money laundering and antiterrorist financing legislation and other measures based on accepted international standards. In 2005, the APG member states conducted a peer review of Pakistan's AML/CTF laws, rules and procedures. APG representatives identified a number of deficiencies and highlighted the need for a comprehensive AML law.

Pakistan is party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Crime and the UN Convention against Corruption. Pakistan is 142 out of 163 countries monitored in Transparency International's 2006 Corruption Perception Index. Pakistan has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

Five years after draft anti-money laundering (AML) legislation was first drafted, the Government of Pakistan should now 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 work quickly to 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. Per FATF Recommendation Nine, Pakistan should implement and enforce cross-border currency reporting requirements at a reporting threshold level that makes sense given the low-per capita income of the Pakistani people. Customs and financial police should be trained in recognizing trade-based money laundering and value transfer. Pakistan should explore establishing a Trade Transparency Unit (TTU) that will work with its major trading partners to examine trade anomalies that may be indicative of customs fraud and/or trade-based-money laundering. The establishment of a TTU could bring needed revenue streams to the government. 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. Pakistan should take additional steps to address pervasive corruption at all levels of government and commerce.

Palau

Palau is an archipelago of more than 300 islands in the Western Pacific with a population of 20,900 and per capita GDP of about $7,267. 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, securities brokers/dealers or casinos in Palau. The Authorities report that within the last year at least one trust company has been registered, though the scope and size of its business is unknown. 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. Subsequently, Palau has prosecuted three more money laundering cases obtaining convictions in two of the cases. Two of the cases involved domestic proceeds of crime, while one of the cases involved criminal conduct both within and outside of Palau.

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 licensed banks in Palau and all are majority foreign owned. On November 7, 2006, the FIC closed the second largest and the only locally owned bank, Pacific Savings Bank, for illiquidity and insolvency. The Receiver has filed several civil actions against former bank insiders and the litigation is ongoing. An amendment intended to strengthen the supervisory powers of the FIC and promote greater financial stability within Palau's bank market passed its first reading in the Senate in January 2005 but the Senate Committee on Ways and Means and Financial Matters did not report out the bill until December 2006 when the bill was referred back to the Committee for further study.

Other entities subject to the provisions of the MLPCA, such as the three money services businesses, four 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 were introduced in the Senate in 2004 and passed in March 2006. The amendments passed their first reading in the House of Delegates in March 2006 and were referred to the House Committee on Ways and Means and Financial Matters where they remain. 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. The bill passed the Senate in March 2006 and went to the House of Delegates where it passed its first reading in the same month and was referred to the House Committee on Ways and Means and Financial Matters where, once again, it remains.

The Counter-Terrorism bill, which also has anti-money laundering provisions, was originally introduced in September 2002, but was not acted on by the Senate. An amended version of the Bill

was reintroduced in January 2005 and the Senate passed it in January 2006. The bill is in the House of Delegates. 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 nonprofit 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 is particularly vulnerable to money laundering because of its proximity to Colombia and other drug-producing countries. Colombian nationals are able to enter Panama without visas, facilitating the investment of drug money into Panama's economy. 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.

Panama's sophisticated international banking sector, Colon Free Zone (CFZ), U.S. dollar-based economy, and legalized gambling sector are utilized to facilitate potential money laundering. The CFZ serves as an originating or transshipment point for some goods purchased with narcotics proceeds (mainly dollars obtained in the United States) through the Colombian Black Market Peso Exchange. There are approximately 1,400 businesses operating in the CFZ, facilitating opportunities for trade-based money laundering. Reports indicate that the amount of money passing through casinos increased by over 200 percent in 2006. The present construction boom also presents opportunities for money laundering. As many as 150 new high-rise buildings are currently being constructed. Some of the new construction is due to construction tax breaks which ended December 31, 2006.

Panama has the second highest number of offshore-registered companies in the world. Panama's large offshore financial sector includes international business companies, offshore banks, captive insurance companies and fiduciary companies. Law No. 42 of October 2000 requires Panamanian trust companies to identify to the Superintendence of Banks the real and ultimate beneficial owners of trusts. Executive Decree 213 of October 2000, amending Executive Order 16 of 1984 (trust operations), provides for the dissemination of information related to trusts to appropriate administrative and judicial authorities.

Law No. 41 (Article 389) of October 2000 amended 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, and international theft or trafficking of motor vehicles. Law No. 41 establishes a punishment of 5 to 12 years' imprisonment and a fine. In June 2003, the Panamanian Legislative Assembly approved the Financial Crimes Bill (Law No. 45), which established 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 penalties criminalized a wide range of activities related to financial intermediation, including illicit transfers of monies, accounting fraud, insider training, and the submission of fraudulent data to supervisory authorities. Law No. 1 of January 2004 added crimes against intellectual property as a predicate offense for money laundering.

Law No. 42 requires financial institutions to report to Panama's financial intelligence unit (FIU), the Financial Analysis Unit of the Treasury Ministry (Unidad de Análisis Financiero, or UAF), suspicious financial transactions and currency transactions in excess of $10,000. Casinos, CFZ businesses, the national lottery, real estate agencies and developers, and insurance and reinsurance companies are also required report to the UAF currency or quasi-currency transactions that exceed $10,000. Under Law No. 48 of June 2003 and Law No. 16 of May 2005, money remitters and pawnshops are also subject to anti-money laundering regulations. Resolutions Nos. 327 and 328 of August 2004 of the Ministry of Commerce and Industries similarly require promotional companies and real estate agents to identify their clients, declare cash transactions over $10,000, and report suspicious transactions to the UAF.

In October 2000, Panama's Superintendent of Banks issued Agreement No. 9 that defines requirements that banks must follow for identification of customers, exercise of due diligence, and retention of transaction records. It also increased the number of inspections of finance companies it conducted. In 2005, the Superintendence of Banks modified that Agreement, in order to include fiduciary (offshore) companies within the measures of prevention of illegal use and to bring the Banking Center into line with the highest international standards, thus increasing compliance with the Financial Action Task Force (FATF) Recommendations.

The Autonomous Panamanian Cooperative Institute established a specialized unit for the supervision of loans and credit cooperatives regarding compliance with the requirements of Law No. 42. The National Securities Commission carried out numerous training sessions and workshops for its personnel and regulated entities. The CFZ possesses and issues a procedures manual for the users of the CFZ, outlining their responsibilities regarding prevention of money laundering and requirements under Law No. 42. In 2006, the UAF continued efforts to raise the level of compliance for reporting suspicious financial transactions, particularly by nonbank financial institutions and trading companies within 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." This Transparency Program is targeted, through enhanced communication and information flow, training programs and technology, at strengthening the capabilities of those government institutions responsible for preventing and combating financial crimes and terrorist financed activities. Employees from 14 different institutions have received training, including bank compliance officials, and representatives of the private sector, stock markets and credit unions. In addition, Panama has launched an educational campaign to prevent money laundering and terrorist financing. The program began in 2002 and is intended to raise consciousness of citizens regarding these crimes. This program has included hosting a hemispheric congress on the prevention of money laundering in 2004 and 2006.

In 2005, a pilot program was developed for money laundering prevention training, which was financed by the IDB and executed by the Caribbean Financial Action Task Force (CFATF). The training has reached over 5,000 public and private sector employees. Participants have been from various financial institutions, insurance companies, the CFZ and money order companies.

To increase GOP interagency coordination, the UAF and the 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 has enabled the UAF to begin more timely investigations. The creation of a joint airport interdiction task force at Tocumen, made up of members from the Panamanian National Police (PNP), Technical Judicial Police (PTJ), National Air Service (SAN),

Customs and Immigration has produced significant seizures of undeclared currency. In 2006, a total of $4.7 million in undeclared currency was seized. The most significant seizures were in two separate incidents where gold bars painted silver were seized from Mexican nationals traveling from Mexico through Panama en route to Colombia. The Task Force also participated in a continuous operation designed to interdict bulk cash smuggling ("Operation Firewall") in coordination with U.S. Embassy Narcotics Affairs Section and U.S. Immigration and Customs Enforcement (ICE).

Executive Order No. 163 of October 2000, which amended the June 1995 decree that created the UAF, allows the UAF to provide information related to possible money laundering directly to the Office of the Attorney General for investigation. Panama has initiated cases for domestic prosecution, and the UAF routinely transfers cases to the PTJ's Financial Investigations Unit for investigation. During 2006, Panama worked with the United States on two large cases. The first involved a gold and jewelry company in the CFZ that was used to launder money. Assets estimated at over $30 million were seized in connection with this case. The second case was connected to an international narcotics trafficking case in which an entire trafficking organization was taken down. In Panama alone an estimated $25 million in assets were seized. Both cases have ongoing investigations as a result of information obtained. Panama assists other Central American countries with investigations. For example, Panama assisted Nicaragua with the corruption case against former Nicaraguan President Arnoldo Aleman. Panama also assisted Costa Rica and Peru in investigating allegations against high ranking political figures in each country.

Panama 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 devote $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 has signed a cooperation agreement with the Public Registry of Panama.

Terrorist financing is a criminal offense in 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. There are no legal impediments to the GOP's ability to prosecute or extradite suspected terrorists. Public security sources and the judicial system have limited resources to deter terrorists; however, there are several special investigations units capable of carrying out investigations.

In January 2003 the GOP entered into a border security cooperation agreement with Colombia and also increased funds to the Frontier Division of the National Police to assist in border security. The GOP and the Government of Colombia hold quarterly meetings to discuss border security initiatives of mutual interest to the two countries. The GOP has 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 (OAS) to investigate transnational issues, including money laundering. Panama has an implementation plan for compliance with the FATF 40 Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing.

In May 2005, the International Monetary Fund (IMF) conducted an assessment of Panama's Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) under the new FATF methodology. The assessment has also been accepted by the CFATF as its mutual evaluation of Panama. Since its assessment, Panama has taken many steps to implement evaluator's recommendations, including providing adequate training to government officials and issuing new regulations to financial institutions to ensure that they continue filing suspicious transaction reports to the UAF.

The GOP remains active in international anti-money laundering efforts, including the multilateral Black Market Peso Exchange Group Directive. In March 2002, the GOP signed the cooperation agreement issued by the working group as part of a regional effort against the black market system. Panama is a member of the OAS Inter-American Drug Abuse Control Commission (CICAD), and served as the Chair of CFATF and the Central American Council of Superintendents of Banks, Insurance Companies and Other Financial Institutions during 2004 and 2005. Panama is currently the vice-president of the Association of Supervisors of Banks in the Americas (ASBA), with the term running through 2007. The GOP is also a member of the Offshore Group of Banking Supervisors. The UAF is a member of the Egmont Group.

Panama 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, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. Panama is also a signatory to 11 of the UN terrorism conventions and protocols. 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. Executive Decree No. 163 authorizes the UAF to share information with FIUs of other countries, subject to entering into a memorandum of understanding (MOU) or other information exchange agreement. Panama currently has 37 such MOUs with other countries, including the United States.

During 2006, the Government of Panama has continued to make progress in strengthening its anti-money laundering regime. The GOP has been a cooperating partner to the United States and other countries throughout the world in investigating money laundering crimes that have a nexus in Panama. Panama should continue its regional assistance efforts. It should emphasize effective law enforcement actions that address Panama's continuing vulnerabilities such as smuggling, abuse of the real estate sector, trade-based money laundering, and the proliferation of nontransparent offshore companies.

Paraguay

Paraguay is a principal money laundering center, involving both the banking and nonbanking financial sectors. The multi-billion dollar contraband re-export trade that occurs on the borders 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. The GOP successfully prosecuted a major money laundering case in 2006 and has demonstrated an increased willingness to press money laundering charges against defendants notwithstanding the limitations of current laws.

Paraguay is particularly vulnerable to money laundering, as little personal background information is required to open a bank account or to conduct 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 Superintendence 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. A number of cooperatives function effectively as financial institutions and may have as much as 30

percent of financial system assets. These co-ops, as they are known, are not regulated by the Superintendent of Banks but are instead self-regulated. The industry organization charged with oversight—INCOOP—issues guidelines, but does not have regulatory authority to compel compliance with anti-money laundering or prudential measures.

