Nigeria

Although the Federal Republic of Nigeria is not an offshore financial center, Nigeria's large economy is a hub for the trafficking of persons and narcotics. Nigeria is a major drug-transit country and is a center of criminal financial activity, reportedly for the entire continent. Individuals and criminal organizations have taken advantage of the country's location, weak laws, systemic corruption, lack of enforcement, and poor socioeconomic conditions to strengthen their ability to perpetrate financial crimes at home and abroad. Nigerian criminal organizations are adept at devising new ways of subverting international and domestic law enforcement efforts and evading detection. Their success in avoiding detection and prosecution has led to an increase in many types of financial crimes, including bank fraud, real estate fraud, and identity theft. In addition, advance fee fraud, also referred to internationally as "419" fraud, in reference to the fraud section in Nigeria's criminal code, is a lucrative financial crime that generates hundreds of millions of illicit dollars annually for criminals. Despite years of government effort to counter rampant crime and corruption, Nigeria continues to be plagued by crime. The establishment of the Economic and Financial Crimes Commission (EFCC) along with the Independent Corrupt Practices Commission (ICPC) and the improvements in training qualified prosecutors for Nigerian courts yielded some successes in 2006 and 2007.

In June 2001, the Financial Action Task Force (FATF) placed Nigeria on its list of noncooperative countries and territories (NCCT). In December 2002, Nigeria enacted two pieces of legislation to remedy the deficiencies. It passed an amendment to the 1995 Money Laundering Act extending the scope of the law to cover the proceeds of all crimes. The Government of Nigeria (GON) also passed an amendment to the 1991 Banking and Other Financial Institutions (BOFI) Act expanding coverage of the law to stock brokerage firms and foreign currency exchange facilities, giving the Central Bank of Nigeria (CBN) greater power to deny bank licenses, and allowing the CBN to freeze suspicious accounts. The third piece of legislation, the 2004 Economic and Financial Crimes Commission (Establishment) Act, established the Economic and Financial Crimes Commission (EFCC), the body that investigates and prosecutes money laundering and other financial crimes, and coordinates information sharing. The Economic and Financial Crimes Commission Act also criminalizes the financing of terrorism and participation in terrorism. Violation of the Act carries a penalty of up to life imprisonment. In May 2006, the FATF visited Nigeria to conduct an evaluation of the revisions made to the government's AML regime. FATF recognized that the GON had remedied the major deficiencies in its anti-money laundering (AML) regime and removed Nigeria from the NCCT list.

Since its inception in April 2004, the EFCC has had the mandate to investigate and prosecute financial crime. It has recovered or seized assets from people guilty of fraud both inside and outside of Nigeria, including a syndicate that included highly placed government officials who were defrauding the Federal Inland Revenue Service (FIRS). Several influential individuals have been arrested and are currently awaiting trial. EFCC members also embarked upon a campaign to identify and prosecute former officials. Some EFCC members have been killed for their efforts to expose and enforce the laws against corruption and financial crime.

The National Assembly passed the Money Laundering (Prohibition) Act (2004), which applies to the proceeds of all financial crimes. Nigeria also employs the 1995 Foreign Exchange (Monetary and Miscellaneous Provisions) Act. The legislation gives the CBN greater power to deny bank licenses and freeze suspicious accounts. This legislation also strengthens financial institutions by requiring more stringent identification of accounts, removing a threshold for suspicious transactions, and lengthening the period for retention of records. Money laundering controls apply to banks and other financial institutions, including stock brokerages and currency exchange house, as well as designated nonfinancial businesses and professions (DNFBPs). These institutions include dealers in jewelry, cars and luxury goods, chartered accountants, audit firms, tax consultants, clearing and settlement companies, legal practitioners, hotels, casinos, supermarkets and other businesses that the Federal Ministry of Commerce designates as obliged. The EFCC Act provides safe-harbor provisions to

obliged entities. Nigeria has no secrecy laws that prevent the disclosure of client and ownership information by domestic financial services companies to bank regulatory and law enforcement authorities.

The Special Control Unit Against Money Laundering (SCUML), is a special unit in the Ministry of Commerce which monitors, supervises, and regulates the activities of all DNFBPs. Oversight, however, has reportedly not been very rigorous or effective. Amendments to the 2004 EFCC Act gave the EFCC the authority to investigate and prosecute money laundering, enlarged the number of EFCC board members, enabled the EFCC police members to bear arms, and banned interim court appeals that hinder the trial court process.

The Nigerian Financial Intelligence Unit (NFIU), established in 2005, derives its powers from the Money Laundering (Prohibition) Act of 2004 and the Economic and Financial Crimes Commission Act of 2004. Housed within the EFCC, it is the central agency for the collection, analysis and dissemination of information on money laundering and terrorist financing. The NFIU is a significant component of the EFCC, complementing the EFCC's directorate of investigations. It does not carry out its own investigations. Legal provisions give the NFIU power to receive suspicious transaction reports (STRs) submitted by financial institutions and designated nonfinancial businesses and professions. The NFIU also receives reports involving the transfer to or from a foreign country of funds or securities exceeding U.S. $10,000 in value. All financial institutions and designated nonfinancial institutions are required by law to furnish the NFIU with details of these financial transactions.

The NFIU fulfills a crucial role in receiving and analyzing STRs. As a result of the NFIU's activities, banks have improved both their timeliness and quality in filing STRs reported to the NFIU. The NFIU has access to records and databanks of all government and financial institutions, and it has entered into memoranda of understandings (MOUs) on information sharing with several other FIUs. In 2006, the NFIU received 3,772,843 currency transaction reports (CTRs). Out of the 47 cases the NFIU developed, 12 investigations are ongoing, and the NFIU disseminated 18 and placed 10 under monitoring. The NFIU closed seven in-house cases. Because the disseminated cases are still under investigation, no formal feedback came from stakeholders in either 2006 or 2007. There were 73 money laundering convictions from January 2005 through October 2006. The trial court process has improved after several experienced judges received assignations specifically to handle EFCC cases; encouraged, EFCC officials have brought more cases to court. Additional information for 2007 is not available.

Due to the EFCC's activities, the enactment of new laws, and a public enlightenment campaign, crimes such as bank fraud and counterfeiting have been reported and prosecuted, sometimes for the first time. The EFCC is the agency with the most capacity to effectively investigate and prosecute financial crimes, including money laundering and terrorist financing. The EFCC coordinates agencies' efforts in pursuing financial crime investigations. In addition to the EFCC, the National Drug Law Enforcement Agency (NDLEA), the Independent Corrupt Practices Commission (ICPC), and the Criminal Investigation Department of the Nigeria Police Force (NPF/CID) are empowered to investigate financial crimes. Reportedly, the Nigerian Police Force is incapable of handling financial crimes because of alleged corruption and poor institutional capacity.

In 2007, the EFCC marked significant successes in combating financial crime. Through EFCC efforts, a former inspector general of police was arrested and prosecuted for financial crimes valued at over U.S. $13 million. The GON seized his assets and froze his bank accounts. Currently serving a prison sentence, he still faces 92 charges of money laundering and official corruption. Five former state governors are under investigation for money laundering. The EFCC is working with the FBI on a case involving a group of money brokers laundering money through banks in the United States. In 2006, the EFCC received a surge of petitions and leads provided by whistleblowers. Reportedly, many of

these alleged abuses of office involved politically exposed persons (PEPs) and/or their collaborators. As the period coincided with preparations for the general elections in 2007, some of the investigations were politically charged. The Legal and Prosecution Unit, responsible for the prosecution of all cases, is examining 437 of these cases for possible prosecution.

The Unit prosecuted several high profile cases involving powerful and well connected persons and their associates. The EFCC filed 588 cases between 2006 and mid-2007. In 2007, the Legal Unit had obtained 53 convictions by mid-year. Investigations led to the recovery of approximately 30 billion naira (approximately U.S. $259 million). Suspects returned several other billions of naira when it became apparent that the Commission was about to expose the abuses. Some governors were arrested for laundering their state government funds. The Executive Chairman, appearing before the Senate to present a report of the Commission's activities, revealed allegations of corrupt practices and abuse of office reportedly associated with 31 out of the 36 then serving Governors. Some of the Governors had constitutional immunity that expired in May 2007. They are now standing trial in various courts for various offenses including money laundering.

While the NDLEA has the authority to handle narcotics-related cases, it does not have adequate resources to trace, seize, and freeze assets. Cases of this nature are usually referred to the EFCC. Depending on the nature of the case, the tracing, seizing, and freezing of assets may be executed by the EFCC, NDLEA, NPF, or the ICPC. The proceeds from seizures and forfeitures pass to the federal government, and the GON uses a portion of the recovered sums to provide restitution to the victims of the criminal acts. The banking community is cooperating with law enforcement to trace funds and seize or freeze bank accounts. Since its establishment the EFCC has reportedly seized assets worth $5 billion.

Section 20 of the 2004 EFCC Act provides for the forfeiture of assets and properties to the federal government after a money laundering conviction. Foreign assets are also subject to forfeiture. The properties subject to forfeiture are set forth in EFCC Act Sections 24-26, and include any real or personal property representing the gross receipts a person obtains directly as a result of the violation of the act, or traceable to such receipts. They also include any property representing the proceeds of an offense under the laws of a foreign country within which the offense or activity would be punishable for more than one year. All means of conveyance, including aircraft, vehicles, or vessels used or intended to be used to transport or facilitate the transportation, sale, receipt, possession or concealment of the economic or financial crimes is likewise subject to forfeiture. Forfeiture is possible only as part of a criminal prosecution. There is no comparable law providing for civil forfeiture independent of a criminal prosecution, but the EFCC has established a committee addressing this deficiency by drafting legislation.

The EFCC has the authority to prevent the use of charitable and nonprofit entities as money laundering vehicles, although it has not reported any cases involving these entities.

Nigerian criminals initially made the advance fee fraud scheme infamous. Today, nationals of many African countries and from a variety of countries around the world also perpetrate advance fee fraud. While there are many variations, the main goal of 419 frauds is to deceive victims into the payment of a fee by persuading them that they will receive a very large benefit in return, or by persuading them to pay fees to "rescue" or help a newly-made "friend" in some sort of alleged distress. A majority of these schemes end after the victims have suffered monetary losses, but some have also involved kidnapping, and/or murder. Perpetrators use the Internet to target businesses and individuals around the world.

The Government of Nigeria continued throughout 2007 with its efforts to eradicate 419 crimes. GON efforts previously led to the successful prosecution and conviction of a number of them, but the problem is far from over. Following the promulgation of the Advance Fee Fraud Act 2006 the EFCC held an interactive session with stakeholders. The EFCC also briefed cyber cafe operators, business

centers, Internet service providers, telecommunication companies and banks on their responsibilities under the new law. One of their requirements is to register their businesses with the EFCC. To keep pace with the sophistication with which the fraudsters operate, the EFCC deployed interception technology to enhance the investigation of crimes, particularly those committed through cyberspace. The Advance Fee Fraud Unit burst several employment, credit card, and e-payment scams, shut down several domains and cloned websites, raided residential houses, seized computers, and blocked fraudulent e-mail addresses, telephone lines and faxes associated with cybercrimes. Despite the progress the EFCC has made, there have been few recorded successes as a result of the EFCC's cybercrime initiatives.

The EFCC's success in investigating and prosecuting financial crime, especially high-level corruption, has brought it both the support of the international community and the ire of corrupt officials. In December 2007, the Government of Nigeria reassigned the EFCC Chairman, the country's highest ranking and most publicly visible anti-corruption official, Nuhu Ribadu, to a year-long training course. This reassignment coincides with the high-profile trials of several officials, including seven former governors. Ribadu has served as the face of Nigerian AML/CTF efforts, and his removal could undermine the perception of the GON's commitment to fighting corruption. The reassignment of Ribadu may also impact the NFIU's autonomy and its ability to act independently.

Nigeria criminalized the financing of terrorism under the Economic and Financial Crimes Commission (Establishment) Act of 2004. The EFCC has authority under the act to identify, freeze, seize, and forfeit terrorist finance-related assets. Nigerian financial institutions periodically receive the UNSCR 1267 Sanctions Committee's consolidated list, but have not yet detected a case of terrorist financing within the banking system.

Nigeria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Nigeria has also ratified the African Union Convention on the Prevention and Combating of Terrorism and the African Union Convention on Preventing and Combating Corruption. Nigeria ranks 147 out of 180 countries in Transparency International's 2007 Corruption Perceptions Index.

The United States and Nigeria have a Mutual Legal Assistance Treaty, which entered into force in January 2003. Nigeria has signed memoranda of understanding with Russia, Iran, India, Pakistan and Uganda to facilitate cooperation in the fight against narcotics trafficking and money laundering. Nigeria has also signed bilateral agreements for exchange of information on money laundering with South Africa, the United Kingdom, and all Commonwealth and Economic Community of West African States countries. The EFCC worked with foreign partners to raid notorious cyber cafes to curtail the activities of the 419 fraudsters. The EFCC collaborated with the United States Postal Service and the UK Serious and Organized Crime Agency (SOCA) to intercept over 15,000 counterfeit checks. A collaboration scheme between the EFCC, the United States, the UK and the Dutch was constituted to more effectively address the problem of international fraud, including identity theft and e-marketing fraud. Nigeria is a member of the Intergovernmental Task Force against Money Laundering in West Africa (GIABA), a FATF-style regional body. During 2007, Nigeria held the Directorship General of GIABA. The NFIU is a member of the Egmont Group.

The Government of Nigeria continued to pursue money laundering both within and outside the country in 2007. Nigeria should continue to pursue its anti-corruption program and support both the ICPC and EFCC in their mandates to investigate and prosecute corrupt government officials and individuals. Nigeria should take steps to ensure the autonomy and independence of those entities. GON should strengthen the authority of the SCUML to supervise designated nonfinancial businesses and professions by moving the Special Control Unit out from under the Ministry of Commerce. The GON should continue to engage with the FATF and other relevant international organizations to identify and

eliminate remaining anti-money laundering deficiencies. Nigeria should ensure that the Police Force has the capacity to function as an investigative partner in financial crime cases, as well as work to eradicate any corruption that might exist within that and other law enforcement bodies. Nigeria should continue to support the EFCC's efforts, including drafting a law for civil forfeiture provisions to the AML/CTF framework, and pursuing those who commit financial crime, regardless of political status. Nigeria should continue towards implementation of a comprehensive AML 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, corruption and fraud are significant problems. Pakistan is a major drug-transit country. The abuse of the charitable 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 does not have firm control of its borders with Afghanistan, Iran and China, facilitating the flow of smuggled goods to the Federally Administered Tribal Areas (FATA) and Baluchistan. Some goods such as foodstuffs, electronics, building materials, and other products transiting Pakistan duty-free under the Afghan Transit Trade Agreement are sold illegally in Pakistan. Counterfeit goods generate substantial illicit proceeds that are laundered. Private unregulated charities are also a major source of illicit funds for international terrorist networks. Madrassas have been used as training grounds for terrorists and for terrorist funding. The lack of control of madrassas, similar to the lack of control of Islamic charities, allows terrorist and jihadist 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 purposes, although controls have been significantly tightened since 2002. In June 2004, the State Bank of Pakistan required all hawaladars to register as authorized foreign exchange dealers and to meet minimum capital requirements. Despite the State Bank of Pakistan's efforts, unlicensed hawaladars still operate illegally in parts of the country (particularly Peshawar and Karachi), and authorities have taken little action to identify and enforce the regulations prohibiting nonregistered hawaladars. Most illicit funds are transacted through these unlicensed operators. Fraudulent invoicing is typical in hundi/hawala counter valuation schemes. However, legitimate remittances from the roughly five million Pakistani expatriates residing abroad, sent via the hawala system prior to 2001, now flow mostly through the formal banking sector and have increased significantly to U.S. $5.5 billion in 2006-2007.

Pakistan has established a number of Export Processing Zones (EPZs) in all four of the country's provinces. Although no evidence has emerged of EPZs being used in money laundering, inaccurate invoicing is common in the region and could be used by entities operating out of these zones. In 2007, the Directorate General of Customs Intelligence (DGCI) investigated a well-known Pakistani business group involved with trade-based money laundering. The business over-invoiced the value and quantity of the exports of garments and textiles to Dubai and Saudi Arabia. The chairman of the business group and his partners held 49 percent shares in the Dubai-based company that imported many of the goods. The investigation also revealed that the business group used hawala to transfer large amounts of money and value through a prominent foreign exchange company based in Karachi. From 2001-2007, the value of the trade consignments totaled U.S. $330 million.

Pakistan has adopted measures to strengthen its financial regulations and enhance the reporting requirements for the banking sector to reduce its susceptibility to money laundering and terrorist financing. For example, financial institutions are required to follow "know your customer" provisions and must report within three days any funds or transactions they believe are proceeds of criminal activity.

Pakistan became a member of the Asia/Pacific Group on Money Laundering (APG) in 2000, therefore accepting the APG requirement that members develop, pass and implement anti-money laundering and counter-terrorist financing legislation and other measures based on accepted international standards. A high-level APG delegation visited Pakistan in early July 2007 to discuss Pakistan's long-delayed passage of comprehensive anti-money legislation. At its July plenary, APG members agreed that unless Pakistan enacts and proclaims into force consolidated AML legislation or issues a Presidential Ordinance prior to December 31, 2007, Pakistan's membership could be suspended.

On September 8, President Musharraf signed an ordinance to implement the long-awaited AML bill through a presidential ordinance. While creating this ordinance averted suspension of membership in the APG, Pakistan still has work ahead to meet international standards, especially the core FATF Recommendations related to the criminalization of money laundering and suspicious transaction reporting.

Some of the weaknesses identified in the new AML Ordinance include the following: Not all of the FATF designated categories of offenses (e.g., smuggling, racketeering, trafficking in persons, sexual exploitation, arms trafficking, and environmental crime) are covered as predicate offenses. The intent and knowledge requirement required to prove the offense of money laundering is not consistent with the standards set out in the Vienna and Palermo Conventions. Only the concealment of criminal proceeds is an offense, not the transfer of legitimate money to promote criminal activity. The definition of what constitutes a suspicious transaction is not adequate as it does not cover cases where an individual "suspects" or "has reason to suspect" that funds are the proceeds of criminal activity. The Ordinance also does not contain any specific requirement to report transactions in relation to terrorist financing. The forfeiture procedures set forth in the law are cumbersome and will inhibit the successful seizure and confiscation of property involved in offenses. Lastly, the reporting structure of the Financial Monitoring Unit may affect its independence and effectiveness.

The AML ordinance formally establishes a Financial Monitoring Unit (FMU) to monitor suspicious transactions. However, it is subject to the supervision and control of the General Committee, comprised of several Government of Pakistan (GOP) cabinet secretaries, thus limiting its independence. Because Pakistan has lacked a central repository for the reporting of suspicious transactions and the lack of protection from liability for reporting, very few suspicious transactions have been reported or utilized. From July 2006 through June 2007, 22 suspicious transactions were reported to the State Bank of Pakistan by various banks and five referred to law enforcement agencies for investigation. Currently, the FMU has yet to be fully staffed and investigators have not been adequately trained.

Several law enforcement agencies are responsible for enforcing financial crimes laws. The National Accountability Bureau (NAB), the Anti-Narcotics Force (ANF), the Federal Investigative Agency (FIA), and the Directorate of Customs Intelligence and Investigations (CII) all oversee Pakistan's financial enforcement efforts. In addition to the 2007 Anti-Money Laundering Ordinance, 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 criminalizes acts of money laundering associated with drug offenses and requires the reporting of narcotics related suspicious transactions. The NAB, FIA, ANF and customs have the ability to seize

assets whereas the State Bank of Pakistan has the ability to freeze assets. The ANF shares information about seized narcotics assets and the number of arrests with the USG.

Pakistan has also adopted measures to strengthen its financial regulations and enhance the reporting requirements for the financial sector to reduce its susceptibility to money laundering and terrorist financing. The State Bank of Pakistan and the Securities and Exchange Commission of Pakistan (SECP) are the country's primary financial regulators. They have established AML units to enhance financial sector oversight. However, these units often lack defined jurisdiction and adequate resources to effectively supervise the financial sector on AML/CTF controls. The State Bank of Pakistan has introduced regulations on AML that are generally consistent with the FATF recommendations in the areas of "know your customer" and enhanced due diligence procedures, record retention, the prohibition of shell banks, and the reporting of suspicious transactions. The Securities and Exchange Commission of Pakistan, which has regulatory oversight for nonbank financial institutions, has also applied "know your customer" regulations to stock exchanges, trusts, and other nonbank financial institutions.

Pakistan has specifically criminalized various forms of terrorist financing under the Anti-Terrorism Act (ATA) of 1997. Sections 11H-K provide that a person commits an offence if he is involved in fund raising, uses and possesses property, or is involved in a funding arrangement intending that such money or other property should be used, or has reasonable cause to suspect that they may be used, for the purpose of terrorism. Pakistan has the ability to freeze bank accounts and property held by terrorist individuals and entities. Pakistan has issued freezing orders for terrorists' funds and property in accordance with UN Security Council Resolutions 1267 and 1373. The State Bank of Pakistan circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. The ATA of 1997 also allows the government to proscribe a fund, entity or individual on the grounds that it is involved with terrorism. This done, the government may order the freezing of its accounts. Section 11B of the ATA specifies that an organization is proscribed or listed if the GOP has reason to believe that it is involved with terrorism. In 1997, 16 names were listed in annex to the ATA; none have been added since. As of 2006, bank accounts of 43 individuals and entities had been frozen under various UNSCRs. However, there have been some deficiencies concerning the timeliness and thoroughness of the asset freezing.

A Charities Registration Act has been under consideration by the Ministry of Welfare for some time. Currently, the Economic Affairs Division of the Ministry of Finance is reviewing the draft text and will then forward the bill to the Ministry of Law for review. The bill will then require approval by the cabinet and National Assembly, unless issued as a Presidential Ordinance by the President. 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 of Social Welfare 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.

Current efforts to crack down on the flow of illicit funds via charitable organizations are limited to closure of the charity. There is little follow-up on suspect individuals associated with charities in question, thus allowing them to operate freely under alternate names. The court system has also failed to affirm Pakistan's international obligations and maintain closure of UN-proscribed charitable organization. In one such case, a provincial court in Karachi permitted a charity to continue operating in the face of a closure order, provided the charity in question only engaged in humanitarian operations. The GOP failed to aggressively appeal this court decision.

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. The State Bank of Pakistan legally allows individuals to carry up to U.S. $10,000 in dollars or

the foreign currency equivalent. In tracking the cross border movement of currency Pakistan currently has reporting requirements only for the exportation of currency not the importation of currency. Although there is no requirement for the inbound reporting of currency, Pakistan is in compliance with FATF's Special Recommendation IX as they have the ability to ask anyone entering Pakistan if they are bringing in any currency. There are joint counters at international airports staffed by the State Bank of Pakistan and Customs to monitor the transportation of foreign currency. As a result of cash courier training received by Pakistan in 2006, their efforts to stop and seize the illicit cross-border movement of cash have increased. For example, during 2007 authorities made a number of significant cash seizures at the international airports in Karachi, Lahore and Peshawar as well as land border crossings.

Pakistan is party to the 1988 UN Drug Convention and the UN Convention against Corruption and has signed, but not ratified, the UN Convention against Transnational Crime. Pakistan is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism. Pakistan is ranked 138 out of 180 countries monitored in Transparency International's 2007 Corruption Perception Index.

Although the Government of Pakistan has adopted a long-awaited AML ordinance by presidential decree after years of delay and stall tactics, the GOP needs to amend the current AML Ordinance or pass additional legislation to remedy the number of deficiencies which exist, ensure that the legal provisions are made permanent, and make it fully compliant with international standards. The Presidential Ordinance was valid for only four months and was due to expire in early January 2008. At expiry, the AML Ordinance must be "re-enacted" or ratified by the National Assembly. Pakistan's Financial Monitoring Unit (FMU) needs to be further staffed and strengthened and should be given operational autonomy rather than subject to the supervision and control of the General Committee, comprised of political ministers. The GOP should also issue implementing regulations to consolidate and de-conflict the reporting obligations of suspicious transactions contained in various laws and regulations. Since few suspicious transaction reports are filed, Pakistan should not become dependent on these reports to initiate investigations but rather law enforcement authorities should be proactive in pursuing money laundering in their field investigations. In light of the role that private charities have played in terrorist financing, Pakistan must work quickly to conduct outreach, supervise and monitor charitable organizations and activities, and close those that finance terrorism. In accordance with FATF Special Recommendation IX, Pakistan should implement and enforce cross-border currency reporting requirements and focus greater efforts in identifying and targeting illicit cash couriers. Pakistan should also become a party to the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of Terrorist Financing.

Palau

Palau is an archipelago of more than 300 islands in the Western Pacific with a population of 20,900 (approximately 5,000 of which are foreign guest workers) and per capita GDP of about U.S. $7,000 (a large percentage of which comes from international financial assistance).

Upon its independence in 1994, the Republic of Palau entered the Compact of Free Association with the United States. The U.S. dollar is the legal tender used by the country, though it is not the official currency of Palau. 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. Palauan authorities 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, human 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 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. Two years after the introduction of proposed amendments, an amended MLPCA was signed into law on December 19, 2007.

The original act did not establish requirements for the recording of cash and bearer securities transactions of U.S. $10,000 and above, and only required the reportage of suspicious transactions in excess of U.S. $10,000. The MLPCA did mandate that records be kept for five years from the date of the transaction. All such transactions (domestic and international) are required to go through a credit or financial institution licensed under the laws of the Republic of Palau. 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 be confirmed, the transaction must cease immediately.

The amended MLPCA, in addition to generally tightening up the original law, now sets higher standards for record keeping, requires the recording of cash and bearer securities transactions in excess of U.S. $10,000, removes the dollar threshold on suspicious transactions and requires "alternative remittance systems" to be licensed and maintain records of all transactions in excess of U.S. $1,000. The amendment also requires currency transactions over U.S. $5,000 to be effected by wire transfer and also authorizes the Financial Institutions Commission (FIC) to conduct random compliance audits on credit or financial institutions. Palau also monitors cross border transportation of currency through a declaration form requiring travelers to declare U.S. $10,000 or more.

The MLPCA defined offenses of money laundering as: 1) conversion or transfer of property for the purpose of concealing its illegal origin; 2) concealing or disguising the illegal nature, source, location, disposition, or ownership of property; and 3) acquisition, possession, or control of property by any person who knows that the property constitutes the proceeds of crime as defined in the law. The law provides for penalties of a fine not less than U.S. $5,000, nor more than double the amount the convicted individual laundered or attempted to launder, whichever is greater, or imprisonment of not more than 10 years, or both. Corporate entities or their agents are subject to a fine double that specified for individuals. The law protects individuals who report suspicious transactions.

The Financial Institutions Act of 2001 established the Financial Institutions Commission (FIC), an independent regulatory agency, which is responsible for licensing, supervising and regulating financial institutions, defined as banks and security brokers and dealers in Palau. An amendment intended to strengthen the supervisory powers of the FIC and promote greater financial stability within Palau's banking sector passed its first reading in the Senate in January 2005. The Senate Committee on Ways and Means and Financial Matters did not report out the bill until December 2006 when it merely referred it back to the Committee for further study. This amendment still has not become law. The insurance industry is not currently regulated by the FIC. Most insurance companies in Palau are companies registered in the U.S. or the U.S. Territory of Guam.

The Free Trade Zone Act of 2003 created the Ngardmau Free Trade Zone (NFTZ). A public corporation, Ngardmau Free Trade Zone Authority, was established to oversee the development of the NFTZ. The Authority also issues licenses for businesses to operate within the free trade zone. Businesses licensed to operate within the free trade zone will not be subject to the requirements of the Foreign Investment Act and will be exempt from certain import and export taxes. No development has taken place within the area designated for the free trade zone and the NFTZ directors continue to search for developers and investors.

Currently there are seven licensed banks in Palau, the majority ownership of which is primarily foreign. The three largest retail banks—Bank of Hawaii, Bank of Guam and BankPacific are all branches of American banks. In addition there are three banks chartered in Palau (Asia Pacific Commercial Bank, First Fidelity Bank and Palau Construction Bank) and one chartered in Taiwan (First Commercial Bank.)

On November 7, 2006, the FIC closed the second largest and the only locally owned bank, Pacific Savings Bank (PSB), for illiquidity and insolvency. The Receiver and a Special Prosecutor hired specifically for the purpose of developing cases related to the failure of PSB have filed a number of civil and criminal actions against former bank managers and insiders. An additional five to ten cases are currently being prepared. Investigations and litigation, though hampered by lack of resources, continue.

With the legal framework now being made more robust, the weakest link in Palau's money laundering prevention regime is the paucity of human and fiscal resources. The operations of the government's Financial Intelligence Unit (FIU) are severely restricted by a lack of dedicated human resources and no dedicated budget. The FIU works under the Office of the Attorney General and is responsible for receiving, analyzing, and processing suspicious transaction reports, and disseminating the reports as necessary. In addition, the FIU is responsible for tracing, seizing, and freezing assets.

Another impediment to enforcement is the lack of implementing regulations to ensure compliance with the amended MLPCA. With the passage of the 2007 amendment, however, these can now be developed.

The will of the Executive branch to comply with international standards 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 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 Taiwan and the Philippines for mutual sharing of information and interagency cooperation in relation to financial crimes and money laundering.

In 2004 The President also sent the Cash Courier Act, drafted by the Palau Anti-Money Laundering Working Group, to the legislature. 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, like the bill intended to strengthen the FIC, it remains.

The Counter-Terrorism Act of 2007 includes 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 Counter-Terrorism Act specifically addresses Palau's obligation under UN Security Council Resolution 1373. Palau is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Under the Act, acts of terrorism that cause loss of life are punishable by a prison term of 20 years to life and a maximum fine of U.S. $1,000,000. All other acts of terrorism are punishable by a prison term of 10 years to life and a maximum fine of U.S. $1,000,000.

Donations over U.S. $5,000 to any nonprofit organization are to be recorded. The organization must maintain the record for 3 years and must provide it to the FIU upon request. Donations over U.S. $10,000 are to be reported to the Office of the Attorney General and FIU. Any suspicious donations are also to be reported to the Office of the Attorney General and FIU. Penalties for violations are: 1) a fine not to exceed U.S. $10,000; 2) a temporary ban on operations for up to 2 years; or 3) the dissolution of the organization.

The Government of Palau (GOP) has taken several steps toward enacting a legal framework by which to combat money laundering. The GOP should circulate the UNSCR 1267 Sanctions Committee Consolidated list of terrorist entities. The GOP should provide more resources to its FIU, and provide more assistance to and proactively support the work of the Pacific Savings Bank Special Prosecutor. The GOP should enact the Cash Courier Act and carefully monitor its border points of entry and exit to protect against the smuggling of bulk cash, narcotics and other contraband. The GOP should also implement all aspects of the legal reforms already 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. Panama is also an important regional financial center. Panama's economy is 77 percent service-based, 15 percent industry and 8 percent agriculture. The maritime sector, construction, tourism, and banking are among Panama's most important and fastest growing sectors. Panama has had one of the fastest growing economies in the Western Hemisphere over the last 15 years, and is estimated to have the fastest growing economy in the region during 2007, with GDP growth approaching 10 percent. The funds generated from illegal activity are susceptible of being laundered through a wide variety of methods in Panama, including the banking system, casinos, bulk cash shipments, pre-paid telephone cards, debit cards, ATM machines, insurance companies, and real estate projects and agents.

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 is the world's second largest free zone after Hong Kong, and 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. The CFZ has over 2,600 business, 25 bank branches, and employs approximately 25,000 personnel. The CFZ is estimated to have imported and re-exported over U.S. $15 billion in goods during 2007. The ports of Panama handle over 4 million twenty-foot equivalent units (TEUs) of container traffic per year. The CFZ has limited resources to conduct supervisory programs and monitor for illegal activities, with a legal staff of approximately five people who, among other things, oversee efforts to detect money laundering, transshipment, goods smuggling, counterfeit products and intellectual property rights violations.

Panama is one of the world's largest offshore financial centers. Panama's offshore financial sector includes international business companies, offshore banks, captive insurance companies and fiduciary companies. Approximately 34,800 new offshore corporations were registered in Panama in 2007, as of October 2007. As of June 2007, Panamas had 85 commercial banks: 2 official banks, 14 local banks of general license, 26 foreign banks of general license, 34 banks of international license, and nine representative offices. Shell companies are permitted and have been used by a wide range of criminal groups around the world. Bearer shares are permitted for corporations and nominee directors and trustees as are allowed by law. The Government of Panama (GOP) regulates casinos, but does not regulate Internet gaming sites.