The multi-billion dollar contraband re-export trade that occurs largely in the Triborder Area shared by Paraguay, Argentina, and Brazil facilitates money laundering in Paraguay. 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. The illicit proceeds from these crimes are an additional source of laundered funds. 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. Paraguay has taken some measures to tackle the "gray" economy and to develop strategies to implement a formal, diversified economy. The Ministry of Industry and Commerce's Specialized Technical Unit (UTE), working in close coordination with the Attorney General's Trademarks and Intellectual Property Unit, has effectively opened a number of significant investigations against groups involved in piracy.

On December 6, 2006, the U.S. Department of Treasury designated nine individuals and two entities in the Triborder Area that have provided financial or logistical support to Hizballah. The nine individuals operate in the Triborder Area and all have provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was previously designated by the U.S. Treasury in June 2004 for his support to Hizballah leadership. The two entities, Galeria Page and Casa Hamze, are located in Ciudad del Este and have been used to generate or move terrorist funds. The GOP has publicly disagreed with the designations, stating that the U.S. has not provided any new information that would prove terrorist financing activity is occurring in the Triborder Area.

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 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 defendants 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 nonbanking 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. 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, finance companies, insurance companies, exchange houses, stock exchanges and securities dealers, investment companies, trust companies, mutual and pension funds administrators, credit and consumer cooperatives, gaming entities, real estate brokers, nongovernmental organizations,

pawn shops, and dealers in precious stones, metals, art and antiques 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 received over 3,000 suspicious activity reports from these entities in 2006, a significant improvement over previous years.

The UAF began operating in 1997 within the Secretariat to Combat 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, and as a result, cooperation between SEPRELAD and other government agencies on anti-money laundering issues has improved. Initially reluctant to seek SEPRELAD's assistance due to past weaknesses, most government entities are increasingly prepared to work with SEPRELAD. 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. In 2005 the UAF and the Superintendence of Banks' Risk Control Division, which 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, signed a memorandum of understanding (MOU) 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, which are included in Resolution 233 of 2005.

The UAF is seeking to strengthen its relationship with other financial intelligence units and has signed agreements for information exchange with regional FIUs. 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 2005, finding Paraguay to be noncompliant with counterterrorist financing standards and its legal framework for investigating cases deficient.

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 2004. This legislation has since been broken down and incorporated into three bills emerging through a multi-institutional legal reform commission. Proposed amendments to Paraguay's Penal Code, including enhanced legislation on money laundering, were introduced to Congress in October 2006. The other two bills addressing procedural reform and administrative structures should be introduced in early 2007. The proposed amendments also include legislation criminalizing the financing of terrorism. A bill on terrorist financing had been drafted in 2004, yet was not introduced until the amendments to the Penal Code were proposed.

In addition to confirming the UAF's role as the sole FIU, the new legislation establishes SEPRELAD as an independent secretariat or agency reporting directly to the Office of the President. The amendments to the Penal Code submitted to Congress in October establish money laundering as an autonomous crime punishable by a prison term up to 8 years, terrorism financing up to 15 years and terrorism punishable up to 30 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 maintain registries of large currency transactions that equal or exceed $10,000, in addition to complying with existing suspicious transaction reporting requirements.

Other provisions of the draft bills include penalties for failure to file, falsification of reports, enhanced "know-your-client" provisions, and standardized record keeping for a minimum of five -years. The

UAF will continue to refer cases as appropriate for further investigation by Paraguay's Anti-Drug Secretariat (SENAD) 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 bills further specify 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 investigations 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 legislation is enacted, most judges have little incentive to receive money laundering cases because many believe that sentencing on predicate offenses is sufficient punishment. 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 and designated by the United States as a financier of terrorism—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 case against Lebanese businessman Kassem Hijazi, suspected of having laundered proceeds from illicit activities in the Triborder Area and sending a portion of those funds to support Lebanese Hizbollah activities, is ongoing on the basis on tax evasion charges, not money laundering.

In spite of limitations in prosecuting Barakat and Hijazi, the GOP is making improvements in its ability to successfully investigate and prosecute some money laundering cases. Daniel Fretes Ventre, a former Inspector General under President Wasmosy in the 1990s, was sentenced by an Appeals Court to 12 years in prison and fined $68,000 for money laundering and other crimes on October 24, 2006. Several members of his family were convicted on the same charges. Fretes and his accomplices laundered money through a family-established college and three family-owned businesses. In addition to the above-noted penalties, authorities confiscated 11 family-owned properties in Asuncion and Ciudad del Este. This case represents the most significant money laundering conviction—from less than a handful to date—and reinforces the fact that convictions are possible, although difficult under the current legal framework. Fretes Ventre has appealed this decision to the Supreme Court.

In cooperation with the U.S. Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Paraguay is in the process of developing a Trade Transparency Unit (TTU) that will examine discrepancies in trade data that could be indicative of customs fraud, trade-based money laundering, or the financing of terrorism. 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 counter valuation in transferring value and settling accounts.

Despite its low rating on corruption and other indices that prevented Paraguay from qualifying to participate fully in the Millennium Challenge Account (MCA) Compact Program, Paraguay was invited to participate in the MCA's Threshold Program. In May, Paraguay signed a Threshold Program agreement to receive $34.9 million in assistance to address the problems of impunity and informality, both of which hamper law enforcement efforts and contribute to money laundering. Paraguay's Millennium Challenge Account Threshold Program also supports the continued development of the

"maquila" sector, which comprises businesses operating for export (of either goods or services) that enjoy special tax advantages. Since the GOP stepped up promotion beginning in 2004, the sector has experienced rapid growth. 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 or laws that regulate 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 nonbank 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. 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. The GOP is only just beginning to recognize and address the problem of the international transportation of currency and monetary instruments derived from illegal sources. Recently, though, the commercial banks operating in Paraguay have dropped exchange houses as clients based on pressure from either their home offices or correspondent banks in the United States, which have told them that they would sever the relationship if the banks maintained accounts of exchange houses. The principal state-owned bank was also forced to drop the accounts of the exchange houses rather than lose its correspondent relationship with a U.S. bank.

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. The GOP has worked with the U.S. Treasury and Justice Departments to trace, account for, and seek the return of the $16 million diverted in 2002 to private accounts linked to the family of former President Luis Gonzalez Macchi. However, corruption charges against Macchi were dropped in November after the court failed to meet the deadline for hearing full testimony on the accusations. Under the current interpretation of laws, the GOP has limited authority to seize, or forfeit assets of suspected money launderers. In most cases, assets that the GOP is permitted to, 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 seizure" (which has the same effect as freezing) 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 seizure is set as the amount of liability of the suspect to the government. More recently, SENAD has been permitted to use on a temporary basis assets seized on cases not yet decided provided it pays no maintenance or repair costs. The new anti-money laundering legislation will, when passed, allow prosecutors to recommend that judges seize 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, which is not yet 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. To date, 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 nonprofit 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, terrorist association and terrorist financing. This draft legislation, also incorporated into the legal reforms to Paraguay's penal, procedural and administrative codes, will allow the GOP to conform to international standards on the suppression of terrorist financing. The anti-money laundering provisions of the proposed legal reforms also specifically criminalize money laundering tied to the financing of terrorist groups or acts.

The GOP is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the Inter-American Convention on Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. Paraguay participates in the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) money laundering experts working group, and is a member of GAFISUD and the "3 Plus 1" Security Group between the United States and the Triborder Area countries. The UAF has been a member of the Egmont Group since 1998.

While the Government of Paraguay took a number of positive steps in 2006, 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 legislation that meets international standards and enables law enforcement authorities to more effectively investigate and prosecute money laundering and terrorist financing cases. Paraguay also should continue its efforts to combat corruption and increase information sharing regarding corruption among concerned agencies when and if the corruption issues arises. Paraguay does not have a counterterrorism law or a law criminalizing terrorist financing, and the GOP should take steps as quickly as possible to ensure that comprehensive counterterrorism legislation, including the terrorist financing legislation introduced in October 2006, is passed in the context of the penal and procedural code reform process. Further reforms in the selection of judges, prosecutors and public defenders are needed, as well as reforms to the customs agency 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. The GOP should also enter into a mutual legal assistance treaty with the United States.

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 in recent years. 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, estimates indicate that the cocaine trade generates in a range of one to two billion dollars per year, or up to 2.5 percent of Peru's GDP. 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.

Since 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.

Peru's financial intelligence unit, the Unidad de Inteligencia Financiera (UIF) began operations in June 2003 and today has 48 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. The entities obligated to report suspicious transactions to the UIF within 30 days include banks, 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. The UIF cannot receive STRs electronically; obligated entities must hand-deliver STRs to the UIF. The UIF received 209 STRs in 2004, 796 in 2005 ($442.3 million), and 948 from January through October 2006. 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.

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. These reporting requirements are not being strictly enforced by the responsible GOP entities.

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.

Law 28.306 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. On July 25, 2006, the Government issued Supreme Decree 018-2006-JUS to better implement Law 28.306. The decree introduces the specific legal framework for the supervision of terrorism financing.

Supreme Decree 018-2006-JUS further strengthened the UIF by allowing it to participate in the on-site inspections performed by the supervisors of obligated entities. The UIF may also conduct the on-site inspections of the obligated entities that do not fall under the supervision of another regulatory body, such as notaries, money exchange houses, etc. The new regulations also detail the procedures by which compliance officials can obtain a secret code from UIF in order to maintain the secrecy of their identities. Supreme Decree 018-2006-JUS contains instructions for supervisors with prior UIF approval to establish which obligated entities must have a full-time compliance official (depending on each entity's size, patrimony, etc.), and allows supervisors to exclude entities with certain characteristics from maintaining currency transaction reports. If an obligated entity does not have a supervisor, the aforementioned faculties fall to the UIF. The UIF can also request that a supervisor review an obligated entity that is not under its supervision. The supervisors of the obligated entities must update their internal regulations with the provisions enacted by Supreme Decree 018-2006-JUS.

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 October 31, 2006, the UIF had sent 47 suspected cases (totaling over $565.5 million) of money laundering stemming from STRs to the Public Ministry for investigation (9 in 2006, totaling $13.9 million).Twenty-one of the 47 cases were linked to drug trafficking, seven involved official corruption, six involved tax fraud, and the remaining 13 had fraud, arms trafficking, contraband, kidnapping, or intellectual property violations as the predicate offenses. The UIF has also participated in 18 joint investigations with the Public Ministry. The Public Ministry has so far presented seven money laundering cases to the judiciary (five stemming from STRs and two from the joint investigations), but there have not yet been any convictions.

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. Under Law 28.306, DINANDRO and the UIF may 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, the Superintendence of Banks only regulates money remittances that are done through special fund-transfer businesses (ETFs) that do more than 680,000 soles (about $200,000) in transfers per year, and remittances conducted through postal or courier services are supervised by the Ministry of Transportation and Communications. Informal remittance businesses are not supervised. 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. 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. 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 nonprofit 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 Laden, 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 is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the Inter-American Convention on Terrorism. However, terrorism has not yet been specifically

and correctly established as a crime under Peruvian legislation as mandated by the UN Convention. The only reference to terrorism as a crime is in Executive Order 25.475, which establishes the punishment of any form of collaboration with terrorism, including economic collaboration. There are several bills pending in the Peruvian Congress concerning the correct definition of the crime of terrorist financing. Peru is also 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 the Egmont Group of financial intelligence units. Although an extradition treaty between the U.S. Government and the GOP entered into force in 2003, there is no mutual legal assistance treaty or agreement between the two countries.

The Government of Peru has made 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. There are a number of bills under review in the Peruvian Congress that would lift bank secrecy provisions for the UIF in matters pertaining to money laundering and terrorist financing. Although there is an Executive Order criminalizing terrorist financing, Peru should also pass legislation establishing this particular crime. The Congress is also considering bills regarding the obligation of nongovernmental organizations to report the origins of their funds. 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 chemicals used in narcotics production in the Philippines are purchased using letters of credit. U.S. dollars are the preferred currency for international narcotics transactions. Drugs circulated within the Philippines are usually exchanged for local currency. Remittances and cash smuggling are also sources of money laundering.

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 $60,000); 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 enacted 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 nonbank 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, evaluating covered and suspicious transactions and investigating reports for possible criminal activity. 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 allowed AMLC to electronically receive, store, and search CTRs filed by regulated institutions. Through 2006, the AMLC had received more than 6200 suspicious transaction reports (STRs) involving 13,474 suspicious transactions, and had received over 72 million covered transaction reports (CTRs). AMLC recently acquired 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 90 prosecutions underway in the Philippine court system that involved AMLC investigations or prosecutions, including 33 for money laundering, 22 for civil forfeiture, and the rest pertaining to freeze orders and bank inquiries. Although some of these cases may conclude shortly, the Philippines had its first conviction for a money laundering offense in early 2006.

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 2006, the AMLC has frozen funds in excess of 500 million Philippine pesos (approximately $10,000,000).

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.

The AMLC continues to work to bring the numerous foreign exchange offices in the country under its purview. 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. This requirement reduced the number of foreign exchange dealers dramatically as many offices chose to close down rather than seek licensing. The remaining exchange dealers around the country have participated in more than 1500 training programs sponsored by the AMLC. 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.

In 2006, the AMLC requested 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 15 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 in the Philippines, though the country is a growing location for internet gaming sites that target overseas audiences in the region.

The Philippines has over 5,000 nongovernmental organizations (NGOs) that do not fall under the requirements of the AMLA. Charitable and nonprofit 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 seven 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 15 percent during the first ten months of 2006, and should exceed $12 billion for the year, equal to 10 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 (APG) and hosted the 9th annual APG plenary in July, 2006. The Philippines FIU 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 and to all 12 international conventions and protocols related to terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism). The Anti-Money Laundering Council must obtain a court order to freeze assets of terrorists and terrorist organizations placed 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. Although the Philippine House passed its version of the Anti-Terrorism Law in April 2006, the Senate version remains stalled due to political infighting and fear the government could use certain provisions against political opponents.

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 noncombatant 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 separate 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 each year. The Government of Poland (GOP) estimates that the unregistered or gray economy, used primarily for tax evasion, may be as high as 13 percent of Poland's $330 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 March 2006, 54 commercial banks were licensed for operation in Poland, as were 585 "cooperative banks" that primarily serve the rural and agricultural community. The GOP considers the nation's banks, insurance companies, brokerage houses, and casinos to be important venues of money laundering. 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. Money laundering through trade in scrap metal and recyclable material is also a newly

emerging trend. It is also believed that some money laundering in Poland originates in Russia or other countries of the former Soviet Union.

The genesis of Poland's anti-money laundering (AML) regime was November 1, 1992, when the President of the National Bank of Poland issued an order instructing banks how to deal with money entering the financial system through illegal sources. The August 29, 1997 Banking Act was followed by a 1998 Resolution of the Banking Supervisory Commission, adding customer identification requirements and instructions on registering transactions exceeding a certain threshold.

On November 16, 2000, a law went into effect that improves Poland's ability to combat money laundering (entitled the Act of 16 November, or the Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources and on Counteracting the Financing of Terrorism, as amended). 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 cash and suspicious transactions. 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.

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 to the Act of 16 November that broadened the definition of money laundering to encompass all serious crimes. In March 2003, Parliament further amended the law to broaden the definition of money laundering to include assets originating from illegal or undisclosed sources.

A major weakness of Poland's initial money laundering regime was that it did not cover many nonbank 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 (approximately $1,200) 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, and the Polish Bar has mounted a challenge to some provisions, and submitted a motion to the Constitutional Tribunal to determine the consistency of certain regulations with ten articles in the Polish Constitution.

In 2002, Parliament adopted measures to bring the nation's anti-money laundering legislation into compliance with EU standards. Poland's customs law was amended in order to require the reporting of any cross-border movement of more than 10,000 euros (approximately $12,000) in currency or financial instruments. Also, in addition to requiring that the GIIF be notified of all financial deals exceeding 15,000 euros (approximately $19,000), 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. During its first three years of operation, the GIIF received 3,326 suspicious transaction reports (STRs) which resulted in the development of 370 cases by the Prosecutor's Office. In 2005 and 2006, the number of STRs received by the FIU continued to increase with a total of 1,558 reports forwarded to the FIU, resulting in the development of 175 cases by the Prosecutor's Office. Between January and October 2006, the GIIF received more than 1,200 STRs, resulting in the creation of 182 cases with violations exceeding $210 million. Banks filed ninety percent of the STRs submitted in 2005. At a minimum, all reports submitted by the GIIF to the Prosecutor's Office have resulted in the instigation of initial investigative proceedings. In 2005, the number of convictions for money laundering exceeded 30, a number of which were connected with fuel smuggling. There were four convictions under the money laundering law in 2004. Many of the investigations begun by the GIIF have resulted in convictions for other nonfinancial offenses. The GIIF receives approximately 1.8 million reports per month on transactions exceeding the threshold level.

The vast majority of required notifications to the GIIF are sent through a newly developed electronic reporting system. The system is very well developed and is considered to be one of Europe's finest electronic reporting systems, collecting more information than the paper version of the report. 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 efficient processing and analyzing of the large number of reports that are sent to the GIIF continues 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 has initiated work on a specialized IT program that will support complex data analysis and improve the FIU's efficiency in handling the increasing number of reports which it receives.

The GIIF also conducts on-site training and compliance monitoring investigations. In 2005, the GIIF carried out 25 compliance investigations, an increase over the 15 completed in 2004, and received several hundred follow-up reports from institutions responsible for routinely supervising covered institutions. The GIIF has also 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. In 2005, 3,443 individuals (mainly from obligated institutions) participated in the GIIF's new electronic learning course, with a total of 3,032 individuals passing the final test. 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 2005, it sent official requests to foreign financial intelligence units on 155 cases concerning 284 national and foreign entities suspected of money laundering, while foreign FIUs sent 59 requests to the GIIF, concerning 164 national and foreign entities suspected of attempting to launder proceeds from crime. The most

intensive exchange of information was conducted with the United States: In 2005 GIIF submitted 31 requests to the financial intelligence of the United States. The GIIF also actively exchanges with the German, Russian, British, and Ukrainian financial intelligence units.

The total number of suspected transactions sent by obliged institutions in 2005 was approximately 70,000. 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 2005, the GIIF suspended five transactions worth $500,000 and blocked 34 accounts worth $ 11 million. In 2006, the GIIF suspended four transactions worth $2.3 million and blocked 85 accounts worth $12.36 million.

The GOP has created an office of counterterrorist operations within the National Police, which coordinates and supervises regional counterterrorism units and trains local police in counterterrorism measures. Poland also has 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 as is required by UNSCR 1373, 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 continues to work on draft amendments to the criminal code that would criminalize terrorist financing as well as elements of all terrorism-related activity.

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). In 2006, MONEYVAL conducted its third round mutual evaluation of Poland. 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. In 2005, Poland twice hosted law enforcement, FIU and financial sector supervisors from the Former Yugoslav Republic of Macedonia on study visits designed to increase the operational capacities of the agencies and the people staffing them.

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 33 MOUs between 2002 and 2005. The MOU between the Polish FIU and the U.S. FIU was signed in fall 2003. The FIU is also currently in the process of negotiating MOUs with FIUs in Canada, Argentina, Turkey, Serbia and Montenegro, Belarus, China and Taiwan. 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. Poland is also a party to 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 to implement a comprehensive anti-money laundering regime that meets international standards. Further improvements should 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, as it is obligated to do as a party to the UN International Convention for the Suppression of the Financing of Terrorism.

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 nonfinancial institutions have a mandatory requirement to report all suspicious transactions to the Public Prosecutor regardless of threshold amount. The October 2006 Financial Action Task Force (FATF) Mutual Evaluation of Portugal stated, "the Portuguese legal framework for combating money laundering and terrorist financing is generally comprehensive." The report notes that the Portuguese confiscation and seizure system is also "generally comprehensive."

Act 11/2004, which implements the European Union's Second Money Laundering Directive, broadened the GOP's anti-money laundering regime. 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. Portugal employs an all-crimes approach to the predicate offense. "Tipping off" is prohibited and liability protection is provided for regulated entities making disclosures in good faith. Despite Law 5/2002, Article 2, which waives banking secrecy in cases related to organized crime and financial crime, in practice 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 until 2004.

If a regulated entity has knowledge of a transaction likely to be related to a money laundering offense, it must inform the GOP, which 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 must identify their customers, maintain records for a minimum of ten years, and demand written proof from customers regarding the origins and beneficiaries of transactions that exceed 12,500 euros (approximately $16,533). Nonfinancial 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.

However, the 2006 FATF mutual evaluation team reported that the mechanism for determining the beneficial owner does not fully comply with FATF requirements. The National Registry of Legal Persons does not include all information to reveal the beneficial owners of legal persons. Requirements for obliged entities to identify beneficial owners are located in instructions and regulatory standards set forth by the Bank of Portugal (BdP) and the Portuguese Insurance Institute (ISP), and not stipulated by law as required by the Methodology; this raises the question of whether these regulations could be considered secondary legislation or other enforceable means. For some entities in the securities sector subject to the Securities Market Commission (CMVM) regulations rather than those from the BdP, the CMVM regulations do not explicitly comply with requirements regarding the identification of the beneficial owners of legal persons.

Decree-Law 295/2003 of November 2003 sets out reporting requirements for the transportation across borders of cash, nonmanufactured gold, and certain negotiable financial instruments, such as travelers' checks. When a person travels across the Portuguese border with more than 12,500 euros worth of such assets, a declaration must be made to Portuguese customs officials. The GOP expects to approve by year's end national legislation per EC Regulation 1899/2005 to more tightly control the movement of cash across borders.

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 facilitate enforcement of other financial crimes as well.

With regard to nonbanking financial institutions, namely financial intermediaries, the Portuguese Securities Market Commission issued 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 June 30 of the following year. The regulation entered into force on January 1, 2006. Regulation 2/2006 entered into force on May 26, 2006, further amending Regulation 12/2000, Articles 36 and 36-A (concerning internal auditing and supervision), to require additional information.

The three principal 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 regulated entities, which include casinos, realtors, dealers in precious metals and stones, accountants, notaries, statutory auditors and registry officials. Attorneys and solicitadores became obliged entities in 2004.

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 operates independently as a department of the Portuguese Judicial Police (Polícia Judiciária). The UIF is comprised of 28 persons and 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. All suspicious transaction reports (STR's) received by the UIF come from the Attorney General's office, as that office is the designated competent authority to receive STRs. At the international level, UIF coordinates with other FIUs. The UIF has policing duties but no regulatory authority.

In 2002, obligated entities filed 166 STRs. In 2005, they had filed 330 STRs and 44,165 currency transaction reports (CTRs). From January to September 2006, UIF received 391 STRs and 13,806 CTRs. Credit institutions and the Central Bank were the source of the vast majority of STRs, with the former submitting 346 and the latter 25. Portugal's Gambling Inspectorate General was the source of 12,599 CTRs, as it reports all transactions at casinos above a certain threshold. In this same time period, UIF sent 203 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. Twelve cases resulted in proposals to freeze assets involving over 17 million euro (approximately $22.5 million).

The FATF mutual evaluation report noted that sixteen persons were found guilty and convicted of money laundering from 2002 to 2005, receiving penalties ranging from one year to eight and one-half years' imprisonment. The GOP has not yet released statistics on arrests or prosecutions for money laundering or terrorist financing in 2006. However, the media reported in November that the Judicial Police detained seven individuals suspected of belonging to a money laundering network in 2006. Portuguese authorities believe these individuals were involved in the transfer of funds generated by illegal activities in Mozambique, Angola, and Dubai.

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 offense occurs 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. 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. It also addresses the criminal liability of legal persons regarding terrorism financing. However, the legislation does not extend the customer due diligence practices to risk association with terrorism financing. While the broadly-worded law covers both illicit and licit funds that support a terrorist act or organization, it does not extend coverage to the provision of funds to an individual terrorist. 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. Names of individuals and entities included on the United Nations Security Council Resolution 1267 Committee's consolidated list, or that the United States and EU have linked to terrorism, are passed to private sector entities 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. While Portugal does not have an administrative procedure to freeze assets independently of the relevant EU directive, judicial procedure exists for the Public Prosecutor to open

a special inquiry and to freeze assets at the request of a foreign country. To date, no significant assets have been identified or seized. In its 2006 report on the mutual evaluation of Portugal, the FATF noted that it found "deficiencies in scope and time" as related to the freezing of terrorism-related funds.

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, similar to international business corporations, account for approximately 6,500 companies registered in Madeira. 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. There is no indication that MIBC has been used for money laundering or terrorist financing.

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.