Law No. 42 of 2000 requires Panamanian trust companies to identify to the Superintendence of Banks the real and ultimate beneficial owners of trusts. Executive Decree 213 of 2000, amending Executive Order 16 of 1984, provides for the dissemination of information related to trusts to appropriate administrative and judicial authorities. Both the onshore and offshore financial entities are subject to similar regulation by the Superintendence of Banks. The onshore and offshore registration of corporations is also handled by the Public Registry. There are no differing regulations governing onshore and offshore corporations. The application process for a banking license in favor of a bank to be constituted in Panama and a banking license in favor of a foreign bank are substantially the same.

Panama's construction sector, which is growing at double-digit rates, is also susceptible to money laundering activities. In Panama City alone, there is either in process or approved the construction of over 150 buildings of twenty stories or greater. It is estimated that approximately 20,000 high-end condominium units will enter the Panamanian real estate market within the next five years. The bulk of these units are for purchase by foreigners. The developer of one residential project (Resort Paraiso Las Perlas on Isla Chapera in the Gulf of Panama), Jose Nelson Urrego Cardenas, was arrested in 2007 on drug money laundering charges.

Money laundering is a criminal offense in Panama under Law No. 41 of October 2000. Law 41 amends the Penal Code by expanding the predicate offenses for money laundering beyond narcotics trafficking to include criminal fraud, arms trafficking, trafficking in humans, kidnapping, extortion, embezzlement, corruption of public officials, terrorism and international theft or trafficking of motor vehicles. Law No. 1 of 2004 also adds crimes against intellectual property as a predicate offense for money laundering. In May 2007, Law No. 14 was adopted, establishing terrorist financing as a predicate offense for money laundering. Law 41 establishes a 5 to 12 year prison sentence, plus possible fines. Law No. 45 of 2003 also establishes criminal penalties of up to ten years in prison and fines of up to one million dollars for financial crimes that undermine public trust in the banking system, the financial services sector, or the stock market. This law criminalizes a wide range of activities related to financial intermediation, including the following: illicit transfers of monies, accounting fraud, insider trading, and the submission of fraudulent data to supervisory authorities.

Law No. 42 of 2000 requires financial institutions (banks, trust companies, money exchangers, credit unions, savings and loans associations, stock exchanges and brokerage firms, and investment administrators) to report currency transactions in excess of U.S. $10,000 and suspicious financial transactions to Panama's financial intelligence unit, the Unidad de Análisis Financiero (UAF). Law 42 also mandates casinos, CFZ businesses, the national lottery, real estate agencies and developers, and insurance and reinsurance companies report to the UAF currency transactions that exceed U.S. $10,000. Furthermore, Law 42 requires Panamanian trust companies to identify to the Superintendent of Banks the beneficial owners of trusts. Additionally, Law 16 of 2005, which regulates the activities of pawnshops, requires such enterprises to report suspicious transactions to the UAF. Financial institutions are prohibited from informing their client or third parties that they have transmitted any information regarding such transactions to the UAF. Law 42 protects reporting entities from civil and criminal suits with respect to providing the information required by the law and otherwise cooperating with law enforcement entities.

The Superintendent of Banks is responsible for supervising both onshore and offshore financial institutions with regard to their anti-money laundering and counter-terrorist financing (AML/CTF) requirements. In 2000, Panama's Superintendence of Banks issued Agreement No. 9 of 2000 that defines requirements that banks must follow for identification of customers, exercise of due diligence, and retention of transaction records and increased the number of finance company inspections. In 2005, the Superintendence of Banks modified that Agreement, to include fiduciary companies within the prevention measures and to bring the banking center into line with international standards and Financial Action Task Force (FATF) recommendations. Financial institutions must have sufficient information to adequately identify their customers. They must examine every cash (or cash equivalent) transaction in excess of $10,000 or a series of transactions that in the aggregate exceed U.S. $10,000 in any given week. Additionally, they must examine with special attention, any transaction, regardless of amount, which could be related to money laundering activity. Financial institutions must also establish procedures and mechanisms for internal controls to prevent money laundering related activities. Financial institutions must also insure that their employees are aware of these laws and regulations.

A number of other supervisory bodies have regulatory responsibility for AML/CTF compliance purposes. The Ministry of Commerce and Industry is responsible for supervising money remittance houses, financing companies, real estate promoters and agents, pawnshops, and companies located in enterprise processing zones. The Panamanian Autonomous Cooperative Institute supervises savings and loan cooperatives, and has established a specialized unit for the supervision of loans and credit cooperatives regarding compliance with Law 42. The National Securities Commission supervises securities firms, stockbrokers, stock exchanges and investment managers, and carries out various training sessions and workshops for its personnel and related entities. The Gaming Commission supervises casinos and other establishments dedicated to betting and games of chance. The Colon Free Zone Authority supervises the companies and activity within the CFZ, and has issued a procedures manual for all CFZ businesses, outlining their responsibilities regarding the prevention of money laundering and the requirements of Law 42. The Superintendence of Insurance supervises insurance companies, reinsurance companies, and insurance brokers.

Executive Decree No. 136 of 1995 establishes the UAF. The UAF falls under the jurisdiction of the GOP's Council for Security and National Defense within the Ministry of the Presidency. The UAF currently has approximately 25 employees. During 2007, the UAF reinforced the analysis department by hiring two new accountants, a financial analyst, and a lawyer. Also, the statistics and typology departments have newly trained personnel. Despite these additions, the UAF is overworked and understaffed, lacks adequate resources, and suffered the loss of experienced personnel in 2007.

The UAF works with other GOP agencies to identify new methods of money laundering and terrorist financing, and participates in the training of financial and nonfinancial sector employees in detecting and preventing money laundering and terrorist financing. During the first six months of 2007, the UAF trained 1,476 individuals, 59 percent of which were banking employees, 29 percent of which were government employees, and 12 percent of which were financial service employees.

The UAF has access to the records or databases of other government entities that have public websites or public investigative offices. The UAF has online access with other GOP entities to access information from the public registry, traffic department, electoral tribunal, as well as information on immigration movements and travelers' declarations of the cross-border transportation of currency. The UAF may also request additional information from financial institutions in writing.

Once the UAF has reviewed all cash transaction reports (CTRs) or suspicious transaction reports (STRs) and gathered any other relevant information from reporting institutions and other government agencies, the UAF provides information related to possible money laundering or terrorist financing to the Office of the Attorney General for investigation. Money laundering cases involving narcotics are

handled by the Drug Prosecutor's Office within the Office of the Attorney General. The Judicial Technical Police (Sección de Investigaciones Financieras, or SIF, similar in function to the Federal Bureau of Investigation) provides expert assistance to the prosecutors. The UAF routinely transfers cases to the financial investigations unit of the SIF for investigation.

As of November, the UAF received 1,012 STRs in 2007, of which 170 were sent to the Attorney General's Office for further action. During all of 2006, the UAF investigated 935 suspicious transaction reports (843 from banks), of which 158 were sent to the Attorney General's Office. During the second quarter of 2007, the UAF received 63,752 CTRs, a 3.8 percent increase from the same period in 2006. The total amount reported via CTRs during the first six months of 2007 was $2.7 billion, a 46.9 percent increase from the same period in 2006. Approximately 91 percent of the reports came from banks, and 4.5 percent from exchange houses. The UAF attributes the increase in CTRs to the growth in the Panamanian economy. As of October, the Drug Prosecutor's Office reported 43 drug-related money laundering arrests in 2007.

Under Panamanian customs regulations, any individual bringing cash in excess of $10,000 into Panama must declare such monies at the point of entry. If such monies are not declared, they are confiscated and are presumed to relate to money laundering. Some GOP officials have expressed concern at the millions of dollars in cash they have seen brought into Panama from Colombia. The actual movement/transfer of this cash is legal insofar that it was declared to both Colombian and Panamanian customs. However, the GOP maintains that it cannot vouch for the legitimate origins of said cash. All instances of cash smuggling are required to be reported into a database maintained by Panamanian customs.

On August 10, 2007, Law 38 entered into force. Law 38 provides for the seizure of assets derived from criminal activity. Upon an arrest, assets are frozen and seized. The assets are released upon a judge's order to the defendant in the event of a dismissal of charges or acquittal. In the event of a conviction, assets derived from money laundering activity related to narcotics trafficking are delivered to the National Commission for the Study and Prevention of Narcotics Related Crimes (CONAPRED) for administration and distribution among various GOP agencies. Seized perishable assets may be sold and the proceeds deposited in a custodial account with the National Bank. Responsibility for tracing, seizing and freezing assets lies principally with the Drug Prosecutor's Office of the Attorney General's Office. The GOP has not enacted legislation allowing for civil forfeiture or the sharing of seized assets with other governments.

Law 50 of 2003 criminalizes the financing of terrorism. Under Law 14 of May 2007, terrorist financing and terrorist acts, among other offenses, are now predicate offenses for money laundering. Panama circulates to its financial institutions the list of individuals and entities included on the United Nations Security Council Resolution 1267 Sanctions Committee list. The Ministry of Foreign Relations sends the UAF and the Superintendence of Banks a copy of a diplomatic note or letter with the names of terrorist organizations or financiers designated by the U.S. Government or the UN. The UAF in turn sends it to the appropriate regulators, who in turn send it to the regulated entities. The GOP does not have an independent national system or mechanism for freezing terrorist assets.

Executive Decree 524 of 2005, as amended by Executive Decree 627 of 2006, establishes procedures to regulate, supervise, and control nongovernmental organizations and charities, including regulatory procedures to combat terrorism and prevent terrorist financing. Press reports, however, have questioned the degree to which the nongovernmental organizations are complying with their reporting and registration requirements.

Decree No. 22 of June 2003, gave the Presidential High Level Commission against Narcotics Related Money Laundering responsibility for combating terrorist financing. The Panama Public Force (PPF) and the judicial system have limited resources to deter terrorists, due to insufficient personnel and lack of expertise in handling complex international investigations. The GOP has a border security

cooperation agreement with Colombia, and has also increased funds to the PPF to help secure the frontier. The GOP also created within the Ministry of Foreign Affairs the Department of Analysis and Study of Terrorist Activities. This department is tasked with working with the United Nations and the Organization of American States to investigate transnational issues, including money laundering. Panama has an implementation plan for compliance with the FATF Forty Recommendations on Money Laundering and its Nine Special Recommendations on Terrorist Financing.

Panama and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. The GOP has also assisted numerous countries needing help in strengthening their anti-money laundering programs, including Guatemala, Costa Rica, Russia, Honduras, and Nicaragua. Executive Decree No. 163 authorizes the UAF to share information with FIUs of other countries, subject to entering into a memorandum of understanding or other information exchange agreement. The UAF has signed more than 43 memoranda of understanding with foreign FIUs, including the Financial Crimes Enforcement Network (FinCEN), the U.S. FIU.

Panama is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD), and the Caribbean Financial Action Task Force. Panama is also a member of the Offshore Group of Banking Supervisors, and the UAF is a member of the Egmont Group. Panama is a party to the 1988 UN Drug Convention, 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.

The Government of Panama has a comprehensive legal framework to detect, prevent, and combat money laundering and terrorist financing, and cooperates with the United States and other countries with criminal investigations of drug trafficking, money laundering, and financial crimes. Panama nonetheless remains vulnerable to money laundering owing to its lack of adequate enforcement, personnel and resources, the sheer volume of economic transactions, its location as a major drug transit country, and corruption. The GOP should consider adopting legislation that allows for civil forfeiture and the freezing of terrorist assets, and enhance law enforcement efforts to address such vulnerabilities as smuggling, abuse of the real estate sector, trade-based money laundering, and the proliferation of nontransparent offshore companies. The GOP should also ensure that the UAF and other law enforcement and regulatory entities have sufficient personnel and resources.

Paraguay

Paraguay is a principal money laundering center involving the banking and nonbanking financial sectors. The multi-billion dollar contraband trade that occurs on the borders shared with Argentina and Brazil, the Tri-Border Area, facilitates much of the money laundering in Paraguay. Paraguay is a major drug-transit country. The Government of Paraguay (GOP) suspects 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, open borders, and minimal enforcement activity for financial crimes allow money launderers and terrorist financiers to take advantage of Paraguay's financial system.

Ciudad del Este (CDE), on Paraguay's border with Brazil and Argentina, represents the heart of Paraguay's informal economy. The area is well known for arms and narcotics trafficking and violations of 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, computer software, and games, are imported from Asia and transported across the border into Brazil, with a 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 involved in smuggling contraband or pirated goods.

Paraguay is particularly vulnerable to money laundering, as little personal background information is required to open a bank account or to conduct financial transactions. 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. Offshore banking in Paraguay is illegal. While casinos exist, offshore casinos do not, and Internet gambling is marginal, largely due to limited Internet connectivity throughout the country. Shell companies and trust funds structures are legal but are seldom used and uncommon in the financial system. At present, the financial sector seems to lack the depth and sophistication to use these structures. The nonbank financial sector operates in a weak regulatory environment with limited supervision. Credit unions or "cooperatives" are one of the main nonbank agents in the economy, rapidly growing in membership and representing over 20 percent of deposits and 33 percent of loans in the financial system. The organization responsible for regulating and supervising credit unions, the National Institute of Cooperatives (INCOOP), is an independent body that provides regulatory and supervisory guidelines, but lacks the capacity to enforce compliance. Exchange houses are another nonbank sector where enforcement of compliance requirements remains limited.

On December 20, 2007, Paraguay's Congress approved a new penal code that includes enhanced legislation on money laundering. In January 2008, the President of Paraguay signed the law and it entered into force. Under the new penal code, money laundering is an autonomous crime, punishable by a prison term of up to five years. The new code establishes predicate offenses for money laundering, but does not require a conviction for the predicate offense before initiating money laundering charges. The law also allows the state to charge financial sector officials who negligently permit money laundering to occur. Under Paraguayan law, the implementation of the new penal code will be delayed for one year to allow for the training of judges and prosecutors.

Another bill amending Paraguay's criminal procedure code is expected in early 2008, and terrorist finance legislation is also expected as a separate bill in 2008, after efforts to include it in the proposed penal code reforms failed in 2007. The proposed amendments to the criminal procedure code would move Paraguay towards a more accusatory system. The reforms would allow criminal investigations to occur without advance notice of the investigation to the subject or the defense attorney, it would lengthen statutes of limitation, and it would allow for confrontation and cross examination of witnesses.

There are other challenges, however, that the proposed money laundering legislation will not address, including limited resources and training. Paraguay added three financial crimes prosecutors in 2007, bringing the total number to 11, but prosecutors still face resource constraints that limit their ability 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 judicial system to its advantage. Now that the new anti-money laundering legislation has been passed as part of the new penal code, training for judges and prosecutors is key to Paraguay's future prosecutorial successes.

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 forms issued by airlines at the time of entry into Paraguay. Persons transporting U.S. $10,000 into or out of Paraguay are required to file a customs report, but these reports are not collected or checked. Customs operations at the airports or land ports of entry provide no control of cross-border cash movements. The nonbank financial sector (particularly exchange houses) is used to move illegal proceeds both from within and outside of Paraguay into the U.S. banking system. 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 beginning to recognize and address the problem of the international transportation of currency and monetary instruments derived from illegal sources.

Bank secrecy laws in Paraguay do not prevent banks and financial institutions from disclosing information to bank supervisors and law enforcement entities. Bankers and others are protected under the anti-money laundering law with respect to their cooperation with law enforcement agencies. 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 are required to know and record the identity of customers engaging in significant currency transactions. These entities must also report suspicious activities to Paraguay's financial intelligence unit (FIU), the Unidad de Análisis Financiera (UAF) within the Secretariat to Combat Money Laundering (SEPRELAD) of the Ministry of Industry and Commerce (MIC). The Superintendence of Banks enforces these reporting obligations for banks, but they are not enforced for other financial institutions. In November 2007, the MIC issued new regulations that define reporting requirements and sanctions for noncompliance for the insurance industry and credit unions.