According to the FATF mutual evaluation report, Portugal has undertaken many mutual legal assistance obligations, especially with regard to identification, seizure and confiscation of assets. Portugal is a member of the Council of Europe, the European Union, and the FATF. The GOP 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 has signed, but not yet ratified, the UN Convention against Corruption. Portugal is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Portugal's FIU 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, and steps taken in 2003 extended the regime's reach to terrorist financing. Legislative measures adopted in 2004 have consolidated the anti-money laundering legal framework, imposing on financial and nonfinancial institutions obligations to prevent the use of the financial system for the purpose of money laundering. The GOP continued to implement these measures in 2006 to effectively combat money laundering and terrorist financing. However, Portugal should collect and maintain more information and data regarding the number of money laundering and terrorism financing investigations, prosecutions and convictions as well as the amount of property and assets frozen, seized and confiscated as it relates to money laundering and terrorism financing. The GOP should work to correct any identified deficiencies regarding its asset freezing and forfeiture regime, improve its mechanisms to determine the beneficial owners, and ensure that the terrorism financing law covers financing to individuals. Lastly, the FIU should be the competent authority to receive and analyze all STRs.

Qatar

Qatar has a 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 16 licensed financial banks, including three Islamic banks and a specialized bank, the Qatar Industrial Development Bank. Qatar Financial Centre (QFC) allows

major international financial institutions and corporations to set up offices and operate in a "free zone" environment. The QFC allows full repatriation of profits and 100 percent foreign ownership. Qatar has 19 exchange houses, three investment companies and one commercial finance company. Although Qatar still has a cash-intensive economy, authorities believe that cash placement by money launderers is a negligible risk due to the close-knit nature of the society 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, 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 fines and penalties of imprisonment of five to seven years. The law expanded the powers of confiscation 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. Article Two includes any activities related to terrorist financing. Article 12 authorizes the Central Bank Governor to freeze suspicious accounts for 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.

The law requires all financial institutions to report suspicious transactions 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 the State of 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 QCB and includes members from the Ministries of Interior, Civil Service Affairs and Housing, Economy and Commerce, Finance, Justice, Customs and Ports Authority and the State Security Bureau.

In February 2004, the Government of Qatar (GOQ) 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 crime. Qatar has a national committee to review the consolidated UN 1267 terrorist designation lists and to recommend any necessary actions against individuals or entities found in Qatar.

The QCB updates regulations regarding money laundering and financing of terrorism on a regular basis, in accordance with international requirements. The Central Bank aims to increase the awareness of all banks operating in Qatar with respect to anti-money laundering efforts by explaining money laundering schemes and monitoring suspicious activities.

In October, 2004, the GOQ established a Financial Intelligence Unit (FIU) known as the Qatar Financial Information Unit (QFIU). The FIU is responsible for receiving and reviewing all suspicious and financial transaction reports, identifying 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 if suspicious transactions or financial activities of concern are identified. The FIU also obtains additional information from the banks and other government ministries. The QCB, Public Prosecutor and the Criminal Investigation Division (CID) of the Ministry of the Interior work together with the FIU to investigate and prosecute money laundering and terrorism finance cases. The FIU also coordinates closely with the Doha Securities Market (DSM) to establish procedures and standards to monitor all financial activities that occur in Qatar's stock market. The FIU coordinates the different regulatory agencies in Qatar. The Qatari FIU became a member of the Egmont Group in 2005.

In December 2004, QCB installed a central reporting system to assist the FIU in monitoring all financial transactions made by banks. All accounts must be opened in person. Banks are required to know their customers; the banking system is considered open in that in addition to Qatari citizens and legal foreign residents, nonresidents can open an account based on a reliable recommendation from his or her primary bank. Hawala transactions are prohibited by law in Qatar.

The Qatar Authority for Charitable Works monitors all charitable activity in and outside of Qatar. 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 nongovernmental 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 also regulates domestic charity collection.

Qatar does not have cross-border reporting requirements for financial transactions. Immigration and customs authorities are reviewing their policies in expanding their ability to enforce money declarations and detect trade-based money laundering.

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 one of the original signatories of the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENA-FATF), a FATF-style regional body that promotes best practices to combat money laundering and terrorist financing in the region.

The Government of Qatar has demonstrated a willingness to fight financial crimes, including terrorist financing, and to work cooperatively with other countries in doing so. Per FATF Special Recommendation Nine, Qatar should initiate and enforce in-bound and out-bound cross-border currency reporting requirements. The data should be shared with the FIU. The government should continue to work to ensure that law enforcement, prosecutors, and customs authorities receive the necessary training and technical assistance to improve their capabilities in recognizing and pursuing various forms of terrorist financing, money laundering and other financial crimes. Qatar should publish the number of annual money laundering investigations, prosecutions, and convictions. 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 central bank, the National Bank of Romania, estimates the dollar amount of financial crimes to range from $1 billion to $1.5 billion per year. Value-added tax (VAT) fraud has fallen to below 10 percent (down from 45 percent in previous years) of this total. Trans-border smuggling of counterfeit goods, fraudulent bankruptcy claims, tax fraud, and fraudulent claims in relation to consumer lending are additional types of financial crimes prevalent in Romania. Romania also has one of the highest occurrences of online credit card fraud in the world.

Laundered money comes primarily from international crime syndicates who conduct their criminal activity in Romania and subsequently launder their illicit proceeds through false limited liability companies. Another source of laundered money is the proceeds of illegally smuggled goods such as cigarettes, alcohol, coffee, and other dutiable commodities. Widespread corruption in Romania's

customs and border control and as well in several neighboring Eastern European countries also facilitates money laundering.

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, suspicious transaction reporting, and currency transaction reporting for transactions (including wire transfers) over 10,000 euros. The list of entities covered by Law No. 21/99 includes banks, nonbank financial institutions, attorneys, accountants, and notaries. 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.

In December 2002, Romania issued modifications to its anti-money laundering law with the passage of the Law on the Prevention and Sanctioning of Money Laundering (Law 656/2002). This law changed the list of predicate offenses to an all crimes approach. The 2002 law also expanded the number and types of entities subject to anti-money laundering (AML) regulations. Some of these new entities include art dealers, travel agents, privatization agents, postal officials, money service businesses, and real estate agents. Even though nonbank financial institutions are covered under Romania's money laundering law, regulatory supervision of this sector is weak and not nearly as rigorous as that imposed on banks.

In July 2005, Romania's money laundering law was further modified by the passage of 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 modified law also responds to Financial Action Task Force (FATF) Recommendations and establishes an STR reporting requirement for transactions linked to terrorist financing.

During 2006, several changes were made in Romania's laws in order to bring the country into harmony with FATF recommendations and EU Directives. Specifically, laws were changed to allow an increase in the level of fines in correspondence with the inflation rate; use of undercover investigators; reports to be sent from the FIU to the General Prosecutor's Office in an unclassified manner so that they may be used in operational investigations; confiscation of goods used in or resulting from money laundering activities; an increase in the length of time that bank accounts may be frozen from ten days up to one month.

In keeping with new international standards, Romania has taken steps to strengthen its know-your-customer (KYC) identification requirements. Romania has implemented KYC regulations that mandate identification of the client upon account opening and when single or multiple transactions meet or approach 10,000 euros (approximately $13,000). In December 2003, Romania's central bank, the National Bank of Romania (BNR), introduced Norm No. 3, "Know Your Customer." This regulation strengthens information disclosure for outgoing wire transfers and correspondent banking by requiring banks to 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. In 2006, the BNR widened the scope of its KYC norms by extending their application to all other nonbanking financial institutions falling under its supervision. In 2005, the Insurance Supervision Commission instituted similar regulations for the insurance industry.

Romania's financial intelligence unit (FIU), the National Office for the Prevention and Control of Money Laundering (NOPCML), was established in 1999. All currency transaction reports and

suspicious transaction reports must be forwarded to the FIU. The FIU oversees the implementation of anti-money laundering guidelines for the financial sector and works to ensure that adequate training is provided for all domestic financial institutions covered by the law. The FIU is also authorized to participate in inspections and controls in conjunction with supervisory authorities, having carried out 118 on-site inspections during the first ten months of 2006. In July 2006, the FIU Board issued regulations implementing KYC standards for nonfinancial reporting agencies that are not the subject of supervision by other national authorities. These norms are consistent with EU Directives and allow the FIU to increase supervision of entities (casinos, notaries, real estate brokers) previously unsupervised for compliance with AML regulations.

In 2006, the FIU received 46,725 currency transaction reports detailing 8,377,762 transactions exceeding the reporting threshold of 10,000 Euros. Of these transactions, 3.9 percent were carried out by individuals; the remainder was carried out by corporate entities. During the same period, the FIU also received 6,054 reports of foreign banking transfers detailing 753,674 transactions that exceed the reporting threshold. Of these transactions, 5.1 percent were carried out by individuals and the rest by corporations. The total number of suspicious transactions reported to the FIU dropped slightly from 2,826 in the first ten months of 2005 to 2,296 in the first ten months of 2006. Of this figure, reporting by banks and other credit institutions dropped from 1,993 in the first ten months of 2005 to 1,756 in the first ten months of 2006. During the first ten months of 2006, the FIU suspended two suspicious transactions totaling $9.65 million and levied fines totaling $81,273.

Upon completion of its analysis, the FIU forwards its findings to the appropriate government agency for follow-up investigation. During the first ten months of 2006, the number of files sent to the General Prosecutor's Office on suspicion of money laundering was 124, compared to 411 in 2005 and 501 in 2004. During the first ten months of 2006, the number of files sent to the National Anti-Corruption Department on suspicion of money laundering was seven, compared to 41 notifications in the first ten months of 2005, and 22 in 2004. With regard to terrorism financing, the FIU did not send any files to the Romanian Intelligence Service (SRI) during the first ten months of 2006. The FIU also sent six notifications to the Police General Inspectorate, three to the Financial Guard and three to the National Agency for Fiscal Administration in the first ten months of 2006.

Efforts to prosecute these cases have been hampered by a lack of specialization and technical knowledge of financial crimes within the judiciary. Moreover, coordination between law enforcement and the justice system remains limited. Between January 1, 2006 and December 31, 2006, 102 defendants were indicted by the Directorate for the Investigation of Organized Crime and Terrorism Offences (DIICOT) in 22 cases involving money laundering. Between January 1, 2006 and September 30, 2006, four persons received final convictions and one person was acquitted on charges originating in previous years. A conviction is not final in Romania until all appeals remedies have been exhausted.

Since its establishment, the NOPCML has had to deal with numerous operational and political challenges. However, in June 2004, the standing of Romania's FIU began to improve when the Government of Romania (GOR) appointed a new director to head the FIU. The new director significantly improved the office's operational efficiency and brought greater visibility to the importance of AML and counterterrorism financing CTF efforts in Romania. Some significant improvements made include the approval of a new organizational structure for the FIU (as mandated by Governmental Decision No. 1078/2004), as well as the passage of legislation that was designed to improve the procedures for analyzing STR information and the suspension of suspicious accounts and transactions.

In February 2006, the GOR again appointed a new director to head the FIU. The new director and the FIU's supervisory board have worked to improve the quality of cases forwarded to prosecutors for judicial action. While the number of cases forwarded to the General Prosecutor's Office in 2006 has declined, the FIU believes that the number of indictments, and eventually convictions, will increase as

the FIU has started to place a greater emphasis on the quality of reports produced as opposed to the quantity of reports forwarded to the Prosecutor's Office. In April 2006, the GOR approved a new organizational charter for the FIU that established a new division (Legal, Methodology, and Control Department) within the FIU and also allowed an increase in the FIU's staff from 84 to 120 people. In July 2006, the FIU moved to new facilities that will better accommodate staff growth and provide improved infrastructure for resource enhancements and security.

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 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 central bank, and the FIU. The GOR has also set up an inter-ministerial committee to investigate the potential use of the Romanian financial system by terrorist organizations.

The GOR announced a national anticorruption plan in early 2003 and passed a law criminalizing organized crime in April 2003. A new Criminal Procedure Code was passed and entered into force on July 1, 2003. The new Code contains provisions for authorizing wiretaps and intercepting and recording telephone calls in money laundering and terrorist financing cases.

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 GOR, and particularly the central bank, 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. 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 frozen. The FIU 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 central bank 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 for the forfeiture of assets used or provided to terrorist entities, together with finances resulting from terrorist activity. To date, no terrorist financing arrests, seizures, or prosecutions have been carried out.

The GOR recognizes the link between organized crime and terrorism. Romania is a member of and host country for the headquarters of the Southeast European Cooperative Initiative's (SECI) 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 FIU is a member of the Egmont Group and participates as a member in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). 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. The FIU has signed bilateral memoranda with Spain, Belgium, Poland, Czech Republic, Austria, Croatia, Slovenia, Italy, Serbia, Greece, Bulgaria, Ukraine, Turkey, South Korea, and Thailand. The NOPCML is currently working on finalizing an MOU with the United States. In an EU project completed in July 2005, the FIU worked closely with Italy to improve its efficiency and effectiveness.

Although Romania's AML legislation and regulations are comprehensive in scope, implementation lags. The FIU has improved in its ability to report and investigate cases in a timely fashion, and has improved the quality of its reporting. However, these investigations have resulted in only a handful of successful prosecutions to date. With the conclusion of the Romanian capital account liberalization in 2006, the risk of money laundering through nonbanking entities will increase. Romania should continue its efforts to ensure that nonbank financial institutions are adequately supervised and that the sector is trained on identification of suspicious transaction and reporting and record-keeping responsibilities. Romania should continue to improve communications between reporting and monitoring entities, as well as between prosecutors and the FIU. There is an over-reliance on financial reporting to initiate investigations. More effort should be made by Romanian law enforcement and customs authorities to recognize money laundering. Increased border enforcement and antismuggling measures are necessary. 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. Romania should take specific steps to combat corruption in commerce and government.

Russia

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. 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 occur. Experts believe that most of the illicit funds flowing through Russia derive from domestic criminal or quasi-criminal activity, including evasion of tax and customs duties and smuggling operations. Despite making progress in combating financial crime, 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 with low public confidence in it, and under-funding of

regulatory and law enforcement agencies. However, due to rapid economic growth in various sectors, the number of depositors has steadily been increasing.

Russia has recently changed its laws to allow direct foreign ownership and investment in Russian financial institutions. Net private capital inflows for 2006 amounted to $41.6 billion according to the Russian Central Bank, an increase from $1.1 billion in 2005. In contrast to the capital flight that occurred during the 1990s, the majority of more recent outflows involved the legitimate movement of money to more secure and profitable investments abroad, which reflects the maturing of the Russian business sector. However, a portion of this money undoubtedly involved the proceeds of criminal activity. According to official statistics, the trend toward net capital inflows involves the transfer of assets from tax havens, such as Cyprus and the Virgin Islands, previously known to be popular destinations for Russian capital outflows in the 1990s.

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, respectively. Law RF 115-FZ obligates banking and nonbanking 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, institutions legally required to report include: banks, credit organizations, securities market professionals, insurance and leasing companies, the federal postal service, jewelry and precious metals merchants, betting shops, and companies managing investment and nonstate pension funds. Amendments to the law that came into force on August 31, 2004 extend the reporting obligation to real estate agents, lawyers and notaries, and to 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).

Various regulatory bodies ensure compliance with Russia's anti-money laundering and counterterrorism finance laws. 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 nongovernmental 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 (AML) 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. Banks must also adopt internal compliance rules and procedures and appoint compliance officers. The amendment to Law 115-FZ has required banks to identify the original source of funds and to report to the financial intelligence unit (FIU) all suspicious transactions since July 2004. 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.

All obligated financial institutions must monitor and report to the government: any transaction that equals or exceeds 600,000 rubles (approximately $22,700) 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.

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 when conducting specific transactions. The CBR has also raised the standards for offshore financial institutions, resulting in a reduction in the number of such institutions. 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, as nominee or anonymous directors are prohibited under Russian law. 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 removing 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.

Article 8 of Law 115-FZ provides for the establishment of Russia's FIU, called the Federal Service for Financial Monitoring (FSFM). FSFM is an independent executive agency administratively subordinated to the Ministry of Finance. All financial institutions with an obligation to report certain transactions must report the required information to the FSFM. The FSFM is also the regulator for the real estate and leasing, pawnshops, and gaming services sectors. An administrative unit, it has no law enforcement investigative powers. Depending on the nature of the activity, the FSFM provides information to the appropriate law enforcement authorities for further investigation, i.e., the Economic Crimes Unit of the Ministry of Interior (MVD) for criminal matters, the Federal Drug Control Service (FSKN) for narcotics-related activity, or the Federal Security Service (FSB) for terrorism-related cases.

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, comprised of twelve ministries and government departments. In addition to receiving, analyzing and disseminating information from the reporting entities, the FSFM has the responsibility of implementing the state policy to combat money laundering and terrorism financing. The Interagency Commission is chaired by the head of the FSFM and is responsible for monitoring and coordinating the government's activity on money laundering and terrorism financing. FSFM authorities credit cooperation among Commission members for the conviction of 257 individuals on money laundering charges between January and June 2006.

Nearly 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 $8 billion in the first three quarters of 2006. The FSFM receives

approximately 30,000 transaction reports daily. Of these daily reports, 25 percent result from mandatory (currency) transaction reports, and 75 percent relate to 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 centers throughout Russia (St. Petersburg, Ekaterinburg, Nizhny Novgorod, Khabarovsk, Novosibirsk and Rostov-on-Don). The territorial offices coordinate with regional law enforcement and other authorities to enhance the 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, nonstate pension funds, gambling businesses, real estate agents, lawyers and notaries, persons rendering legal/accountancy services, and sellers of precious metals and jewelry.

During the first eight months of 2006, the FSFM carried out 2,700 financial investigations, referring 1,050 of them to law enforcement agencies for possible criminal investigations. According to the MVD, in the first half of 2006 Russian law enforcement investigated 6,300 cases of money laundering, sent 3,500 of the cases to court, and convicted 257 individuals on money laundering charges. Both the FSFM and MVD report that the number of suspicious transaction reports in 2006 has grown nearly ten-fold over the previous year, an increase which both agencies attribute to a greater focus government-wide on financial crimes and terrorism financing.

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 counter narcotics and economic crimes. This division cooperates closely with the FSFM in pursuing narcotics-related money laundering cases. From January through August 2006, the FSKN reportedly initiated 1,332 money laundering cases and referred over 340 of these cases to the General Procuracy for prosecution. 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. Through September 2006, the CBR revoked the licenses of 48 banks for failing to observe banking regulations. Of these, 25 banks lost their licenses for violating Russia's anti-money laundering laws. First Deputy Chairman Andrey Kozlov led the CBR's efforts to implement stronger anti-money laundering guidelines until his assassination in September 2006. He worked to implement the managerial and reporting requirements that made license revocation politically feasible, and had taken steps to prohibit individuals convicted of money laundering from serving in leadership positions in the banking community. This latter issue remains pending with the CBR. President Putin publicly committed to continuing Kozlov's work to preclude shadow economy groups from finding haven in the country's financial sector.

In October 2006, the Interior Ministry's Department for Economic Security reported that it had shut down a Georgian crime ring that had laundered as much as $9 billion from April 2004 to January 2005 through as many as five Russian banks. The announcement stated that the FSFM's analysis and cooperation with law enforcement authorities in Germany, Austria, Latvia, Lithuania, and Israel provided sufficient information to freeze the crime ring's bank assets. According to Interior Ministry representatives, two of the suspected banks' licenses had been revoked more than a year before the Department of Economic Security action.

Russian legislation provides for the tracking, seizure and forfeiture of criminal proceeds. None of this legislation is specifically tied to narcotics proceeds. Legislation provides for investigative techniques such as search, seizure, and the identification, freezing, seizing, and confiscation of funds or other assets. Authorities can also compel targets to produce documents. 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. The law allows the FSFM, in concert with banks, to freeze possible terrorist-related financial transactions for 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 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 to facilitate the commission of a crime.

The Presidential Administration as well as Russian law enforcement agencies have expressed concern about ineffective implementation of Russia's confiscation laws. The government has proposed amendments that are currently under review by the Duma (Parliament) 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. When this latter clause conflicted with existing domestic legislation, the Duma within the year approved an amendment to the anti-money laundering law, resolving the conflict and allowing banks to freeze assets immediately pursuant to UNSCR 1373. Article 205.1 of the criminal code, 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 ($1.1 million) in support of federal counterterrorism programs and improvement of national security.

The FSFM reports that in regard to terrorism financing, it has compiled a list of 1,300 organizations and individuals suspected of financing terrorism, 400 of which were foreign. There are five sources of information that may designate entities for inclusion on the FSFM's list of proscribed organizations. International organizations' designations, such as the UN 1267 Sanctions Committee, constitute the first source. Second, Russian court decisions provide a basis for inclusion. Third, resolutions from the Prosecutor General can identify individuals and organizations for inclusion. Fourth, Ministry of Interior investigations serve as a basis for inclusion if subsequent court decisions do not dismiss the investigation's findings. Finally, bilateral agreements, which include information sharing regarding entities on the counterpart's entities list, may provide a basis for inclusion on the FSFM list. As of a year ago, the FSFM has uncovered 113 bank accounts related to organizations and individuals included on Russia's terrorist list.

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.

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 the United States. The FSFM has been an active member of the Egmont Group since June 2002, having sponsored candidate FIUs from the former Soviet republics, including current FIU members in Ukraine and Georgia. 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. This close cooperation between Russian and U.S. agencies has continued and strengthened in 2006.

Russia became a full member of the Financial Action Task Force in June 2003 and participates as an active member in two FATF-style regional bodies. It is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and was instrumental in the creation of the Eurasian Group on Combating Legalization of Proceeds from Crime and Terrorist Financing (EAG). The EAG Secretariat is located in Moscow. In December 2005, under the auspices of the EAG, the FSFM established the International Training and Methodological Center of Financial Monitoring (ITMCFM). The main function of the Center is to provide technical assistance to EAG member-states, primarily in the form of staff training for FIUs and other interested ministries and agencies involved in AML/CFT efforts. The ITMCFM also conducts research on AML/CFT issues. As Chairman of the EAG, Russia's FIU 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.

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, and ratified on May 9, 2006, the UN Convention against Corruption.

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. Given its role in the creation and maintenance of the EAG, Russia has also demonstrated the will and capability to improve the region's capacity for countering money laundering and terrorism financing.

Nevertheless, serious vulnerabilities remain. Russia is among the world's most sophisticated perpetrators of fraud and money laundering through electronic and internet-related means. To meet its 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, including making all offshore operations subject to the identical due diligence and reporting requirements as other sectors. 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. Additionally, Russia should work to increase the effectiveness of its confiscation laws and their implementation including enacting legislation providing for the seizure of instruments, in addition to 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. The MLPA has received 69 suspicious transaction reports as of September 2006. In 2003, Samoa established an independent and permanent Transnational Crime Unit (TCU) under the authority of the Ministry of the Prime Minister. 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." 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." Reportedly, 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 "[i]f funds to be deposited or invested are being supplied by or on behalf of a third party, the identity of the third party (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 Samoa International Finance Authority, and the MLPA regulate the financial system. There are four locally incorporated commercial banks, supervised by the Central Bank. The Samoa International Finance Authority has responsibility for regulation and administration of the offshore sector. There are no casinos, but two local lotteries are in operation.

Samoa is an international offshore financial center, with six licensed international banks which have offices and employees. 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 six offshore banks, Samoa currently has 19,000 international business corporations (IBCs), three international insurance companies, six trustee companies, and 175 international trusts. Section 20 of the International Banking Act prohibits 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 International 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 information exchange requests. Samoa has reviewed 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, have prepared amendments to the Money Laundering Prevention Act of 2000 to strengthen and complement legislation that is being drafted or developed, including the Proceeds of Crime Bill, the Mutual Assistance in Criminal Matters Bill, the Extradition Amendment Bill and the Insurance Bill. These Bills are expected to be enacted in the first quarter of 2007.

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 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 assist a criminal in obtaining, concealing, retaining or investing funds, or to finance or facilitate the financing of terrorism.

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 international financial sector, principally the establishment of due diligence procedures for owners and directors of banks and the elimination of anonymous accounts. The Government of Samoa 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 has prepared the necessary changes to the Money Laundering Prevention Act to enable information exchange with overseas counterparts.

Samoa is a member of the Asia/Pacific Group on Money Laundering (APG)_and the Pacific Island Forum. Samoa hosted the annual plenary of the Pacific Island Forum in August 2004. Samoa is a party to the 1988 UN Drug Convention. Samoa has not signed the UN Convention against Transnational Organized Crime.