In recent years, the GOP has made significant efforts to strengthen SEPRELAD, but weak leadership and suspicious activity caused SEPRELAD to falter in the first half of 2007, resulting in a halt in information sharing and the departure of several analysts. The GOP dismissed SEPRELAD's director and appointed a new director, former Central Bank president Gabriel Gonzalez, in August 2007. SEPRELAD received over 3,600 suspicious activity reports (SARs) in 2007, but its former director left a backlog of over 3,000 SARs not entered into its system. Director Gonzalez has now updated the system by entering the entire backlog of SARs. He has hired new analysts, who have been vetted and are being trained. SEPRELAD has drafted a bill, not yet pending before Congress, which would make it an independent secretariat reporting directly to the president. SEPRELAD is also hampered by a lack of effective inter-agency cooperation, as there is no formal mechanism for sharing sensitive information. Director Gonzalez is working on creating information sharing mechanisms within the Paraguayan government law enforcement agencies.

SEPRELAD is seeking to strengthen its relationship with other financial intelligence units and has signed agreements for information exchange with regional FIUs. However, its relationship with international and regional anti-money laundering groups, including the Egmont Group and the Financial Action Task Force for South America (GAFISUD), is tenuous. As a result of the GOP's failure to pay any of its dues dating back to 2002 (totaling approximately U.S. $76,000), GAFISUD placed sanctions on Paraguay in July and suspended its membership on December 1. However, the GOP made a partial payment of its dues after the December 1 deadline, and GAFISUD agreed to reinstate its membership on the condition that the remainder of its arrears will be paid by July 2008. Likewise, while SEPRELAD has been a member of the Egmont Group since 1998, it may be suspended from the Egmont Group in May 2008 if the GOP fails to approve terrorist financing legislation.

Paraguay has taken some measures to tackle illicit commerce and trade in the informal economy and to develop strategies to implement a formal, diversified economy. Transparency International Corruption Perceptions Index ranks Paraguay at number 138 of the 180 countries ranked. The GOP has signed an agreement with the Millennium Challenge Corporation for a $34.9 million Threshold Program to address corruption problems of impunity and informality, both of which hamper law enforcement efforts and contribute to money laundering. Paraguay's 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. The MIC's Specialized Technical Unit (UTE), working in close coordination with the Attorney General's Trademarks and Intellectual

Property Unit, seized U.S. $51 million worth of pirated goods during the first ten months of 2007. The Attorney General's Trademarks and Intellectual Property Unit initiated criminal proceedings in 110 cases, but most offenders paid a fine instead of serving jail time. In cooperation with the U.S. Department of Homeland Security's Agency of Immigration and Customs Enforcement (ICE), the GOP established a Trade Transparency Unit (TTU) that examines discrepancies in trade data that could be indicative of customs or tax fraud, trade-based money laundering, or the financing of terrorism. ICE estimates that U.S. $20 million left Paraguay for the U.S. on a daily basis in 2006, but less than U.S. $1 million was reported coming in.

Under its current 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 defendant is convicted. 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 the suspect's liability to the government. In the past few years, the anti-narcotics agency, SENAD, has been permitted on a temporary basis to use assets seized in pending cases, but SENAD cannot fully use such assets because the law does not permit the assets to be maintained or repaired. New asset forfeiture legislation is required to make improvements in this regard.

The GOP has no authority to freeze, seize, or forfeit assets related to the financing of terrorism, which is not a criminal offense under Paraguayan law. However, the Ministry of Foreign Affairs often provides the Central Bank and other government entities with the names of suspected terrorists on the UNSCR 1267 Sanctions Committee list. To date, the GOP has not identified, seized, or forfeited any 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.

The GOP has been slow to recognize terrorist financing within its borders. In December 2006, the U.S. Department of Treasury designated nine individuals and two companies operating in the Tri-Border Area as entities that provide financial and logistical support to Hezbollah. The nine individuals have all provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was designated by the U.S. Treasury in June 2004 for his support to Hizballah leadership. Two companies, Galeria Page and Casa Hamze, are located in Ciudad del Este and are used to generate or move terrorist funds. The GOP publicly disagreed with the designations, stating that the U.S. has not provided any new information that would prove terrorist financing activity occurs in the Tri-Border Area.

In spite of limitations in prosecuting suspected terrorist financiers such as Assad Ahmad Barakat and Kassem Hijazi, who were charged with tax evasion rather than terrorist financing or money laundering, the GOP is making improvements in its ability to successfully investigate and prosecute some money laundering cases. Leoncio Mareco was sentenced to 20 years in prison on August 14, 2007, for drug trafficking and money laundering. His wife, Zulma Rios de Mareco, was sentenced to 10 years in prison for money laundering. According to GOP authorities, the General Attorney's office has eight other active cases pending. These cases reinforce the fact that convictions are possible, although difficult, under the current legal framework.

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 the "3

Plus 1" Security Group between the United States and the Tri-Border Area countries. The GOP is a member of GAFISUD, and SEPRELAD is a member of the Egmont Group.

The Government of Paraguay took a number of positive steps in 2007 to combat money laundering, particularly with the passage of the new penal code and the GOP's money laundering convictions. However, it should continue to pursue other initiatives to increase its effectiveness in combating 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. The GOP should take steps to ensure that the penal and procedural code reforms are approved and implemented, allowing for a more effective anti-money laundering regime. 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 and counter-terrorist financing legislation is introduced again and adopted. Paraguay also should continue its efforts to combat corruption and increase information sharing among concerned agencies .It should also take the necessary steps to ensure that its Trade Transparency Unit is comprised of vetted employees from all relevant agencies, including SEPRELAD. Further reforms in the selection of judges, prosecutors and public defenders are needed, as well as reforms to the customs agency to allow for increased inspections and interdictions at ports of entry and to develop strategies targeting the physical movement of bulk cash. The GOP should also ensure that its GAFISUD dues are paid, preventing suspension of its membership. It is essential that SEPRELAD continues to receive the financial and human resources necessary to operate as an effective, fully functioning financial intelligence unit capable of combating money laundering, terrorist financing, and other financial crimes.

Peru

Peru is not a major regional financial center, nor is it an offshore financial center. 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. 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 annually, or up to 2.5 percent of Peru's GDP. As a result, money laundering is believed to occur on a significant scale 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. Approximately 60 percent of the economy is informal and approximately 65 percent 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. There have not been any official studies to establish an approximate percentage of the relationship between money laundering and drug trafficking. However, reports sent from Peru's financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), to the Public Ministry (Attorney General's office) indicate that approximately 45 percent of the money laundering cases have connections to criminal activity stemming from the drug trade.

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 and Insurance, and the Peruvian Congress have conducted numerous investigations, some of which are ongoing, involving dozens of former GOP officials.

Law 27.765 of 2002 criminalizes money laundering in Peru. Prior to its passage, money laundering was only a crime when directly linked to narcotics trafficking, "narcoterrorism," and nine specific predicate offenses that did not include corruption, bribery, or fraud. Law 27.765 expands the predicate offenses for money laundering 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 prosecutors 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.

Law 27.765 also revises the penalties for money laundering in Peru. 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.

The UIF began operations in June 2003 and today has approximately 48 personnel. In June 2007, the UIF was incorporated into the Office of the Superintendent of Banks and Insurance and a new director was appointed. 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 1,179 STRs in 2006, and 1,007 from January through September 2007.

Obligated entities must also maintain reports on large cash transactions. Individual cash transactions exceeding U.S. $10,000 or transactions totaling U.S. $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. Nonfinancial institutions, such as exchange houses, casinos, lotteries or others, must report individual transactions over U.S. $2,500 or monthly transactions over U.S. $10,000. Individuals or entities transporting more than U.S. $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. Any cash transactions that appear suspicious must be reported to the UIF. These reporting requirements are not being strictly enforced by the responsible GOP entities. However, the UIF is able to sanction persons and entities for failure to report suspicious transactions, large cash transactions, or the transportation of currency or monetary instruments.

The UIF does not automatically 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 U.S. $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.

Law 28.306 of 2004 mandates that obligated entities also report suspicious transactions related to terrorist financing, and expanded the UIF's functions to include the ability to analyze reports related to terrorist financing. In July 2006, the GOP issued Supreme Decree 018-2006-JUS to better implement Law 28.306. The decree also introduces the specific legal framework for the supervision of obligated entities with regard to combating terrorist financing.

Law 28.306 establishes regulatory responsibilities for the UIF. Most obligated 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. Under Supreme Decree 018-2006-JUS, the UIF may participate in the on-site inspections of obligated entities performed by the supervisory body. 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 UIF can also request that a supervisor review an obligated entity that is not under its supervision. 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.

In spite of the expanded regulatory responsibilities of the UIF, some obligated 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 U.S. $200,000) in transfers per year, and remittances conducted through postal or courier services are supervised by the Ministry of Transportation and Communications. As a result, informal remittance businesses, including travel agencies and small wire transfer 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.

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. The UIF disseminates STRs and other reports that require further investigation or prosecution to the Public Ministry.

Within the counternarcotics section of the Public Ministry, two specialized prosecutors are responsible for dealing with money laundering cases. As of September, the UIF had sent 6 suspected cases of

money laundering stemming from STRs to the Public Ministry for investigation in 2007. To date, there has not been a money laundering conviction in Peru.

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 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 Financial Investigative Office of DINANDRO has seized numerous properties over the last several years, but few were turned over to the police to support counternarcotics efforts. While Peruvian law does provide for asset forfeiture in money laundering cases, and these funds can be used in part to finance the UIF, no clear mechanism exists to distribute seized assets among government agencies. The Garcia Administration included an asset forfeiture law in a package of organized crime legislation presented to the Peruvian Congress in July 2007. The law went into force in November 2007.

Legislative Decree No. 992, published on July 22, 2007, established the procedure for loss of dominion, which refers to the extinction of the rights and/or titles of assets derived from illicit sources, in favor of the GOP, without any compensation of any nature. Likewise, through Legislative Decree No, 635, the penal code was modified to provide more comprehensively for seizure of assets, money, earnings, or other products or proceeds of crime.

Terrorism is considered a particular and long-standing 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 known actions to thwart the misuse of charitable or nonprofit entities that can be used as conduits for the financing of terrorism. Nongovernmental organizations are obliged to report the origins of their funds, according to UIF regulations.

Peru is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the Inter-American Convention against 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 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 a member of the Financial Action Task Force for South America (GAFISUD) and is scheduled to undergo its third GAFISUD mutual evaluation in April 2008. The UIF is a member of 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 and counter-terrorist financing regime in recent years. However, some progress is still required to better comply

with international standards. Although there is an Executive Order criminalizing terrorist financing, Peru should pass legislation that criminalizes terrorist financing. The GOP should also enact legislation that allows for administrative as well as judicial blocking of terrorist assets. There are still a number of weaknesses in Peru's anti-money laundering system: bank secrecy must be lifted to allow the UIF 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. 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 and the GOP should ensure their expedient passage. Anti-corruption efforts in Peru should be a priority. The GOP should address these issues to strengthen its ability to combat money laundering and terrorist financing.

Philippines

Although the Philippines is not a regional financial center, the illegal drug trade in the Philippines 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. Insurgency groups operating in the Philippines partially fund their activities through local crime, the trafficking of narcotics and arms, and engage in money laundering through ties to organized crime. The proceeds of corrupt activities by government officials are also a source of laundered funds. Smuggling continues to be a major problem. The Federation of Philippine Industries estimates that lost government revenue from uncollected taxes on smuggled items could be over U.S. $2 billion annually, including substantial losses from illegal imported fuel and automobiles. Remittances and bulk cash smuggling are also channels of money laundering. The Philippines has a large expatriate community.

The Government of the Republic of the Philippines (GOP) initially established its AML/CTF regime by passing the Anti-Money Laundering Act (AMLA) of 2001. The GOP enacted Implementing Rules and Regulations 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 U.S. $70,000) but no more than twice the value of proceeds 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, as well as insurance companies, securities dealers, foreign exchange dealers, money remitters, and dealers in valuable objects or cash substitutes regulated by the Securities and Exchange Commission (SEC). The GOP amended the AMLA in 2003 to correct certain inadequacies identified by the Financial Action Task Force. The amendments included lowering the threshold amount for covered transactions (cash or other equivalent monetary instrument) from 4,000,000 pesos to 500,000 pesos (approximately U.S. $100,000 to $12,000) 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 financial institution in the course of a periodic or special examination (in accordance with the rules of examination of the Central Bank); 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 original 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 "covered transaction reports" (CTRs) filed by regulated institutions. By the end of 2007, the AMLC had received more than 10,469 suspicious transaction reports (STRs) involving 18,269 suspicious transactions, and 103,714,619 CTRs. The AMLC has begun the second phase of its information technology upgrades by installing 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.

On February 28, 2007, the AMLC entered into a Memorandum of Understanding with the Central Bank setting forth the procedures for improved information exchange, compliance and enforcement policies. AMLC's role goes beyond traditional FIU responsibilities and includes the investigation and prosecution of money laundering cases. AMLC has the ability to seize assets involved in money laundering on behalf of the GOP after a money laundering offense has been proven beyond a reasonable doubt. 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 AMCL 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 AMLC has frozen funds at the request of the UN Security Council, the United States, and other foreign governments. Through the end of 2007, the AMLC had frozen funds in excess of 1.4 billion Philippine pesos (approximately U.S. $32 million) and had received 67 official requests for anti-terrorism action, many concerning groups on the UNSCR 1267 Sanction Committee's consolidated list.

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 be forfeited after conviction, even if the assets constitute a legitimate business. In December 2005, the Supreme Court issued a 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, eliminating confusion arising from the amendment to the AMLA in 2003. As of December 2007, there have been 107 money laundering, civil forfeiture, and related cases in Philippines court system that involved AMLC investigations or prosecutions, including 37 for money laundering, 20 for civil forfeiture, and the rest pertaining to freeze orders and bank inquiries. 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 and the Central Bank jointly and closely monitor compliance by banks and other financial institutions with AMLA provisions. Both have full mechanisms in place to ensure that the financial community is adhering to reporting and other AMLA requirements. Commercial banks, whose assets account for 88 percent of the Philippine banking industry, adopted on October 15, 2007 an electronic money laundering transaction monitoring system which generates transaction reports and suspicious transactions reports in compliance with Central Bank rules. During regular bank examinations, Central

Bank examiners test the capabilities of the banks' electronic money laundering transaction monitoring system. The remaining 12 percent of the banking industry (without electronic monitoring systems) are still required to establish a system for flagging and monitoring suspicious transactions, regardless of the amount.

The AMLC continues to work to bring the numerous foreign exchange offices in the country under its purview. The Monetary Board issued a circular on January 24, 2005 to bring the registration and operations of foreign exchange dealers and remittance agents under the AMLA. To obtain a license, dealers must attend an AML/CTF training course conducted by the AMLC. To date, only about 5,000 of the estimated 15,000 exchange dealers/remittance agents have registered. There are still several sectors operating outside of AMLC control. Although the revised AMLA specifically covers exchange houses, insurance companies, and securities brokers, it does not cover accountants. The AMLC requires car dealers and vendors of construction equipment, which are emerging as money laundering methodologies, to report suspicious transactions to the AMLC. On March 15, 2007 the Central Bank issued Circular 564 establishing guidelines governing the acceptance of valid identification cards including the AMLA's "two-ID requirement" for conducting financial transactions with banks and nonbank financial institutions.

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. All nonstock and nonprofit organizations registered with the Securities and Exchange Commission (SEC) are required to annually submit General Information Sheets and Audited Financial Statements. 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 with the SEC to bring charitable and not-for-profit entities under regulations for covered institutions. To promote transparency, SEC Circular 8 issued in June 2006 revised regulations on the registration, operations, and audit of foundations which are nonstock, nonprofit corporations.

There are seven offshore banking units (OBUs) established since 1976. OBUs account for less than two percent of total banking system assets in the country. The Central Bank regulates onshore banking and exercises regulatory supervision over OBUs, and requires OBUs 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 Central Bank 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 Philippine 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 U.S. $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 18 percent during the first ten months of 2007, and should exceed $14 billion for the year, equal to 11 percent of GDP. The Central Bank 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 Philippines 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. OFWs also use underground remittance systems such as hawala.

The Philippines is a founding member of the Asia/Pacific Group on Money Laundering (APG). The AMLC became the 101st member of the Egmont Group of FIUs in July 2005. The GOP 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 GOP is a party to the UN Convention against Corruption. The Philippines is listed 131 out of 180 countries surveyed by Transparency International's 2007 International Corruption Perception Index.

On June 20, 2007 the ALMC filed 165 counts of money laundering against a retired Philippine Army Major General and family members charging them with amassing more than U.S. $6.5 million in ill-gotten wealth.