The Asia Pacific Group on Money Laundering and the Offshore Group of Banking Supervisors (APG/OGBS) undertook a second Mutual Evaluation of Samoa's compliance with international standards in February 2006. The resulting Mutual Evaluation Report (MER) was adopted at the APG Annual Meeting in Manila, the Philippines in July 2006. The MER noted that the GOS has sought to remedy major deficiencies with only partial success. Major deficiencies were noted in the legal and regulatory systems of both the onshore and offshore sectors as well as with what appears to be lack of political will throughout the system. STRs have continuously declined in the past several years and none have been disseminated to the Police for investigation, with the result that there have been no prosecutions or convictions for money laundering. There are serious impediments to exchanging information domestically and internationally. In sum, Samoa's anti-money laundering/counterterrorist regime is not functioning. An offshore sector that enables the anonymous establishment of IBCs violates the fundamental principal of transparency that underlies all international standards. The Government of Samoa should take all necessary steps to establish a regime that comports with all international standards, to which it has committed to adhere by virtue of its membership in the APG. The GOS has stated that the main noncompliance issues raised in the MER will be addressed when the proposed pieces of legislation mentioned above are passed and enacted in early 2007. The Government of Samoa should become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Saudi Arabia

Saudi Arabia is a growing financial center in the Gulf Region of the Middle East. There is little 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 Central Bank, the Saudi Arabian Monetary Agency (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 in Saudi Arabia are not primarily related to narcotics proceeds.

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 (STRs); 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; fund transfer systems be capable of detecting specially designated nationals; banks strictly adhere to SAMA circulars on opening accounts and dealing with charity and donation collection; and 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 (approximately $26,670); and develop internal control systems and compliance systems. SAMA also issued "know your customer" guidelines, requiring banks to freeze accounts of customers who do not provide updated account information. Saudi law prohibits nonresident 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 the Saudi Arabia Financial Investigation Unit (SA FIU) under the oversight of the Ministry of Interior. Saudi banks are required to have anti-money laundering units with specialized staff to work with SAMA, the SA FIU, and law enforcement authorities. All banks are also required to report any suspicious transactions in the form of an STR to the SA FIU. The SA FIU collects and analyzes STRs and other available information and makes referrals to the Bureau of Investigation and Prosecution, the Mabahith (the Saudi Intelligence Service), and the Public Security Agency for further investigation and prosecution. The SA FIU is staffed by officers from the Mabahith and SAMA. In September 2006, the SA FIU had its final on-site review by FinCEN, one of the Egmont co-sponsors, for possible Egmont membership in 2007.

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 to create fast, efficient, high quality, and cost-effective fund transfer systems that have proven capable of attracting customers accustomed to using hawala. 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 more than $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 has not issued new declaration forms, and therefore cannot enforce the current regulation.

Contributions to charities in Saudi Arabia usually consist of Zakat, which refers to an Islamic religious duty with specified humanitarian purposes. According to a 2002 report to the United Nations Security Council, over the past decade al-Qaida and other jihadist organizations collected between $300 and $500 million; and the majority of those funds originated from Saudi charities and private donors. The 9/11 Commission Report noted that the GOSA failed to adequately supervise Islamic charities in the country. To help address this problem, in 2002 Saudi Arabia announced its intention to establish the High Charities Commission to oversee Saudi charities with foreign operations. In 2004, the GOSA issued guidelines for the High Charities Commission (also known as the National Commission for Relief and Charitable Work Abroad). As of October 2006, GOSA has stated it is reviewing the role of the High Charities Commission and its relationship to Sharia law. The High Charities Commission has not been formally established, and the GOSA has made no further announcement of structure, leadership or staffing.

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 to track the operations of the charities. Banking rules implemented in 2003 that apply to all charities include stipulations which require charities to: only open accounts in Saudi Riyals; adhere to enhanced identification requirements; utilize one main consolidated account; and make payments only by checks payable to the first beneficiary and deposited in a Saudi bank. Regulations also forbid charities from using ATM and credit cards for charitable purposes, and making 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 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 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), a FATF-style regional body inaugurated in Bahrain in November 2004.

Saudi Arabia is working to implement 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 August 2006, the United Nations Security Council Resolution 1267 Sanctions Committee designated the International Islamic Relief Organization's (IIRO) branches in Indonesia and the Philippines, as well as the Kingdom's Eastern Province branch's Director, Abdulhamid Al-Mujil. Saudi Arabia is able to administratively freeze and seize terrorist assets. Saudi Arabia is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime.

The Government of Saudi Arabia is moving to monitor and enforce its anti-money laundering and terrorist finance laws, regulations and guidelines. However, Saudi Arabia should formally establish the High Commission for Charities. As with many countries in this region, there is still an over-reliance on suspicious transaction reporting to generate money laundering investigations. Law enforcement agencies should take the initiative and proactively generate leads and investigations, and be able to follow the financial trails wherever they lead. Saudi Arabia'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. Charitable donations in the form of gold, precious stones and other gifts should be scrutinized. International charities should be made subject to the same government oversight as domestic charities, including the rules of both SAMA and the Charities Commission. Saudi Customs should issue cross-border currency declaration forms and enforce the reporting requirements. The GOSA should become a party to the UN International Convention for Suppression of the Financing of Terrorism.

Senegal

Senegal is vulnerable to money laundering. Reportedly, most money laundering involves domestically-generated proceeds from corruption and embezzlement. Dakar's hot real-estate market is largely financed by cash, and ownership of properties is nontransparent. The building boom and high property prices suggest that an increasing amount of funds with an uncertain origin circulates in Senegal. Other areas of concern include: cash, gold and gems transiting Senegal's airport and porous borders; real estate investment in the Petite Cote south of Dakar; and trade-based money laundering centered in the region of Touba, a largely autonomous and unregulated free-trade zone under the jurisdiction of the Mouride religious authority. This latter region reportedly receives between 550 and 800 million dollars per year in funds repatriated by networks of Senegalese vendors abroad. There is some evidence of increasing criminal activity by foreigners, such as drug trafficking by Latin American groups and illegal immigrant trafficking involving Pakistanis.

Seventeen commercial banks operate alongside a thriving micro-credit sector. Western Union, Money Gram and Money Express, associated with banks, are ubiquitous, suggesting that, while informal remittance systems exist, they are not a large threat to the business of the licensed remitters. The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU or UEMOA): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal and Togo, all of which use the French-backed CFA franc (CFAF) currency, which is pegged to the euro. The Commission Bancaire, responsible for bank inspections, is based in Abidjan.

In 2004, Senegal became the first WAEMU country to enact the WAEMU Uniform Law on Money Laundering (the Uniform Law). The new legislation meets many international standards with respect to money laundering, but does not comply with all Financial Action Task Force (FATF) recommendations concerning politically-exposed persons, and lacks certain compliance provisions for nonfinancial institutions. The law does not deal with terrorist financing.

Senegal's Financial Intelligence Unit (FIU) became operational in August 2005. Since that date it has received 59 (11 in 2005 and 48 in 2006) suspicious declarations and has referred nine cases (three in 2005, six in 2006) to the Prosecutor General. All but two of the declarations have been made by banks. The other two came from Customs. Of the referrals, one concerns drug trafficking, one concerns diamond trafficking, one relates to tax fraud, and three are corruption related. No cases have concluded, although one arrest has been made. The FIU currently has a staff of 23, including six appointed members: the President of the FIU, who by law is chosen from the Ministry of Economy and Finance, and five others detailed from the Customs Service, the BCEAO, the Judicial Police, and the judiciary. The FIU also relies on liaison officers in relevant governmental institutions that can provide information relevant to the FIU's investigations. With French sponsorship, Senegal's FIU is a candidate for membership in the Egmont Group. Its candidacy is on hold pending the adoption of a terrorist financing law.

Official statistics regarding the prosecution of financial crimes are unavailable. There is one known conviction for money laundering since January 1, 2005. The conviction led to the confiscation of a private villa.

The BCEAO is working on a Directive against Terrorist Financing. If adopted, the member states would be directed to enact a law against terrorist financing, which most likely would be presented as a Uniform Law in the same manner as the AML law. Like the AML law, it is a penal law, and each national assembly must then enact enabling legislation to adopt the new terrorist finance law. In addition, the FATF-style regional body for the 15-member Economic Community of Western African States (ECOWAS), GIABA (African Anti-Money Laundering Inter-governmental Group) has drafted a uniform law, which it hopes to have enacted in all of its member states, not just the WAEMU states.

The UN 1267 Sanctions Committee consolidated list is circulated both by the FIU and by the BCEAO to commercial financial institutions. To date, no assets relating to terrorist entities have been identified. The WAEMU Council of Ministers issued a directive in September 2002 requiring banks to freeze assets of entities designated by the Sanctions Committee.

Senegal has entered into bilateral criminal mutual assistance agreements with France, Tunisia, Morocco, Mali, The Gambia, Guinea Bissau, and Cape Verde. Multilateral ECOWAS treaties deal with extradition and legal assistance. Under the Uniform Law, the FIU may share information freely with other FIUs in WAEMU. However, only Senegal and Niger have operational FIUs. The FIU has signed an MOU to exchange information with the FIUs of Belgium and Lebanon, and is working on other accords. In general, the Government of Senegal (GOS) has demonstrated its commitment and willingness to cooperate with United States law enforcement agencies. In the past the GOS has worked with INTERPOL, Spanish, and Italian authorities on international anticrime operations.

Senegal is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the 1999 UN International Convention for the Suppression of the Financing of Terrorism, and the Convention against Corruption. Senegal is listed as 70 out of 163 countries monitored in Transparency International's 2006 Corruption Perception Index.

Senegal has made considerable progress in establishing an operational FIU and raising the awareness of the threat of money laundering. However, a complicated political climate in advance of the 2007 elections, a generally nontransparent police and judiciary, and conflicting governmental interests in the banking sector threaten to retard any efforts to take this progress to the next level of actual prosecutions and convictions. Recent arrests of opposition politicians, journalists, and a corruption scandal that resulted in the early retirement, rather than prosecution, of the implicated judges, illustrate the weakness of the rule of law in Senegal.

The Government of Senegal should continue to work with its partners in WAEMU and ECOWAS to establish a comprehensive anti-money laundering and counterterrorist financing regime. Senegal should work on achieving transparency in its financial and real estate sectors. Senegal and the region should establish better control of cross-border currency transfers. Senegalese law enforcement and customs authorities should take the initiative to identify and investigate money laundering at the street level and informal economy. Senegal should pass an antiterrorist finance law.

Serbia

Serbia is not a regional financial center. At the crossroads of Europe and on the major trade corridor known as the "Balkan route," Serbia confronts narcotics trafficking, smuggling of persons, drugs, weapons and pirated goods, money laundering, and other criminal activities. Serbia continues to be a significant black market for smuggled goods. Illegal proceeds are generated from drug trafficking, official corruption, tax evasion and organized crime, as well as other types of crimes. Proceeds from illegal activities are invested in all forms of real estate. Trade-based money laundering, in the form of over- and under-invoicing, is commonly used to launder money.

A significant volume of money flows to Cyprus, reportedly as the payment for goods and services. The records maintained by various government entities vary significantly on the volume and value of

imports from Cyprus. According to official statistics from the National Bank of Serbia, over $1 billion in payments in 2005, coded as being for goods and services, rank Cyprus among the top five exporters of goods or services to Serbia. The Serbian Statistical Office reflected imports from Cyprus of roughly $40 million in 2005. According to Government of the Republic of Serbia (GOS) officials, much of the difference is due to payments made to accounts in Cyprus for goods, such as Russian oil, that actually originate in a third jurisdiction.

Serbia's banking sector is more than 80 percent foreign-owned. There is no provision in the banking law that allows the establishment of offshore banks, shell companies or trusts. Reportedly, there is no evidence of any alternative remittance systems operating in the country. Nor, reportedly, is there evidence of financial institutions engaging in currency transactions involving international narcotics trafficking proceeds. Serbia has 14 designated free trade zones, three of which are in operation. The free trade zones were established to attract investment by providing tax-free areas to companies operating within them. These companies are subject to the same supervision as other businesses in the country.