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. In 2007, the GOP enacted an anti-terrorism law that defines and criminalizes terrorism and terrorist financing. The Human Security Act which went into effect in July 15, 2007 criminalizes terrorism and conspiracy to commit terrorism; penalizes an offender on the basis of his participation; empowers Philippine law enforcement to use special investigative techniques, inquire into bank accounts, and freeze and forfeit terrorist related funds and assets; creates an Anti-Terrorism Council comprised of cabinet members and support agencies.

The Financial Action Task Force removed the Government of the Republic of the Philippines from its list of Non-Cooperative Countries and Territories in 2005 due to the progress the GOP had made in remedying the deficiencies that resulted in its being placed on the list in 2001.The GOP has continued to make progress enhancing and implementing its amended anti-money laundering regime, including the enactment in 2007 of new legislation that criminalizes terrorism and terrorist financing. The Central Bank should be empowered to levy administrative penalties against covered entities in the financial community that do not comply with reporting requirements. Accountants should be required to report CTRs and STRs. Casinos should be fully regulated and supervised for AML/CTF procedures and required to file STRs. The Philippines 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 GOP should also consider establishing a civil forfeiture regime. 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 lies directly along one of the main routes between the former Soviet Union republics and Western Europe that narcotics traffickers and organized crime groups use. 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 U.S. $3 to $5 billion each year. According to the Government of Poland (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. With regard to economic offenses, the largest illegal income is connected with lost customs duties and taxes. Money laundering through trade in scrap metal and recyclable material is a fast developing trend. It is also believed that some money laundering in Poland originates in Russia or other countries of the former Soviet Union. The GOP estimates that the unregistered or gray economy, used primarily for tax evasion, may be as high as 13 percent of Poland's U.S. $460 billion gross domestic product (GDP). The GOP believes the black economy comprises only one percent of GDP.

Reportedly, some of Poland's banks serve as transit points for the transfer of criminal proceeds. As of June 2007, 51 commercial banks and 584 "cooperative banks" primarily serving the rural and agricultural community had licenses to operate. The GOP considers the nation's banks, insurance companies, brokerage houses, and casinos to be important venues of money laundering. The Finance Ministry maintains that the effectiveness of actions against money laundering involving transfer of money to so-called tax havens is limited. 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 anti-money laundering (AML) regime began in November 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 1997 Banking Act and 1998 Resolution of the Banking Supervisory Commission, add customer identification requirements and institute a threshold reporting requirement.

The November 2000 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, further improves Poland's ability to combat money laundering. This law, which the GOP has updated to conform to EU standards and to improve its operational effectiveness, increased penalties for money laundering and contains safe harbor provisions that exempt financial institution employees from normal restrictions on the disclosure of confidential banking information. Parliament has further amended the law to broaden the definition of money laundering to include assets originating from illegal or undisclosed sources. Poland's initial money laundering regime neglected to address many nonbank financial institutions that had traditionally been used for money laundering. To remedy this deficiency, 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. Entities subject to the reporting requirements include 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, notaries public, 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. Lawyers strongly opposed the amendments, claiming that the law violates attorney-client confidentiality privileges. The Polish Bar 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.

The law also requires casinos to report the purchase of chips worth 1,000 euros (approximately U.S. $1,400) or more. In addition to requiring that obliged entities notify the financial intelligence unit (FIU) of all financial deals exceeding 15,000 euros (approximately U.S. $21,000), covered institutions must also file reports of suspicious transactions, regardless of the size of the transaction. Polish law also requires financial institutions to put internal AML procedures into effect, a process that is overseen by the FIU.

The Criminal Code criminalizes money laundering for all serious crimes. Article 299 of the Criminal Code addresses self-laundering and criminalizes tipping off. The Polish Code of Criminal Procedure, Article 237, allows for certain Special Investigative Measures (SIM). Although money laundering investigations are not specifically discussed in relation to SIM, the organized crime provisions might apply in some cases. Poland's National Security Strategy rates the AML effort as a top priority.

The "Act on Counteracting Money Laundering and Terrorism Financing" is undergoing revisions. The revised legislation will implement the EU's Third Money Laundering Directive (Directive 2005/60/EC of the European Parliament and of the Council, on preventing usage of the financial system for money laundering and terrorist financing). The Directive was to be transposed into Polish legislation by 15 December 2007, but October 2007 parliamentary elections and the recent change of government delayed the implementation process.

As of June 15, 2007, travelers entering Poland from a nonEU country or traveling to a nonEU country with 10,000 euros (approximately $14,500) or more in cash must declare their cash or monetary instruments in writing. To comply with EU standards, Poland's customs law requires travelers to complete and present a customs and currency declaration if they are transporting more than 10,000 euros (approximately U.S. $14,700) in currency or financial instruments upon entry. In December 2007 the new Schengen countries, including Poland, were enveloped within EU borders. Land border controls between EU member states disappeared on December 20, 2007.

The 2000 AML law provides for the creation of a financial intelligence unit (FIU), the General Inspectorate of Financial Information (GIIF) within the Ministry of Finance, to collect and analyze large cash and suspicious transactions. The vast majority of required notifications to the GIIF come through the electronic reporting system. Only some small institutions lacking the equipment to use the electronic system submit notifications on paper. Although the new system is an important tool for Poland's AML regime, the efficient processing and analyzing of the large number of reports that are sent to the GIIF is 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 continues 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.

In 2006, the GIIF received over 26 million reports from obliged institutions, including 26.7 million cash transaction reports and 48,229 suspicious transaction reports (STRs), the majority of which were cash transaction reports and 90 percent of which came from the banking community. Of these, 47,817 related to money laundering and 412 related to terrorist financing. However, upon completion of preliminary analysis, it was determined that 68 percent of these STRs were erroneous due to a technical error by the filing institution or incomplete information provided on the STR. As a result, only 15,061 of the STRs were accurate and subject to further analysis by the GIIF. The FIU's analysis resulted in the production of 1,139 analytical reports. As a result of these 1,139 reports, GIIF sent 198 notifications to the Prosecutor's Office. At a minimum, all reports submitted by the GIIF to the Prosecutor's Office result in initial investigative proceedings. From 198 notifications sent to the prosecutor's office by the GIIF in 2006, two cases reached the court. As of September 2007, the courts are still investigating 175 notifications. In the past, many of the GIIF-instigated investigations have resulted in convictions for other nonfinancial offenses. The GIIF receives approximately 2.3 million reports per month on transactions exceeding the threshold level.

In addition to the Prosecutor's Office, the GIIF also cooperates with several domestic law enforcement agencies, including the General Investigative Bureau (a police unit), the Internal Security Agency (which investigates the most serious money laundering cases), and the Central Anti-Corruption Office. 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, has improved. The GIIF and the National Prosecutor's Office have signed a cooperation agreement that 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.

In 2006, GIIF conducted an assessment of the effectiveness of Poland's anti-money laundering reporting system. According to the GIIF's 2006 annual report, the analysis identified three main threats to efficiency of the system: disproportionate reporting among Poland's 16 provinces (three provinces had extremely high reporting rates); delays in prosecutorial handling of GIIF notifications; and inadequate use of the GIIF by domestic agencies in Poland (76 percent of all queries to the GIIF were from the Prosecutor's office).

The GIIF also conducts training for specified target groups as well as e-learning, which is available to all obligated institutions and cooperating entities. In 2006, the GIIF re-introduced the electronic learning course designed to familiarize obliged institutions with Poland's AML regulations. Over 1,800 individuals (mainly from obligated institutions) participated in the GIIF's electronic learning course.

The GIIF exchanges information with its foreign counterparts. The United States, along with the United Kingdom and Ukraine, is among its most active information-sharing partners. In 2006, GIIF sent official requests to foreign financial intelligence units on 158 cases concerning 287 national and foreign entities suspected of money laundering. Foreign FIUs sent 62 information requests concerning 154 national and foreign entities to the GIIF.

The GIIF has the authority 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. Article 45 of the criminal code reverses the burden of proof so that an alleged perpetrator must prove that his assets have a legal source; otherwise, the assets are presumed to be related to the crime and the government can seize them. Both the Ministry of Justice and the GIIF reportedly desire more aggressive asset forfeiture regulations. However, lingering political sensitivities reportedly hamper approval of stringent asset seizure laws. In the first half of 2007, funds totaling U.S. $46 million have been frozen and 39 notifications of possible crimes committed have been sent to the prosecutor's office, with the GIIF suspending one transaction worth U.S. $92,000 and blocking 59 accounts worth U.S. $5.1 million. In 2006, the GIIF suspended four transactions worth U.S. $2.6 million and blocked 92 accounts worth U.S. $16.6 million.

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 has prepared a draft of amendments to the criminal code that would criminalize terrorist financing as well as elements of all terrorism-related activity, but withdrew the draft in 2007 before it had been approved by the Council of Ministers.

The GOP has created an office of counter-terrorist operations within the National Police, which coordinates and supervises regional counter-terrorism units and trains local police in counter-terrorism measures. In December 2006, the GOP established the Intra-ministerial Unit for Terrorist Threats. Poland has also created its own 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 obliged institutions must 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. In 2006, the GIIF worked on eight terrorist financing cases involving 89 subjects. Upon completion of its analysis, the GIIF forwarded three reports to the Internal Security Agency (ABW) for further analysis. The cases involved transactions related to large amounts of cash being sent to Poland as well as numerous noncash transfers involving terrorist groups or transactors from a country supporting terrorism.

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 36 MOUs. 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 six additional FIUs.

Poland is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), which in 2006 conducted its third round mutual evaluation of Poland. The report is not yet available. The GIIF is a member of the Egmont Group and is enrolled 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.

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

Over the past several years, the Government of Poland has worked to implement a comprehensive AML regime that meets international standards. However, work remains, as Poland's AML regime remains noncompliant with various Financial Action Task Force (FATF) standards. Most significantly, Poland must criminalize terrorist financing. No terrorist financing prosecutions have yet been undertaken or cases brought before the court. Under current provisions, it is unclear how Poland could prosecute the funding of a terrorist or terrorist organization. Poland must also strengthen AML regulations pertaining to customer due diligence obligations, DNFBPs, nonprofit organizations, politically exposed persons, cross-border correspondent banking, and suspicious transaction reporting as it pertains to terrorist financing. The GOP should promote additional training at the private sector level and 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 specifically allow the use of Special Investigative Measures in money laundering investigations, which would assist law enforcement attain a better record of prosecutions and convictions.

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 criminals use currency exchanges, wire transfers, and real estate purchases to launder their proceeds.

The Portuguese Madeira Islands International Business Center (MIBC) has a free trade zone, an international shipping register, offshore banking, trusts, holding companies, stock corporations, and private limited companies. The latter two business groups, of which there are approximately 6,500 companies registered in Madeira, are similar to international business corporations. All entities established in the MIBC will remain tax exempt until 2011. Twenty-seven offshore banks have licenses to operate within the MIBC. Decree-Law 10/94 permits existing banks and insurance companies to establish offshore branches. Institutions submit applications to the Central Bank of Portugal. Institutions already in the European Union have a notification process, while nonEU or new entities receive authorization. The law allows establishment of "external branches" that conduct operations exclusively with nonresidents or other Madeira 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. The Madeira Development Company supervises offshore banks. 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.

Accessing Internet gambling sites is illegal in Portugal. There are no known cases of casinos or Internet gaming sites whose Internet service provider (ISP) is headquartered in Portugal. However, Internet gaming is still widely available.

Portugal has a comprehensive anti-money laundering and counter-terrorist financing (AML/CTF) regime that criminalizes the laundering of proceeds of serious offenses, including terrorism, arms trafficking, kidnapping, and corruption. Article 11 of Law No. 59/2007, dated September 4, 2007, defines money laundering and expands the list of crimes related to money laundering, and makes legal entities criminally accountable.

Act 11/2004, which implements the European Union's (EU's) Second Money Laundering Directive, defines the legal framework for the prevention and suppression of money laundering. The law also mandates suspicious transaction reporting by financial and nonfinancial institutions, including credit institutions, investment companies, life insurance companies, traders in high-value goods (e.g., precious metals and stones, aircraft), regardless of transaction amount. Suspicious transaction reports (STRs) go to the Public Prosecutor's Office. If a regulated entity has knowledge of a transaction likely to be related to a money laundering offense, it must inform the Portuguese financial intelligence unit (FIU). The GOP may order the entity not to complete the transaction. If stopping the transaction is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, the government may also allow the entity to proceed with the transaction but require the entity to provide the authorities with complete details. "Tipping off" is prohibited and safe harbor provisions protect regulated entities making disclosures in good faith from liability.

All financial institutions, including insurance companies, must identify their customers, maintain records for a minimum of ten years, and demand written proof from customers regarding the origin and beneficiary of transactions that exceed 12,500 euros (approximately U.S. $18,250). 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. Beyond the requirements to report large transactions, foreign exchange bureaus are not subject to any special requirements to report suspicious transactions. Portuguese law gives the GOP the authority to investigate suspicious transactions without notifying the targets of the investigation.

In 2007, through Decree-Law No. 61/2007, Portugal implemented EU regulation EC 1889/2005, on cash entering or leaving the European Community. The law requires all individuals to declare currency valued at 10,000 euros (approximately U.S. $14,600) or greater when entering or exiting the European Community. The law also stipulates that authorities gather and exchange information at the national

and international levels. Portugal is in the process of transposing the EU's Third Money Laundering Directive (Directive 2005/60/EC) into Portuguese law.

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 and Food Safety Authority, the Economic Activities Inspectorate General, the Registries and Notaries General Directorate, the National Association for Certified Public Accountants and the Association for Assistant Accountants, the Bar Association, and the Chamber of Solicitors also monitor and enforce the reporting requirements of the obliged entities.

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

Portuguese Securities Market Commission Regulation 7/2005 requires financial intermediaries to submit detailed annual Control and Supervision Reports to the Commission every June. The regulation entered into force on January 1, 2006.

There is no single body that oversees charitable organizations or their possible terrorist finance-related activities. The Intelligence Security Service, the Judicial Police, and the Public Prosecutor's office share supervisory authority. International financial transactions that may involve terrorist financing require the same monitoring protocol as those involving possible money laundering.

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

In 2006, the UIF received 584 STRs. The FIU also received over 15,000 other reports, primarily from the General Inspectorate for Gaming. The UIF sent 272 cases for further investigation to the Judicial Police and other police departments. 2007 STR information is not yet available. Between January and September of 2007, the UIF seized or confiscated approximately 32.4 million euros (approximately U.S. $47.3 million).

Police may request files of individuals under investigation and, with a court order, can obtain and use audio and video recordings as evidence in court. 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). The Judicial Police can do this even if the predicate crime is committed outside of Portugal. Act 5/2002 defines criminal assets as those owned by an individual at the time of indictment and thereafter. Act 5/2002 also shifted the burden of proof in cases of criminal asset forfeiture from the government to the defendant; an individual must prove that his or her assets were not obtained as a result of his illegal activities. The law also presumes that assets transferred by an individual to a third party within the previous five years still belong to the individual in question, unless proven otherwise. GOP law enforcement agencies have seized a total of 20.7 million euros (approximately U.S. $30.2 million) in nonmonetary goods in association with drug and money laundering investigations. The law allows the Public Prosecutor to request that a lien be placed on the assets of individuals being prosecuted, to facilitate asset seizures related to narcotics and weapons trafficking, terrorism, and money laundering. Portugal

has comprehensive legal procedures that enable it to cooperate with foreign jurisdictions and share seized assets.

Act 52/2003 specifically defines terrorist acts and organizations and criminalizes the transfer of funds related to the commission of terrorist acts. Portugal has created a Terrorist Financing Task Force that includes the Ministries of Finance and Justice, the Judicial Police, the Security and Intelligence Service, the Bank of Portugal, and the Portuguese Insurance Institution. Names of individuals and entities included on the UN Security Council Resolution 1267 Committee's consolidated list or that the United States and EU have linked to terrorism are passed to private sector organizations. The Bank of Portugal, the Stock Exchange Commission, and the Portuguese Insurance Institution circulate the lists to the obliged entities. In practice, while the government has the authority to immediately freeze funds, an actual seizure of assets would only occur once the EU's clearinghouse process resulted in agreement to the EU-wide seizure of assets of terrorists and terrorist-linked groups. Portugal is actively cooperating in the search and identification of assets used for terrorist financing. To date, no significant assets have been identified or seized.