As the result of a public referendum on May 21, 2006, the State Union of Serbia and Montenegro (SAM) was dissolved and Montenegro became an independent country. The GOS became the legacy member of the Council of Europe and the United Nations. As a result, all treaties and agreements signed by the State Union are now applicable to Serbia, including the1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The GOS is a party to all 12 UN Conventions and Protocols dealing with terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism, although domestic implementation procedures do not provide the framework for full application. In December 2005, the GOS ratified the UN Convention against Corruption.

In September 2005, Serbia codified an expanded definition of money laundering in the Penal Code. This legislation gives police and prosecutors more flexibility to pursue money laundering charges, as the law broadens the scope of money laundering and aims to conform to international standards. The penalty for money laundering is a maximum of 10 years imprisonment. Under this law and attendant procedure, money laundering falls into the serious crime category and permits the use of Mutual Legal Assistance (MLA) procedures to obtain information from abroad.

On November 28, 2005, Serbia adopted a revised anti-money laundering law (AMLL), replacing the July 2002 Law on the Prevention of Money Laundering. The revised AMLL expands the number of entities required to collect certain information on all cash transactions over EUR 15,000 (approx. $19,500), or the dinar equivalent, and to file currency transaction reports (CTRs) for all such transactions exceeding this threshold to the financial intelligence unit (FIU). Suspicious transactions in any amount must be reported to the FIU. The law expands those sectors subject to reporting and record keeping requirements, adding attorneys, auditors, tax advisors and bank accountants, currency exchanges, insurance companies, casinos, securities brokers, dealers in high value goods and travel agents to those already required to comply with the AMLL provisions. Required records must be maintained for five years. These entities are protected with respect to their cooperation with law enforcement entities. The AMLL requires obligated entities and individuals to monitor customers' accounts when they have a suspicion of money laundering, in addition to reporting to the FIU. The AMLL also eliminates a previous provision limiting prosecution to crimes committed within Serbian territory. Significant improvement has been noted in financial institution compliance, i.e., gathering and keeping records on customers and transactions. The flow of information to the FIU has been steadily increasing, but not all entities are yet subject to implementing bylaws.

The Law on Foreign Exchange Operations, adopted in 2006, criminalizes the use of false or inflated invoices or documents to effect the transfer of funds out of the country. This law was enacted in part to counter the perceived problem of import-export fraud and money laundering. According to the law,

residents and nonresidents are obliged to declare to Customs authorities all currency (foreign or dinars), or securities in amounts exceeding EUR 5,000 being transported across the border.

The National Bank of Serbia (NBS) has supervisory authority over banks, currency exchanges, insurance and leasing companies. The NBS has issued regulations requiring banks to have compliance and know-your-customer (KYC) programs in place and to identify the beneficial owners of new accounts. In June 2006, the NBS expanded its customer identification and record keeping rules by adopting new regulations mandating enhanced due diligence procedures for certain high risk customers and politically exposed persons. Similar regulations are being developed for insurance companies. The Law on Banks includes a provision allowing the NBS to revoke a bank's license for activities related to, among other things, money laundering and terrorist financing. To date, the NBS has not used this revocation authority. The legal framework is in place, but the NBS currently lacks the expertise needed for effective bank supervision. It is building these capacities through training and staff development.

The Securities Commission (SC) supervises broker-dealers and investment funds. The Law on Investment Funds and the Law on Securities and Other Financial Instruments Market provide the SC with the authority to "examine" the source of investment capital during licensing procedures. The SC is also charged with monitoring its obligors' compliance with the AML Laws. Regulations to implement this authority are being developed.

The Administration for the Prevention of Money Laundering serves as Serbia's FIU. The revised AMLL elevates the status of the FIU to that of an administrative body under the Ministry of Finance from its previous status as a "sector" in that Ministry. This provides more autonomy for the agency to carry out its mandate, as well as additional resources. One important change is that the FIU now has its own line item operating budget. The FIU currently has 24 employees. In accordance with the revised AMLL, the FIU developed listings of suspicious activity red flags for banks, currency exchange offices, insurance companies, securities brokers and leasing companies. Other significant changes include the authority of the FIU to freeze transactions for a maximum of 72 hours. The FIU has signed memoranda of understanding (MOU) on the exchange of information with the NBS and Customs and is negotiating one with the Tax Administration.

The FIU received 279 suspicious transaction reports (STRs) in 2005 and 361 through September 1, 2006. Virtually all of the STRs received by the FIU have been filed by commercial banks. Currency exchange offices have filed only seven STRs since 2003, and none in either 2005 or 2006. Since its inception in 2003, the FIU has opened 240 cases, 74 based on the STRs it received and 166 based on CTRs or referrals from other entities; 103 cases were referred to either law enforcement or the prosecutor's office for further investigation. Since 2004, authorities filed 41 criminal charges against 48 persons for money laundering violations. The most common predicate crime is "abuse of office". Of this number, eighteen are currently under investigation, six were dismissed or terminated; fourteen were indicted; and two court decisions have been reached to date. One person has been acquitted and the other was convicted, but has appealed the verdict.

Serbia introduced a value-added tax (VAT) in 2005, and the full impact of refund fraud associated with the administration of the VAT is still not clear. Serbia's Tax Administration lacks the audit and investigative capacity or resources to adequately investigate the large number of suspicious transactions that are forwarded by Serbia's FIU. In addition, current tax law sets a low threshold for auditing purposes and has increased the burden on the Tax Administration. 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.

The difficulty of convicting a suspect of money laundering without a conviction for the predicate crime 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. The Suppression of Organized Crime Service (SOCS) of the Ministry of Interior houses a new Anti-Money Laundering Section to better focus financial investigations.

In August 2005, the GOS established the Permanent Coordinating Group (PCG), an interagency working group originally tasked with developing an implementation plan for the recommendations from MONEYVAL's first-round evaluation in October 2003. A subgroup was 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 reporting to the FIU of transactions suspected to be terrorist financing. The PCG meets intermittently as required for completing specific tasks. The government still needs better interagency coordination to improve information sharing, record keeping and statistics.

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. The FIU is charged with enforcing the UNSCR 1267 provisions regarding suspected terrorist lists. A draft law on terrorist financing, now pending Parliamentary approval, will apply all provisions of the AML laws to terrorist financing and will implement a freezing mechanism based on UNSCR provisions. Although the FIU routinely provides the UN list of suspected terrorist organizations to the banking community, examination for suspect accounts have revealed no evidence of terrorist financing within the banking system and no evidence of alternative remittance systems. The SOCS, the Special Anti-Terrorist Unit (SAJ), and Gendarmarie, in the Ministry of Interior, are the law enforcement bodies responsible for planning and conducting the most complex antiterrorism operations. SOCS cooperates and shares information with its counterpart agencies in all of the countries bordering Serbia. Although Serbia has criminalized the financing of terrorism, the freezing, seizing and confiscation of assets of terrorists in accordance with UN Security Council resolutions still lacks a legal basis, pending enactment of the Anti-terrorism Finance legislation.

Serbia has no laws governing its cooperation with other governments related to narcotics, terrorism, or terrorist financing. Bases for cooperation include 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.

Serbia does not have a mutual legal assistance arrangement with the United States, but information exchange via a letter rogatory is standard. The 1902 extradition treaty between the Kingdom of Serbia and the United States remains in force. The GOS has bilateral agreements on mutual legal assistance with 31 countries. As a member of the Council of Europe, the GOS is an active member of the Council's MONEYVAL. In July 2003, the FIU became a member of the Egmont Group and actively participates in information exchanges with counterpart FIUs including FinCEN. The Serbian FIU has also signed information sharing memoranda of understanding (MOUs) with Macedonia, Romania, Belgium, Slovenia, Montenegro, Albania, Georgia, Ukraine, Bulgaria, Croatia, and Bosnia and Herzegovina.

Serbia should continue to work toward eliminating the abuses of office and culture of corruption that enables money laundering and financial crimes. Among the pending legal infrastructure necessary for Serbia to be fully compliant with international standards are laws providing for the liability of legal persons for money laundering and terrorist financing; regulations to apply all requirements of the Revised AML Law to covered nonbank financial institutions; legislation to establish a robust asset seizure and forfeiture regime; and legislation providing for the sharing of seized assets. Serbia also needs to enact and implement proposed legislation needed to comply with UN Security Council resolutions regarding the freezing, seizing and confiscation of suspected terrorist assets and require suspicions of terrorist financing to be reported to the FIU.

The National Bank and other supervisory bodies need training and additional staff. The GOS should enforce regulations pertaining to money service businesses and obligated nonfinancial business and professions. The supervisory scheme should be completed, and implementing regulations should be binding, for the insurance and securities sectors. On an operational level, law enforcement needs audit and investigative capacity in order to investigate the STRs that the FIU disseminates. Training is also required for prosecutors and judges. Rather than address specific tasks as an ad hoc group, the PCG should meet on a regular basis to discuss issues and projects, and work to improve interagency coordination in such areas as information sharing, record keeping and statistics.

Seychelles

Seychelles is a not a major financial center. The existence of a developed offshore financial sector, however, makes the country vulnerable to money laundering. The Government of Seychelles (GOS), in efforts to diversify its economy beyond tourism, developed an offshore financial sector to increase foreign exchange earnings and actively markets itself as an offshore financial and business center that allows the registration of nonresident companies. As of September 2006, there were 31,000 registered international business companies (IBCs) and 157 trusts that pay no taxes in Seychelles, and are not subject to foreign exchange controls. The Seychelles International Business Authority (SIBA), a body with board members from both the government and the private sector, licenses and regulates offshore activities. The SIBA acts as the central agency for the registration for IBCs and trusts and regulates activities of the Seychelles International Trade Zone.

In addition to IBCs and trusts, Seychelles permits offshore insurance companies, mutual funds, and offshore banking. The GOS is currently in the process of establishing the Non-Bank Financial Services Authority, which will be responsible for regulating these sectors under the Mutual Funds Act, the Securities Act, and the Insurance Act. Three offshore insurance companies have been licensed: one for captive insurance and two for general insurance. Seychelles has one offshore bank to date: the Barclays Bank (Offshore Unit). The International Corporate Service Providers Act 2003, designed to regulate all activities of corporate and trustee service providers, entered into force in 2004.

In 1996, the GOS enacted the Anti-Money Laundering Act (AMLA), which criminalized the laundering of funds from all serious crimes, required covered financial institutions and individuals to report to the Central Bank transactions involving suspected cases of money laundering, and established safe harbor protection for individuals and institutions filing such reports. The AMLA also imposed record keeping and customer identification requirements for financial institutions, and provided for the forfeiture of the proceeds of crime. In October 2004, the International Monetary Fund (IMF) released a report on its 2002 financial sector assessment of the Seychelles. The IMF report noted deficiencies in the AMLA and practice, and recommended closing existing loopholes as well as updating the AMLA to reflect current international standards and best practices.

In May 2006, the Anti-Money Laundering Act 2006 came into force. This new legislation replaces the AMLA of 1996 and addresses many of the deficiencies cited by the IMF report. Under the new AMLA, money laundering controls, including the obligation to submit suspicious transaction reports (STRs), are applied to the same financial intermediaries as under the 1996 law, as well as nonbanking financial institutions, including exchange houses, stock brokerages, insurance agencies, lawyers, notaries, accountants, and estate agents. Offshore banks are also explicitly covered. Gaming operations, including internet gaming, are also obligated, but the law does not state explicitly that offshore gaming is covered in an identical manner. Currently, no offshore casinos or Internet gaming sites have been licensed to operate. There is no cross-border currency reporting requirement. The 2006 AMLA discusses record-keeping and institutional protocol requirements, sets a maximum delay of two working days to file a suspicious transaction report, criminalizes tipping off, and sets safe harbor provisions. The new law also requires the identification of beneficial owners, but leaves open

exceptions for “an existing and regular business relationship with a person who has already produced satisfactory evidence of identity”; for “an occasional transaction under R50,000” ($9,200); and in other cases “as may be prescribed”.

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. Money laundering is sanctioned by imprisonment for up to fifteen years and/or R3,000,000 ($554,500) in penalties. While there have been about thirty investigations, there have been no arrests or prosecutions for money laundering or terrorist financing since January 1, 2003. This is problematic.

The Financial Institutions Act of 2004, imposes more stringent rules on banking operations. The law, which was drafted in consultation with the International Monetary Fund, aims to ensure 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 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.

The Central Bank of the Seychelles has been acting as the financial intelligence unit (FIU) for the Seychelles in that it receives and analyzes suspicious activity reports and disseminates them to the competent authorities. It cannot freeze or confiscate property, but can get a court order to effect an asset freeze. The courts have the authority to freeze or confiscate money or property. Section 16 of the 2006 AMLA provides for the creation of an FIU within the Central Bank. This FIU will receive reports, have access to information in public or governmental databases and may request information from reporting entities, supervisory bodies and law enforcement agencies. The FIU will analyze the information and disseminate information to the appropriate entities if the FIU deduces that there is unlawful activity. The law provides for the FIU to have a proactive targeting section that will research trends and developments in not only money laundering, but also terrorism financing. The FIU will also perform examinations of the reporting entities and, in concert with regulators, issue guidance related to customer identification, identification of suspicious transactions, and record keeping and reporting obligations. The law provides for the possibility that the FIU would in the future perform training related to these matters. Authorities are also discussing the establishment of an AML interagency Task Force that would incorporate the FIU, Police, Customs, Immigration, and Internal Affairs.

Judges in the Supreme Court have the authority to restrain a target from moving or disposing of his or her assets, and will do so if a law enforcement officer requests it, provided that the Court is “satisfied that there are reasonable grounds” for doing so. The Court also has the authority to determine the length of time for the restraint order and the disposition of assets, should it become necessary. Should the target violate the order, he or she becomes subject to financial penalties. Law enforcement may seize property subject to this order to prevent property from being disposed of or moved contrary to the order. The Court also is authorized to order the forfeiture of assets.

In 2004, the GOS enacted the Prevention of Terrorism Bill. The legislation specifically recognizes the government’s authority to identify, freeze, and seize terrorist finance-related assets. The 2006 AMLA also makes the legal requirements applicable to money laundering applicable to suspected terrorist financing transactions. 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 support other 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. The Prevention of Terrorism Act 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. Seychelles underwent a mutual evaluation review conducted by ESAAMLG in November 2006. The Seychelles 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. 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 prohibiting bearer shares and clarifying the new legislation regarding the complete identification of beneficial owners. Seychelles should also clarify the legislation to state explicitly that all offshore activity is covered in the same manner and to the same degree as onshore. Seychelles should continue to work towards the establishment of its FIU, ensuring that it develops with a degree of independence and autonomy from its parent agency, the Central Bank. The GOS should also consider codifying the ability to freeze assets rather than issuing restraining orders, and develop a currency reporting requirement for entry into its borders. Seychelles should continue to participate in ESAAMLG, and when the mutual evaluation report is finalized, work to address any further deficiencies outlined therein.

Sierra Leone

Sierra Leone has a cash-based economy and is not a regional financial center. Government of Sierra Leone (GOSL) officials have reportedly stated that money laundering activities are pervasive, particularly in the diamond sector. Although there have been some attempts at tighter regulation, monitoring, and enforcement, in some areas significant diamond smuggling still exists. Loose oversight of financial institutions, weak regulations, pervasive corruption, and a widespread informal money-exchange and remittance system also work to create an atmosphere conducive to money laundering.

The President signed the Anti-Money Laundering Act (AMLA) in July 2005. The AMLA incorporates international standards, including setting safe harbor provisions, know your customer and identification of beneficial owner requirements, as well as mandatory five-year record-keeping. There is a currency reporting requirement for deposits larger than 25 million leones (approximately $8,330) and no minimum for suspicious transaction reporting. The law requires that international financial transfers over $10,000 go through formal financial institution channels. The AMLA calls for cross-border currency reporting requirements for cash or securities in excess of $10,000. The law designates the Governor of the Bank of Sierra Leone as the national Anti-Money Laundering Authority.

The AMLA applies to Sierra Leone's financial sector institutions such as depository and credit institutions, money transmission and remittance service centers, insurance brokers, investment banks and businesses including securities and stock brokerage houses, and currency exchange houses. Designated nonfinancial businesses and professions such as casinos, realtors, dealers in precious metals and stones, notaries, legal practitioners, and accountants are also included.

A financial intelligence unit (FIU) exists but lacks the capacity to effectively monitor and regulate financial institution operations. Law enforcement and customs have limited resources and lack

training. There have reportedly been a small number of arrests under the AMLA but no convictions due to lack of capacity by police investigators and judicial authorities.

The AMLA empowers the courts to freeze assets for seventy-two hours if a suspect has been charged with money laundering or if a charge is imminent. Upon a conviction for money laundering, all property is treated as illicit proceeds and can be forfeited unless the defendant can prove that possession of some or all of the property was obtained through legal means. The AMLA also provides for mutual assistance and international cooperation.

In July 2006, the Bank of Sierra Leone hosted a United Nations Office on Drugs and Crime and Group for Action Against Money Laundering (GIABA)-sponsored training workshop on strategy development for anti-money laundering and combating financing of terrorism. Workshop participants recommended that the Bank of Sierra Leone draft a national strategy and regulations for the operations of the FIU, establish a system for the receipt, analysis, and dissemination of financial disclosures, and develop a formal system to report suspicious financial transactions to the FIU.

Workshop participants also recommended creating a special unit comprised of two staff from the police's organized crime unit and two from the counterterrorism unit to deal with issues pertaining to anti-money laundering issues. They also recommended creating protocols to improve the exchange of information between government offices, including the Attorney General's Office, Police, National Revenue Authority, and Anti-Corruption Commission.

Sierra Leone is member of GIABA. It is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Sierra Leone is a party to the UN Convention against Corruption. Sierra Leone is listed 148 of 162 countries monitored in Transparency International's 2006 Corruption Perception Index.

Although the Government of Sierra Leone has passed anti-money laundering legislation, it remains to be effectively implemented or harmonized with other legislation relating to anti-money laundering and combating financing of terrorism, including the Anti-Corruption Act, National Drug Control Act, and Anti-Terrorism Act. The GOSL should ensure its antiterrorist finance countermeasures adhere to world standards, including the regular distribution to financial institutions of the UNSCR 1267 Sanctions Committee's consolidated list. The GOSL must increase the level of awareness of money laundering issues and allocate the necessary human, technical, and financial resources. Sierra Leone should continue its efforts to counter the smuggling of diamonds. Sierra Leone should take steps to combat corruption at all levels of commerce and government. It needs to 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, transnational criminals, terrorist organizations and their supporters seeking to launder money, as well as for flight capital.

Structural gaps remain in financial regulation that may hamper efforts to control these crimes. To address some of these deficiencies, Singapore is beginning to map out legal and regulatory changes to implement the Financial Action Task Force's (FATF) revised recommendations on anti-money laundering (AML) and countering the financing of terrorism (CFT).

Singapore amended the Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) in May 2006 to add 108 new categories to its "Schedule of Serious Offenses."

The CDSA criminalizes the laundering of proceeds from narcotics transactions and other predicate offenses, including ones committed overseas that would be serious offenses if they had been committed in Singapore. Included among the new offenses are crimes associated with terrorist financing, illicit arms trafficking, counterfeiting and piracy of products, environmental crime, computer crime, insider trading, and rigging in commodities and securities markets. With an eye on Singapore's two new multibillion-dollar casinos slated to be operational in 2009, the list also addresses a number of gambling-related crimes. However, tax and fiscal offenses are still absent from the expanded list.

Singapore has a sizeable offshore financial sector. As of September 2006, there were 109 commercial banks in operation, including five local and 24 foreign-owned full banks, 45 offshore banks, and 35 wholesale banks. All offshore and wholesale banks are 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 Prime Minister's Office, serves as Singapore's central bank and financial sector regulator, particularly with respect to Singapore's AML/CFT efforts. MAS performs extensive prudential and regulatory checks on all applications for banking licenses, including whether banks are under adequate home country banking supervision. Banks must have clearly identified directors. Unlicensed banking transactions are illegal.

Singapore has increasingly become a center for offshore private banking and asset management. Total assets under management in Singapore grew 26 percent between 2004 and 2005 to $450 billion, according to MAS. Private wealth managers estimate that total private banking and asset management funds increased nearly 300 percent between 1998 and 2004.

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 births 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, futures brokers and advisors, trust companies, approved trustees, and money changers and remitters.

Singapore is in the process of revising its AML/CFT regulations for banks and other financial institutions. The relevant Notices should further align certain parts of Singapore's AML/CFT regime more closely with FATF recommendations. Among the proposed regulations are new provisions that would proscribe banks from entering into, or continuing, correspondent banking relationships with shell banks; require originator information on cross-border wire transfers; clarify procedures for customer due diligence (CDD), including adoption of a risk-based approach; and mandate enhanced CDD for foreign politically exposed persons. Terrorist financing activities will also be addressed in the Notices for the first time. As part of this process, MAS issued for public comments draft regulations for banks in January 2005. In August 2006, it issued for public comments revised draft regulations for banks and new draft regulations for other financial institutions. Singapore is also considering regulations governing designated nonfinancial businesses and professions to bring them into conformity with FATF recommendations.

In addition to banks that offer trust, nominee, and fiduciary accounts, Singapore has 12 trust companies. All banks and trust companies, whether domestic or offshore, are subject to the same

regulation, record-keeping, and reporting requirements, including for 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 August 2006, MAS issued for public comments draft regulations that would require approved trustees and trust companies to complete all mandated CDD procedures before they could establish relations with customers. Other financial institutions are allowed to establish relations with customers before completing all CDD-related measures.

Singapore amended its Moneylenders Act in April 2006 to require moneylenders under investigation to provide relevant information or documents. The Act imposes new penalties for giving false or misleading information and for obstructing entry and inspection of suspected premises.

In April 2005, Singapore lifted its ban on casinos, paving the way for development of two integrated resorts scheduled to open in 2009. Combined total investment in the resorts is estimated to exceed $5 billion. In June 2006, Singapore implemented the Casino Control Act. The Act establishes the Casino Regulatory Authority of Singapore, which will administer the system of controls and procedures for casino operators, including 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 legal changes that would allow for 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. Procedural regulations and bank secrecy laws limit STRO's ability to provide information relating to financial crimes. 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, Brazil, Canada, Greece, Hong Kong, Italy, Japan and Mexico. To improve its suspicious transaction reporting, STRO has developed 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 participate in this system.

Singapore is an important participant in the regional effort to stop terrorist financing in Southeast Asia. The Terrorism (Suppression of Financing) Act 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.

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

Based on regulations issued in 2002, MAS has broad powers to direct financial institutions to comply with international obligations related to terrorist financing obligations. 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 are periodically updated to include 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 September 2006, there were 395 money-changers and 95 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 provide information concerning 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). In August 2006, MAS issued for public comments draft regulations that would require licensees to establish the identity of all customers; currently, no such identification is mandatory for transactions in aggregate of up to S$5,000 (approximately US$3,000). MAS would also be required to approve any non face-to-face transactions.

Singapore has five free trade zones (FTZs), four for seaborne cargo and one for airfreight, regulated under the Free Trade Zone Act. The FTZs may be used for storage, repackaging of import and 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 1,807 registered charities as of December 2005. All charities must register with the Commissioner of Charities which, since September 1, 2006, has reported to the Minister for Community Development, Youth and Sports instead of the Minister for Finance. Charities must submit governing documents outlining their objectives and particulars of 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 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, effective 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 that 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, amounts transferred to persons outside Singapore, and names of recipients. The government issued 36 permits in 2005 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. Parliament amended the MACMA in February 2006 to allow the government to respond to requests for assistance even in the absence of a bilateral treaty, MOU or other agreement with Singapore. The MACMA provides for international cooperation on any of the 292 predicate "serious offenses" listed under the CDSA. 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 (Drug Designation Agreement or DDA). This was the first agreement concluded pursuant to the MACMA. The DDA, which came 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 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 mutual legal assistance agreements with Hong Kong in 2003 and with India in 2005. Singapore is a party to the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters along with Malaysia, Vietnam, Brunei. Cambodia, Indonesia, Laos, the Philippines, Thailand, and Burma. The treaty will come into effect after ratification by the respective governments. Singapore, Malaysia, Vietnam and Brunei have ratified thus far.

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 adopt measures to regulate and monitor large currency and bearer negotiable instrument movements into and out of the country, in line with 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. Singapore should add tax and fiscal offenses to its schedule of serious offenses.

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. Singapore should lift its rigid bank secrecy restrictions to enhance its law enforcement cooperation in areas such as information sharing and to conform to international standards and best practices.