Portugal is a member of the Financial Action Task Force (FATF), and underwent a mutual evaluation by that body in 2006. Portugal's FIU is a member of the Egmont Group. Portugal is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the UN International Convention for the Suppression of the Financing of Terrorism. Portugal is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. The U.S. and Portugal signed a mutual legal assistance agreement (MLAT) and an extradition agreement in 2005, designed to complement and implement the U.S.-European Union Mutual Legal Assistance and Extradition Treaties of 2003. These agreements are pending U.S. ratification.

Portugal should collect and maintain more information and data regarding the number of money laundering and terrorist 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 terrorist 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 terrorist financing law covers financing to individuals. The FIU should be the competent authority to receive and analyze all STRs. Portugal should strengthen its legal requirements relating to politically exposed persons. The GOP should also improve its implementation of AML/CTF rules for obliged nonfinancial businesses and professions.

Qatar

Qatar has fewer than one million residents with a low rate of general and financial crime. Historically, Qatar has not been an important regional financial center, though with the country's remarkable energy-driven growth in recent years it aims to become an increasingly important banking and financial services center in the Gulf.

The Qatar Central Bank (QCB) exercises regulatory authority over the financial sector. There are 17 licensed banks, including three Islamic banks and a specialized bank, the Qatar Industrial Development Bank. There is a separate Qatar Financial Center (QFC) that allows major international financial institutions and corporations to set up offices with 100 percent foreign ownership, unlike most business sectors in Qatar. There are currently 18 banks, 6 investment banks, 5 asset management companies, and 7 insurance companies authorized to operate in the QFC. QFC firms are limited to providing services to wholesale clients, except for insurance companies who can provide services to both wholesale and retail clients. The QFC has a separate, independent regulatory authority, the QFC Regulatory Authority, with a regulatory regime based on international standards. There are plans underway to create a unified regulatory authority for the country within the next two years. Qatar has

20 exchange houses, three investment companies and two commercial finance companies. 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.

Qatar has a clear legal framework for financial crimes that is based on a 2002 law on money laundering and a 2004 law on terrorist financing. The judicial system has yet to be tested as there have been no arrests or prosecutions for money laundering or terrorist financing crimes since enactment of the laws.

On September 11, 2002, the Amir (Head of State) 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 to the Financial Information Unit 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 QFC law provides that Qatari criminal laws apply in the QFC, including those Qatari laws criminalizing money laundering and the financing of terrorism. In addition, the QFC has implemented its own anti-money laundering regulations and corresponding rules. The QFC Regulatory Authority is responsible for supervising QFC firms' compliance with QFC AML requirements.

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 Qatar Central Bank, FIU, Ministries of Interior, Labor and Social Affairs, 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 separate from the NAMLC to review the consolidated UN 1267 terrorist designation lists and to recommend any necessary actions against individuals or entities found in Qatar. The committee is chaired by the Minister of State for Interior Affairs and includes the FIU and various law enforcement representatives. The committee and the Central Bank circulate to financial institutions the individuals and entities included on the UN 1267 Sanctions Committee's consolidated list, but have thus far not identified or frozen any related assets.

The QCB updates regulations regarding money laundering and financing of terrorism on a regular basis, in accordance with international requirements. The QCB 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. Suspicious transaction reports (STRs) are now sent to the FIU by hardcopy or electronically, but the FIU is developing an all-electronic system with bank compliance offices that should speed the reporting process. 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 FIU also works closely with the QFC Regulatory Authority to ensure that QFC firms, and specifically their Money Laundering Reporting Officers, understand and implement appropriate AML and counter-terrorist finance policies and procedures. The Qatari FIU became a member of the Egmont Group in 2005.

In December 2004, the 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.

Law No. 13 from 2004 established The Qatar Authority for Charitable Works, which 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 reports to the Ministry of Labor and Social Affairs and 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. Article 13 of the law provides penalties of up to a year in prison, a fine of 50,000 Qatari riyals (approximately U.S. $13,750), and confiscation of the money involved for "anyone who collects donations, or transfers money outside the country, bestows or accepts loans or grants or donations or bequests or endowments" outside of The Authority's purview.

Qatar does not have mandatory cross-border currency reporting requirements. Customs officials are given authority under the law to, in suspicious cases, require travelers to fill out forms declaring cash currency or other negotiable financial instruments in their possession. Officials then forward the traveler's information to the FIU for evaluation. The FIU has received about 60 reports from Customs for evaluation. Immigration and customs authorities are reviewing their policies to expand their ability to enforce money declarations and detect trade-based money laundering.

The Government of Qatar is a party to the 1988 UN Drug Convention. Qatar has not signed the UN Convention for the Suppression of the Financing of Terrorism or the UN Convention against Corruption. The Ministerial Council approved Qatar's accession to the UN Convention against Transnational Organized Crime in fall 2007, but final approval is still pending. Qatar is ranked 32 out of 179 countries surveyed in Transparency International's 2007 Corruption Perception Index. Qatar is one of the original signatories of the 2004 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 should continue to implement AML/CTF policies and procedures that adhere to world standards. 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 become a party to the UN International Convention for the Suppression of the Financing of Terrorism, and complete its accession to the UN Convention against Transnational Organized Crime.

Romania

Romania's geographical 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. According to law enforcement entities, estimates of crimes involving money laundering amount to approximately $15 million per year. Trans-border smuggling of counterfeit goods, 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 cybercrime and online credit card fraud in the world, with the vast majority of victims residing in the United States.

Laundered money comes primarily from international crime syndicates who conduct their criminal activity in Romania and subsequently launder their illicit proceeds through illegitimate front companies. Another source of laundered money is the proceeds of illegally smuggled goods such as cigarettes, alcohol, gasoline, and other dutiable commodities. Corruption in Romania's customs and border control and as well in several neighboring Eastern European countries also facilitates money laundering. In 2003, Romania instituted an anti-corruption plan and passed a law criminalizing organized crime.

Romania's Law No. 21/99, On the Prevention and Punishment of Money Laundering, criminalizes money laundering and requires customer identification, record keeping, suspicious transaction reporting, and currency transaction reporting for transactions (including wire transfers) over 10,000 euros (approximately U.S. $14,700). The list of entities covered by Law No. 21/99 includes banks, nonbank financial institutions, attorneys, accountants, and notaries. Romania has also criminalized tipping off suspected money launderers. Romanian law permits the disclosure of client and ownership information to bank supervisors and law enforcement authorities, and safe harbor provisions protect banking officials when they cooperate with law enforcement.

The Law on the Prevention and Sanctioning of Money Laundering (Law 656/2002) expands the list of predicate offenses to include all crimes and expands the number and types of entities subject to anti-money laundering (AML) regulations. The additional entities include art dealers, travel agents, privatization agents, postal officials, money service businesses, and real estate agents. Although nonbank financial institutions are covered under Romania's AML law, regulatory supervision of this sector is weak and not as rigorous as that imposed on banks.

In keeping with international standards, Romania has taken steps to strengthen its know-your-customer (KYC) identification requirements. The National Bank of Romania's (BNR) 2003 Norm No. 3, "Know Your Customer," strengthens information disclosure requirements 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 measures 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. The Insurance Supervision Commission has instituted similar regulations for the insurance industry.

Law 230/2005 provides for a uniform approach to combating and preventing money laundering and terrorist financing. With this law, Romania meets the requirements of two European Union (EU) Money Laundering Directives, 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 a suspicious transactions reporting requirement for transactions linked to terrorist financing.

In 2006, Romania made further changes to its laws to bring the country into harmony with FATF recommendations and EU Directives. Romania amended its laws to increase the amount of fines corresponding to the inflation rate; to allow the use of undercover investigators; and to send reports from the financial intelligence unit (FIU) to the General Prosecutor's Office in an unclassified manner for use in operational investigations. The law also provides for confiscation of goods used in or resulting from money laundering activities; and an increase in the length of time that bank accounts may be frozen from ten days up to one month.

The FIU Board has 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. As a member of the EU, Romania was required to fully adopt the EU's Third Money Laundering Directive, known as European Commission Directive 2005/60/EC, on preventing the use of the financial system for the purpose of money laundering and terrorist financing by December 15, 2007.

Romania's FIU, the National Office for the Prevention and Control of Money Laundering (NOPCML), was established in 1999. All obliged entities must submit their currency transaction reports and suspicious transaction reports (STRs) to the FIU. The FIU oversees the implementation of AML guidelines for the financial sector and works to ensure that all domestic financial institutions covered by the law receive adequate training. The FIU is also authorized to participate in inspections and controls in conjunction with supervisory authorities. In the first ten months of 2007, the FIU carried out 189 on-site inspections in cooperation with the Financial Guard or other supervision authorities—an increase from the 109 inspections for the same period in 2006.

Since its establishment, the FIU has faced numerous challenges, including charges against a former director for the destruction of public records and corruption. Under its current President, the FIU has worked to improve the quality of cases forwarded to prosecutors for judicial action. The FIU believes that the number of indictments, and eventual convictions, will increase over time as the FIU places greater emphasis on the quality of reports produced as opposed to the quantity of reports forwarded to the Prosecutor's Office.

During the first ten months of 2007, the FIU received 10,747 currency transaction reports for transactions exceeding the 10,000 euros (approximately U.S. $14,700) threshold, an increase from 9,110 in the same period in 2006. During the first nine months of 2007, the FIU received 6,511 reports of cross-border transfers, compared with 6,735 reports in 2006. During the same period, the total number of STRs received was 1,542, down from 2,218 reports in 2006. Of this figure, banks submitted 1,435 reports and individuals submitted 25 reports. Money transfer agents substantially increased their submissions, sending 18 reports compared with 10 reports last year; as did independent legal professionals, who submitted seven reports, up from three reports in 2006. The remainder came from various other entities, including: financial investment services; insurance/re-insurance firms; real

estate brokers; leasing companies; foreign exchange houses; consulting; and fiscal/accounting service providers.

During the first ten months of 2007, the FIU suspended one suspicious transaction (down from three suspensions in 2006). The total amount of fines levied by the FIU in the first ten months of 2007 amounted to U.S. $129,098 (up from $98,940).

Upon completion of its analysis, the FIU forwards its findings to the appropriate government agency for follow-up investigation. During the first nine months of 2007, the FIU sent 256 files on suspicion of money laundering to the General Prosecutor's Office; the Police General Inspectorate; the National Agency for Fiscal Administration; the Financial Guard; the National Anti-Corruption Department; and the Romanian Intelligence Service. In the same interval in 2006, the FIU forwarded 127 cases onward.

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. In the first half of 2007, the Directorate for the Investigation of Organized Crime and Terrorism Offenses (DIICOT), the agency primarily responsible for the prosecution of money laundering cases, indicted 70 defendants in 27 cases involving money laundering totaling approximately U.S. $7 million. Of the 70 indicted, 15 defendants have been placed under preventive arrest. During this same period, DIICOT opened criminal investigations on 236 cases involving suspicion of money laundering.

In response to the events of September 11, 2001, Romania passed a number of legislative measures designed to criminalize 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. The Supreme Defense Council of the Country (CSAT) has adopted a National Security Strategy, which includes the 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 Government of Romania (GOR) has also set up an inter-ministerial committee to investigate the potential use of the Romanian financial system by terrorist organizations. A revised Criminal Procedure Code entered into force in July 2003, containing 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 strengthens 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 authorized 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 working days.

Law 535/2004 on preventing and combating terrorism 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 reported

The FIU is aware of the potential misuse of charitable or nonprofit entities as conduits for terrorist financing. In 2007, the FIU conducted two training events with charitable foundations and associations on preventing and combating money laundering and terrorist financing. The FIU has drafted guidelines concerning reporting entities' obligations in this respect, and has published them on its website.

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 the South East Europe Security Cooperation Steering Group (SEEGROUP) a working body of the NATO initiative for southeast Europe to coordinate counter-terrorist measures undertaken by the states of southeastern Europe. The Romanian and Bulgarian Interior Ministers have signed an inter-governmental agreement 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). The most recent mutual evaluation of Romania was conducted in May 2007 by MONEYVAL and is scheduled to be discussed and adopted by that body in 2008.

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 anti-crime initiatives by participating in regional and global anti-crime efforts. Romania is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. Romania also is a party to the UN International Convention for the Suppression of the Financing of Terrorism. The FIU has signed bilateral memoranda with fifteen countries and in 2007, concluded bilateral memoranda of understanding with FIUs from the United States, United Kingdom, Hungary, Israel, and Russia.

While Romania's AML legislation and regulations will soon be compliant with many FATF and EU standards, implementation has moved at a slower pace. The FIU has improved the timeliness and quality of its analysis and case 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 nonbank entities has been on the rise. 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 communication between reporting and monitoring entities, as well as between prosecutors and the FIU. The General Prosecutor's Office should continue to place a high priority on money laundering cases. Romania should improve implementation of existing procedures for the timely freezing, seizure, and forfeiture of criminal or terrorist-related assets. Romania should continue to make progress in combating corruption in commerce and government. Romania should enact and implement legislation to subject nongovernmental organizations (NGOs) and charitable organizations to reporting requirements.

Russia

Russia is a regional center. Its financial system does not attract a significant number of depositors, although due to rapid economic growth in various sectors, the number of depositors has steadily been increasing. 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 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, reportedly, a high level of corruption. Other vulnerabilities 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. Russia's financial intelligence unit (FIU) estimates that Russian citizens may have laundered as much as U.S. $11 billion in 2007.

Russia has recently changed its laws to allow direct foreign ownership and investment in Russian financial institutions. Net private capital inflows for 2007 reached U.S. $82.3 billion according to the Russian Central Bank, an increase from U.S. $41.6 billion in 2006.

The Russian Federation has a legislative and regulatory framework in place to pursue and prosecute financial crimes, including money laundering and terrorism finance. Federal Law No. 115-FZ "On Combating Legalization (Laundering) of Criminally Gained Income and Financing of Terrorism," introduced in 2001, obliges banking and nonbanking financial institutions to monitor and report certain types of transactions, maintain records, and identify their customers. According to 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. Other obliged entities include real estate agents, lawyers and notaries, and to persons rendering legal or accounting services that involve certain transactions.

Various regulatory bodies ensure compliance with Russia's anti-money laundering and counterterrorism finance (AML/CTF) 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; the Federal Service for Financial Monitoring (FSFM) regulates real estate and leasing companies, pawnshops, and participants in the gaming industry; and the Assay Chamber (under the Ministry of Finance) supervises entities buying and selling precious metals or stones.

The CBR has issued guidelines regarding AML practices within credit institutions, including "know your customer" (KYC) and bank due diligence programs. Banks must obtain, and retain for a minimum of five years from the date of the termination of the business relationship, information regarding individuals, legal entities and the beneficial owners of corporate entities. Banks must also adopt internal compliance rules and procedures and appoint compliance officers. The AML Law (Law 115-FZ) requires banks to identify their customers before providing natural or legal persons with financial services. Banks are required to report all transactions subject to mandatory or suspicious transaction requirement to the to the financial intelligence unit (FIU). Credit institutions that fail to meet mandatory or suspicious reporting requirements face revocation of their licenses, limits on certain banking operations, and possible criminal or administrative penalties. The CBR can levy administrative fines on credit institutions and officials of credit institutions for violations of Russia's AML/CTF law. Criminal liability does not apply to legal persons under Russian law. The maximum

criminal penalty for natural persons convicted of money laundering or financing terrorism is 10 years in prison in addition to applicable fines.

All obligated financial institutions must monitor and report to the government any transaction that equals or exceeds 600,000 rubles (approximately U.S. $22,700) and involves or relates to cash payments, remittances, bank deposits, gaming, pawn shop operations, precious stones and metals transactions, payments under life insurance policies, or persons domiciled in countries determined by the Russian Government to be deficient in AML/CTF. Obligated institutions must also report real estate transactions valued at 3,000,000 rubles (approximately U.S. $115,400) or more. Financial institutions must develop criteria for determining suspicious transactions and report such transactions to the FIU in a timely fashion. All transactions involving an entity or person included on the Russian government's list of those involved in extremist activities or terrorism must be reported to the FIU an

Under Order 1317-U, Russian financial institutions must inform the CBR when it establishes correspondent relationships with nonresident banks in operating in offshore zones (as defined by the Russian Federation in Annex 1 of this Order). The CBR recommends that financial institutions apply enhanced due diligence to transactions with nonresident institutions. Foreign banks may only open subsidiary operations on the territory of Russia. The CBR must authorize the establishment of a subsidiary operation, and these subsidiaries must be subject to domestic Russian supervisory authorities. Foreign banks are not permitted to open branches in Russia. Russian banks must also obtain CBR approval to open operations abroad.

According to the Law No. 395-I "On Banks and Banking Activities," credit institutions must identify and inform the CBR of all appointments of individuals to senior management positions and to the managing and supervisory boards. Russian law prohibits the appointment of anonymous parties or proxy individuals to a credit institution's managing or supervisory board. The CBR has the authority to deny the appointment of a senior official if the official does not meet "fit and proper" requirements established by the CBR.

Russia has established a Deposit Insurance System (DIS) for banks. To gain admission to the DIS, a bank must verifiably demonstrate to the CBR that it complies with applicable banking and AML/CTF laws. Currently, 911 of Russia's 1,145 banks participate in the DIS.

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 that was administratively subordinated to the Ministry of Finance until September 2007, but which is now subordinated to the Prime Minister. The FSFM is responsible for receiving, analyzing, and disseminating reports from those entities obligated to file mandatory and suspicious reports. Nearly all financial institutions submit reports to the FSFM via encrypted software provided by the FSFM. According to the FSFM's annual report for 2006, Russia's national database contains 6.3 million reports on operations with monetary funds or other assets, with a total value of approximately $900 billion. The FSFM receives approximately 30,000 transaction reports daily. The FSFM is also the regulator for real estate and leasing companies, pawnshops, and gaming outlets. The FSFM is authorized to provide information to relevant 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. As an administrative unit, it has no law enforcement or investigative powers.

The head of the FSFM chairs an Interagency Commission on Money Laundering, which is responsible for monitoring and coordinating the government's activity on money laundering and terrorist financing. Twelve ministries and government departments sit on the Commission.

Each of the seven federal districts comprising the Russian Federation contains an FSFM territorial office. 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 counter-terrorist financing (AML/CTF) legislation by the institutions that the FSFM supervises. Additionally, the territorial offices must identify and register at the regional level all pawnshops, leasing companies, real estate firms, and gaming entities under their jurisdiction. The regional offices also coordinate the efforts of the CBR and other supervisory agencies to implement AML/CTF regulations. Russia's AML legislation 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 or accounting services, and sellers of precious metals and stones.

During the first half of 2007, the FSFM registered 5,603 crimes involving money laundering, compared to 7,957 reports for all of 2006. Interior Ministry officials reported that 4,535 of the 2007 cases went to trial. Both the FSFM and MVD report that the number of suspicious transaction reports (STRs) for the year roughly equaled those of 2006 and credit increased cooperation among law enforcement agencies for the number of cases brought to trial.

With its legislative and enforcement mechanisms in place, Russia has begun to prosecute high-level money laundering cases. During 2007, the CBR revoked the licenses of 44 banks for failing to observe banking regulations. Of these, 30 banks lost their licenses for violating Russia's AML laws. The CBR's initiative to prohibit individuals convicted of money laundering from serving in leadership positions in the banking community—a cause championed by Andrey Kozlov, the First Deputy Chairman of the CBR who was assassinated in 2006—remains pending.

Russian legislation provides for the tracking, seizure and forfeiture of all criminal proceeds, not just those linked to narcotics trafficking. Russian law also provides law enforcement bodies the authority to use investigative techniques such as search, seizure, and the identification, freezing, seizing, and confiscation of funds or other assets. Authorities can compel individuals to produce documents related to criminal activity, including money laundering. Investigators and prosecutors can apply to the court to freeze or seize property obtained as the result of crime, although there are some exceptions in the law restricting seizure of property identified as a primary residence. 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. According to the AML/CTF law, financial institutions must freeze transactions suspected of involvement in terrorism finance for up to two days and report the transaction to the FIU. The FSFM may extend the freeze by an additional five days. A court order is required to extend the freeze beyond seven 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. Authorities can seize businesses only if they can demonstrate that the businesses 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.

Russia's Presidential Administration as well as law enforcement agencies have, however, expressed concern about ineffective implementation of Russia's confiscation laws. The government has proposed amendments that are currently under review by the Duma These amendments would facilitate the identification and seizure of criminal instrumentalities and proceeds. Russian law enforcement has adequate police powers to trace assets, and the law permits confiscation of assets. However, most Russian law enforcement personnel reportedly 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. The decree entitled "On Measures to Implement the UN

Security Council Resolution (UNSCR) No. 1373 of September 28, 2001" introduces criminal liability for intentionally providing or collecting assets for terrorist use and instructs relevant agencies to seize assets of terrorist groups. Article 205.1 of the criminal code, enacted in October 2002, criminalizes terrorist financing. Banks can freeze assets suspected of involvement in terrorism finance immediately pursuant to UNSCR 1373.

The FSFM reports that it is monitoring 1,300 entities suspected of financing terrorism, including over 900 Russian citizens, 170 Russian organizations, and over 200 foreign entities. The Russian Government maintains a list of domestic and international organizations and individuals involved in extremist activities or terrorism. This list is distributed to all institutions subject to the AML/CTF law and is used by law enforcement agencies to target and seize assets. Russian authorities rely on five sources of information to compile the designated entities list: a) international organizations, such as the UN 1267 Sanctions Committee lists; b) Russian court decisions; c) designations made by the Prosecutor General; d) Ministry of Interior investigations (provided that subsequent court decisions do not reverse or dismiss the investigation's findings); and e) bilateral agreements to designate entities mutually determined to be involved in extremist or terrorist activity. At the request of the General Procuracy, the Russian Supreme Court has, to date, authorized an official list of 17 terrorist organizations.

The United States and Russia signed a Mutual Legal Assistance Treaty in 1999, which entered into force on January 31, 2002. Although Russia has assisted the U.S. in investigating cases involving terrorist financing, Russia and the U.S. continue to differ about the purpose of the UN 1267 Sanctions Committee's designation process. These political differences have hampered bilateral cooperation in this forum. U.S. law enforcement agencies exchange operational information with their Russian counterparts on a regular basis. The close cooperation between Russian and U.S. agencies has continued and strengthened in 2007.

Russia is a member of the Financial Action Task Force (FATF) and underwent its third mutual evaluation during the fourth quarter of 2007. The FATF's mutual evaluation report (MER) is expected to be released in June 2008. Russia is also a member of two FATF-style regional bodies (FSRBs). It is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and the Eurasian Group on Combating Legalization of Proceeds from Crime and Terrorist Financing (EAG), of which it was a co-founder. The EAG Secretariat is located in Moscow. The FSFM has established the International Training and Methodological Center of Financial Monitoring (ITMCFM) that exists to provide technical assistance, primarily in the form of staff training for FIUs and other interested ministries and agencies involved in AML/CTF efforts. The ITMCFM also conducts research on AML/CTF issues. As Chair of the EAG, Russia's FIU continues to play a strong leadership role in the region. The FSFM is a member of the Egmont Group The FSFM has signed cooperation agreements with the Financial Intelligence Units (FIUs) of 24 countries, including the United States.

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, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption.

Through aggressive enactment and implementation of comprehensive AML/CTF legislation, Russia has established legal and enforcement frameworks to deal with money laundering and terrorist financing. Russia has also contributed to improving the region's capacity for countering money laundering and terrorist financing. Nevertheless, serious vulnerabilities remain. Russia is home to some of the world's most sophisticated perpetrators of fraud and money laundering, who rely heavily on electronic and Internet-related means. Russia should improve federal oversight of shell companies and scrutinize more closely those banks that do not carry out traditional banking activities. To prevent

endemic corruption and deficiencies in the business environment from undermining Russia's efforts to establish a well-functioning anti-money laundering and counter-terrorism finance regime, Russia should strive to stamp out official corruption, 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 to enable them to fulfill their responsibilities. Russia should work to increase the effectiveness of its asset forfeiture 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 through sustained involvement in the regional and international bodies focusing on AML/CTF 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. However, according to law enforcement intelligence sources, criminal organizations based in Hawaii and California are involved in the trafficking of cocaine, MDMA and crystal methamphetamine into the island nations including Samoa. Additionally, South American and Australian based organizations use the South Pacific islands as transhipment locations for cocaine being shipped from South America into Australia and New Zealand

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) initially enacted the Money Laundering Prevention Act (the Act) in 2000 that was repealed and replaced by the new Money Laundering Prevention Act 2007. This law criminalizes money laundering associated with numerous crimes sets measures for the prevention of money laundering and requires related financial supervision. 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 U.S. $354,000), a term of imprisonment not to exceed seven years, or both. This penalty is not found in the 2007 Act itself but derives from the separate Proceeds of Crime Act of 2007, which includes specific penalties for money laundering.

The Act requires financial institutions to report transactions considered suspicious to the Samoa Financial Intelligence Unit (FIU) established by the Money Laundering Prevention Authority presently under the auspices of the Governor of the Central Bank. The FIU receives and analyses disclosures from either a local financial or government institution or agency (either domestic or of a foreign state). If it establishes reasonable grounds to suspect that a transaction is suspicious, it may disclose the report to an appropriate local or foreign government or law enforcement agency. A Money Laundering Prevention Task Force (MLPTF) is established under the new Act to advise or make recommendations to the MLPA. More importantly, the MLPTF is tasked to ensure close liaison and cooperation and coordination between various GOS departments and corporations. In 2003, Samoa established under the authority of the Ministry of the Prime Minister an independent and permanent Transnational Crime Unit (TCU). The TCU is staffed by personnel from the Samoa Police Service, Immigration Division of the Ministry of the Prime Minister and Division of Customs. The TCU is responsible for intelligence gathering and analysis and investigating transnational crimes, including money laundering, terrorist financing and the smuggling of narcotics and people.

The Act requires financial institutions to establish and maintain with appropriate backup or recovery all business transactions records and correspondence records for a minimum of five years, and to identify and verify a customer's identity when establishing a business relationship; when there is a suspicion of a Money Laundering offense or terrorist financing; or when there is doubt about the veracity or adequacy of the customer identification, or verification, documentation, or information previously obtained.

Section 31 of the Act requires that all financial institutions have an obligation to appoint a compliance officer responsible for ensuring compliance with the Act, and to establish and maintain procedures and systems to implement customer identification requirements, implement record keeping, retention, and reporting requirements and to make its officers and employees aware of procedures, policies and audit systems. Each financial institution is also required to train its officers, employees and agents to recognize suspicious transactions. A financial institution required to be audited must incorporate compliance with the MLPA 2007 as part of its audit to be confirmed by the auditor. Currency reporting at the border requires any person leaving or entering Samoa with more than $20,000 or other prescribed amount in cash or negotiable bearer instruments (in Samoan currency or equivalent foreign currency) either on their person or in their personal luggage to report this to the Financial Intelligence Unit.

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

Samoa is an offshore financial jurisdiction with six offshore banks licensed. For entities registered or licensed under the various Offshore Finance Centre Acts, there are no currency or exchange controls or regulations, and no foreign exchange levies payable on foreign currency transactions. No income tax or other duties, nor any other direct or indirect tax or stamp duty is payable by registered/licensed entities. In addition to the six offshore banks, Samoa currently has 25,383 international business corporations (IBCs) three international insurance companies, seven trustee companies, and 182 international trusts. Section 19 of the International Banking Act requires the directors and Chief Executive to be “fit and proper” and 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, which is defined in section 3 of the Act.

International cooperation can occur in several ways under the provisions of three pieces of legislation: the Money Laundering Prevention Act 2007, the Proceeds of Crime Act 2007, and Mutual Assistance in Criminal Matters Act 2007. All cooperation under the MLPA is through the Financial Intelligence Unit (FIU) under the new Money Laundering Prevention Act 2007, which allows exchange of information not only on a national but also on an international basis between the FIU and other domestic law enforcement and regulatory agencies. Under the Proceeds of Crime Act 2007, a foreign State can request assistance to issue a restraining order in respect of a foreign serious offense. The Attorney General under the Mutual Assistance in Criminal Matters Act 2007 can authorize the giving of assistance to a foreign state. Assistance to a foreign state can be in the form of locating or identifying persons or providing evidence or producing documents or other articles in Samoa. In 2002, Samoa enacted the Prevention and Suppression of Terrorism Act. The Act defines and criminalizes terrorist offenses, including offenses dealing specifically with the financing of terrorist activities. The combined effect of the Money Laundering Prevention Act of 2007 and the Prevention and Suppression

of Terrorism Act of 2002 is to make it an offense for any person to provide assistance to a criminal to obtain, conceal, retain or invest funds or to finance or facilitate the financing of terrorism.

Samoa is a member of the Asia/Pacific Group on Money Laundering and the Pacific Islands Forum. Samoa hosted the annual plenary of the Pacific Islands Forum in August 2004. Samoa has not signed the 1988 UN Drug Convention or the UN Convention against Transnational Organized Crime. Samoa became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. However there is no information to indicate whether Samoa circulates either the UNSCR 1267 or the U.S. lists of designated terrorist entities.

The Financial Intelligence Unit (FIU) within the Central Bank has continued to strengthen its anti-money laundering regime as evident in the new Money Laundering Prevention Act 2007. The new Act is explicitly mandates that all financial institutions conduct customer due diligence and prohibit any transactions where there is no satisfactory evidence of a customers identity. A financial institution is obliged to keep records of all business transaction records and related correspondence, records of a customer's identity, and of all reports made to the FIU, and any enquiries made to it by the FIU on money laundering and terrorist financing matters. Anonymous accounts are strictly prohibited, and transactions are required to be monitored by financial institutions. The scope of record keeping by financial institutions (like banks and money transmission service providers) is extended to include accurate originator information and other related messages made via electronic fund transfers.

The Government of Samoa (GOS) has made progress in developing its anti-money laundering/counter-terrorist finance regime in 2007 by enacting the Money Laundering Prevention Act. The GOS should ensure that financial institutions submit suspicious transaction reports (STRs) to the FIU and that the FIU forwards any STR worthy of investigation to law enforcement for possible prosecution. The GOS should effectively regulate its offshore financial sector by ensuring that the names of the actual beneficial owners of international business companies and banks are on a registry accessible to law enforcement. The GOS should ensure that the UNSCR 1267 Sanctions Committee Consolidated and U.S. lists are circulated and an effective asset forfeiture regime is established and implemented. The GOS should adhere to the FATF's 9 Special Recommendations on Terrorist Financing. In particular, Samoa should take steps to implement Special Recommendation IX on cash couriers and ensure that its entry and exit points are not used for either the transhipment of narcotics, the sale of imported narcotics, or the funds derived from either illicit activity.

Saudi Arabia

Saudi Arabia is a growing financial center in the Gulf Region of the Middle East. There is little known narcotics related money laundering in the Kingdom. Saudi officials acknowledge difficulty in detecting terrorist financing due to the abundance of cash funds in the country. 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, 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 trans-shipment of goods not entering the country. There was no significant increase in financial crimes during 2007, although the proceeds of crime from stolen cars and counterfeit goods are substantial. A definitive determination is hard to make because of the absence of official criminal statistics.

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 Government officials individually, funded al-Qaida. Following the al-Qaida bombings in Riyadh on May 12, 2003, the Saudi Arabian government (SAG) has taken significant steps to counteract terrorist financing.

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

SAMA guidelines generally correspond to the Financial Action Task Force (FATF) 40 Recommendations and the Nine Special Recommendations on Terrorist Financing. On May 27, 2003, SAMA issued updated anti-money laundering and counter-terrorist finance guidelines for the Saudi banking system. The guidelines require that banks have mechanisms to monitor all types of "Specially Designated Nationals" as listed by SAMA; that fund transfer systems be capable of detecting specially designated nationals; banks strictly adhere to SAMA circulars on opening accounts and dealing with charity and donation collection; and the banks be able to provide the remitter's identifying information for all outgoing transfers. The guidelines also require banks to use software to profile customers to detect unusual transaction patterns; establish a monitoring threshold of 100,000 Saudi Riyals (U.S. $26,667); 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 SAG provides anti-money laundering training for bank employees, prosecutors, judges, customs officers and other government officials.

In 2003, the SAG established an anti-money laundering unit in SAMA, and in 2005 the SAG established the Saudi Arabia Financial Investigation Unit (SAFIU), which acts as the country's financial intelligence unit (FIU) within the Ministry of Interior. Saudi banks are required to have anti-money laundering units with specialized staff to work with SAMA, the SAFIU and law enforcement authorities. All banks are also required to file suspicious transaction reports (STR) with the SAFIU. The SAFIU collects and analyzes STRs and other available information and makes referrals to the Bureau of Investigation and Prosecution, the Mabahith (the Saudi Security Service), and the Public Security Agency for further investigation and prosecution. The SAFIU is staffed by officers from the Mabahith and SAMA. The SAFIU is not yet a member of the Egmont Group of FIUs.

Hawala transactions outside banks and licensed moneychangers are illegal in Saudi Arabia. Some instances of money laundering and terrorist finance in Saudi Arabia have involved hawala. 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 an effort to further regulate the more than $16 billion in annual remittances that leave Saudi Arabia, SAMA consolidated the eight largest moneychangers into a single bank, Bank Al-Bilad, in 2005.

In June 2007 the SAG enacted stricter regulations on the cross-border movement of money, precious metals, and jewels. Money and gold in excess of U.S. $16,000 must be declared upon entry and exit from the country using official Customs forms.

Contributions to charities in Saudi Arabia usually consist of Zakat, which refers to an Islamic religious duty with specified humanitarian purposes. In 2002, Saudi Arabia announced its intention to establish a National Commission for Relief and Charitable Work Abroad (aka the Charities Commission), a mechanism that would oversee all private charitable activities abroad. Until the Charities Commission is established, no Saudi charity can send funds abroad. As of October 2007, the proposal was still under review by Saudi officials. 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' financial records and has established an electronic database to track the operations of such charities. New banking rules implemented in 2003 that apply to all charities include stipulations that they can be only opened in Saudi Riyals; must adhere to enhanced identification requirements; must utilize one main consolidated account; and must make payments only by checks payable to the first beneficiary, which then must be 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 SAG officials, these regulations apply to international charities as well and are 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) in November 2004 and was one of MENAFATF's original charter signatories.

It is the policy and practice of the SAG to comply with obligations under UN Security Council resolutions (UNSCR) 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.

The SAG is a party the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The SAG has signed but has not yet ratified the UN Convention against Corruption. In August 2007, Saudi Arabia ratified the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Saudi Arabia is taking steps towards enforcing its anti-money laundering/counter-terrorist finance laws, regulations, and guidelines. However, it needs to take concrete steps to establish the Charities Commission and to enhance its oversight and control of Saudi charities with overseas operations. Charitable donations in the form of gold, precious stones and other gifts should be scrutinized. 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. The public dissemination of statistics regarding predicate offenses and money laundering prosecutions would facilitate the evaluation and design of enhancements to the judicial aspects of its AML system. The SAG should ratify the UN Convention against Corruption.

Senegal

A regional financial center with a largely cash-based economy, Senegal is vulnerable to money laundering. Reportedly, most money laundering involves domestically generated proceeds from corruption and embezzlement. Recent arrests of opposition politicians, journalists, and a corruption scandal that resulted in the early retirement, rather than prosecution of the implicated judges, illustrate these vulnerabilities. There is also concern that criminal figures launder and invest their own and their organization's proceeds from the growing West Africa narcotics trade. There is also evidence of

increasing criminal activity by foreigners, such as narcotics trafficking by Latin American groups and illegal immigrant trafficking involving Pakistanis.

Dakar's active real estate market is largely financed by cash and property ownership and transfer is nontransparent. The building boom and high property prices suggest that an increasing amount of funds with an uncertain origin circulates in Senegal. Trade-based money laundering (TBML) is centered in the region of Touba, a largely autonomous and unregulated free-trade zone under the jurisdiction of the Mouride religious authority. Touba reportedly receives between U.S. $550 and $800 million per year in funds repatriated by networks of Senegalese traders and vendors abroad. Other areas of concern include cash, gold and gems transiting Senegal's airport and porous borders, as well as real estate investment in the Petite Cote south of Dakar.

Seventeen commercial banks operate alongside thriving micro credit and informal sectors. The Government of Senegal (GOS) is attempting to discourage its civil servants from using cash by depositing salaries into formal bank accounts, and the Banking Association has begun a publicity campaign to encourage the populace to use the formal banking system. Western Union, Money Gram and Money Express, associated with banks, compete with Senegal's widespread informal remittance systems, including hawala networks and the use of cash couriers. Small-scale, unregulated and nonlicensed currency exchange operations are also common, especially outside urban centers. The Banque de l'Habitat du Senegal (BHS), a Senegalese bank, has affiliates licensed as money remitters in the United States. New York State authorities have brought an enforcement action against BHS New York for failing to comply with anti-money laundering (AML) regulations.

The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the eight countries in the West African Economic and Monetary Union (WAEMU or UEMOA), including Senegal, and uses the CFA franc currency. The Commission Bancaire, the BCEAO division responsible for bank inspections, is based in Abidjan. However, it does not execute a full AML examination during its standard banking compliance examinations. Senegal has no offshore banking sector.

Senegal's currency control and reporting requirements are not uniform and are reportedly laxly enforced. There is no publicity about currency declaration requirements at major points of entry. Nonresidents on entry must declare any currency they are transporting from outside the "zone franc" greater than one million CFA (approximately U.S. $2,000). They must also declare monetary instruments denominated in cash in any amount. When departing Senegal, nonresidents must declare any currency from outside the franc zone greater than approximately U.S. $1,000 as well as all monetary instruments from foreign entities. The law does not require residents to declare currency on entry; on exit, they must declare amounts any foreign currency and any monetary instruments greater than approximately U.S. $4,000. All declarations must be in writing. Customs authorities are primarily concerned with the importation of dutiable goods. Because land border crossings are patrolled by other authorities with differing mandates, currency control is not a priority.

The legal basis for Senegal's anti-money laundering/counter-terrorist financing (AML/CTF) framework is Loi Uniforme Relative a Lutte Contre le Blanchiment de Capiteaux No. 2004-09 of February 6, 2004, or the Anti-Money Laundering Uniform Law (Uniform Law). As the common law passed by the members of l'UEMOA/WAEMU, all member states are bound to enact and implement the legislation. Among the union, Senegal is the first country to have the legal framework in place. Senegal has an "all crimes" approach to money laundering. Self launderers may be prosecuted and it is not necessary to have a conviction for the predicate offense. Intent may be inferred from objective factual circumstances. Criminal liability applies to all legal persons as well as natural persons.

The new legislation meets many international standards with respect to money laundering, and eclipses them in some areas such as with regard to the microfinance sector, but does not comply with all Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations.

The legislation also lacks certain compliance provisions for nonfinancial institutions. Although Senegal has not passed a CTF law, the penal code was amended in March 2007 to incorporate the United National Security Council Resolution (UNSCR) requirements for terrorist financing. In July 2007, l'UEMOA/WAEMU released guidance on terrorist financing for the sub-region alongside Directive No. 04/2007/CM/UEMOA, obliging member states to pass domestic CTF legislation.

The law requires banks and other financial institutions to know their customers and record and report the identity of any engaged in significant transactions, including the recording of large currency transactions. Banks monitor and record the origin of any deposit higher than 5 million CFA (approximately U.S. $10,000) for a single individual account and 20 to 50 million CFA (approximately U.S. $40,000 to 100,000) for any business account. Commercial banks in Senegal are improving their internal controls and enhancing their "know your customer" (KYC) requirements. The law also contains safe harbor provisions for individuals who file reports.

Cellule Nationale de Traitement des Informations Financiers (CENTIF), Senegal's financial intelligence unit (FIU) became operational in August 2005. The FIU currently has a staff of 27, 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 Ministry of Justice. Senegal's FIU is working to improve its operational abilities and is raising the awareness of the threat of money laundering in Senegal. CENTIF has provided outreach and training for obliged entities to familiarize them with their requirements and to improve the quality and variety of STRs that the FIU receives. Senegal's FIU has applied for membership in the Egmont Group.

The police, gendarmerie and Ministry of Justice's judicial police are technically responsible for investigating money laundering and terrorist financing. However, in reality, CENTIF reportedly retains its information and tasks law enforcement entities to investigate or retrieve information for its cases. CENTIF reportedly does not share or disseminate its information or financial intelligence to law enforcement. In 2007, CENTIF received 71 suspicious transaction reports (STRs), mostly from banks, and referred 11 cases to the Prosecutor General who, in turn, passed the cases directly to the investigating judge. No cases have concluded, although authorities have made one arrest. Official statistics regarding the prosecution of financial crimes are unavailable. There is one known conviction for money laundering since 2005. The conviction led to the confiscation of a private villa.

The Uniform Law provides for the freezing, seizing, and confiscation of property by judicial order. In addition, the FIU can order the suspension of the execution of a financial transaction for 48 hours. The BCEAO can also order the freezing of funds held by banks. The Uniform Law allows explicitly for criminal forfeiture. There is no provision for civil forfeiture.

The BCEAO has released a Directive against Terrorist Financing. Member states must enact a law against terrorist financing, which is a Uniform Law to be adopted by all WAEMU/UEMOA members parallel to the AML law. Like the AML law, the terrorist financing law is a penal law. Each national assembly must enact enabling legislation to adopt the new terrorist finance law. The FATF-style regional body (FSRB) for the 15 members of the Economic Community of Western African States (ECOWAS) known as the Intergovernmental Action Group Against Money Laundering in West Africa (GIABA) has also drafted a uniform law, which it hopes that all of its member states will enact. Senegal is a member of this body, which evaluated Senegal in 2007.

The BCEAO and the FIU circulate the UN 1267 Sanctions Committee consolidated list to commercial financial institutions. To date, no entity has been identified. The WAEMU/UEMOA Council of Ministers issued a directive in September 2002 requiring banks to freeze the assets of any 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 address extradition and legal assistance among the member countries. Under the Uniform Law, the FIU may share information freely with other WAEMU/UEMOA FIUs. However, Senegal has the only operational FIU within this community. CENTIF has signed a Memorandum of Understanding (MOU) for information exchange with the FIUs of Belgium, Nigeria, Algeria and Lebanon, and is working on other accords. CENTIF is open to information exchange on a reciprocity basis and shares information with FIUs of the Egmont group even without signed MOUs. The Senegalese government and law enforcement agencies are generally willing to cooperate with United States law enforcement agencies. The Government of Senegal (GOS) has also worked with INTERPOL, Spanish, and Italian authorities on international anti-crime operations.

Senegal is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the 1999 UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. In 2007, Senegal was ranked 71 out of 180 countries in Transparency International's Corruption Perceptions Index.

The Government of Senegal should continue to work with its partners in WAEMU/UEMOA and ECOWAS to establish a comprehensive anti-money laundering and counter-terrorist financing regime. Senegal should work on achieving transparency in its financial and real estate sectors, and continue to encourage the populace to use the formal banking system, steering them away from cash transactions. Senegal should increase the frequency and effectiveness of financial reviews and audits and continue to battle corruption. Senegal should lead its regional partners and establish better uniform control of cross-border flow of currency and other bearer-negotiable instruments for both residents and nonresidents. Senegalese law enforcement and customs authorities need to develop their expertise in identifying and investigating both traditional money laundering and money laundering within the informal economy. CENTIF should perform more outreach for obliged nonbank financial institutions to ensure a better understanding of STRs, when to file them and the information they should contain. CENTIF, law enforcement and Ministry of Justice authorities should work together to coordinate roles and responsibilities with regard to case investigation and assembly, and develop a deeper interagency understanding of money laundering and terrorist financing. Senegal should amend its AML legislation to address the remaining shortcomings, and criminalize terrorist financing.

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, 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 (TBML), 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 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. Serbia has 14 designated free trade zones, three of which are in operation. Serbia established the free trade zones 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. 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's expanded definition of money laundering in the Penal Code broadens the scope of money laundering and aims to conform to international standards. This legislation also gives police and prosecutors more flexibility to pursue money laundering charges. 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.

Under Serbia's 2005 revised anti-money laundering law (AMLL) obliged entities must report suspicious transactions in any amount to the FIU. The law expands those sectors subject to reporting and record keeping requirements, adding attorneys, auditors, tax advisors and accountants, currency exchanges, insurance companies, casinos, securities brokers, dealers in high value goods, real estate agencies, and travel agents to those already required to comply with the AMLL provisions. The AMLL also expands the number of entities required to collect certain information and file currency transaction reports (CTRs) with the financial intelligence unit (FIU) on all cash transactions exceeding 15,000 euros (approximately U.S. $22,000), or the dinar equivalent. These entities must also retain records for five years. Financial institutions have realized significant improvement in their compliance, i.e., gathering and keeping records on customers and transactions. 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. Safe harbor provisions protect the entities with respect to their cooperation with law enforcement entities. The flow of information to the FIU has been steadily increasing, but not all entities are yet subject to implementing bylaws. The AMLL also eliminates a previous provision limiting prosecution to crimes committed within Serbian territory.

The Law on Foreign Exchange Operations, adopted in 2006, criminalizes the use of false or inflated invoices or documents to conceal the illicit transfer of funds out of the country. Serbia enacted this law in part to counter the perceived problem of import-export fraud and TBML. The Foreign Currency Inspectorate, part of the Ministry of Finance, is responsible for supervising import/export companies for compliance. The law also requires residents and nonresidents declare to Customs authorities all currency (foreign or dinars), or securities in amounts exceeding 5,000 euros (approximately U.S. $7,000) 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. The NBS is developing similar regulations 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, but the NBS has not yet used this revocation authority. Although the legal framework is in place, 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 and monitors its obligors' compliance with the AML Laws. The SC is developing regulations to implement this authority. 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.

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 has created 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 Administration for the Prevention of Money Laundering (APML) 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. This provides more autonomy for the agency to carry out its mandate, as well as additional resources. APML has its own line item operating budget. The FIU has developed listings of suspicious activity red flags for banks, currency exchange offices, insurance companies, securities brokers and leasing companies. APML also has the authority to freeze transactions for 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.

From January 1, 2007 through November 19, 2007, the FIU received 1,572 suspicious transaction reports (STRs). Nearly all of the STRs received by the FIU have been filed by commercial banks. In 2007, the FIU opened 46 cases and referred 119 cases to law enforcement, investigative agencies, or the prosecutor's office for further investigation. A total of six criminal charges were submitted for money laundering charges in 2007. The most common predicate crime is "abuse of office".

In Serbia, it is difficult to convict a suspect of money laundering without a conviction for the predicate crime. In addition, courts are unwilling to accept circumstantial evidence to support money laundering or tax evasion charges. This hampers law enforcement and prosecutorial authorities from 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 counter these challenges and better focus financial investigations.

The GOS has established the Permanent Coordinating Group (PCG), an interagency working group originally tasked with developing an implementation plan for the recommendations from the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures' (MONEYVAL), first-round evaluation. Subgroups have since worked to draft amendments to the AMLL that will bring the country's laws into compliance with the European Union's Third Directive on money laundering. The PCG and the working groups meet intermittently as required for completing specific tasks. However, the GOS still lacks consistent interagency coordination.

Under the law, the GOS can, upon conviction for an offense, confiscate assets derived from criminal activity or suspected of involvement in terrorist financing. The FIU enforces the United Nations Security Council Resolution (UNSCR) 1267 provisions regarding suspected terrorist lists. Although the FIU routinely provides the UN list of suspected terrorist organizations to the banking community, examinations for suspect accounts have revealed no evidence of terrorist financing within the banking system. 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 draft anti-terrorism finance legislation. This draft law on terrorist financing, now pending Parliamentary approval, will apply all provisions of the AMLL to terrorist financing, require reporting to the FIU of transactions suspected to be terrorist financing and will create mechanisms for freezing, seizing and confiscation of suspected terrorist assets based on UNSCR provisions.

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.

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 Republic 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 MONEYVAL, Serbia will undergo a mutual evaluation in 2009. The FIU is a member of the Egmont Group and participates in information exchanges with counterpart FIUs including FinCEN. APML has also signed information sharing memoranda of understanding (MOUs) with eleven counterpart FIUs.

Serbia is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN Convention Against Transnational Organized Crime. The GOS also 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. Domestic implementation procedures, however, do not provide the framework for full application of Convention provisions.

Serbia should continue to work toward eliminating the abuses of office and the culture of corruption that enables money laundering and financial crimes. The GOS should take action to realize and implement the pending legislative initiatives necessary for Serbia to fully comply with international standards. These include the laws providing for the liability of legal persons and regulations applying all requirements of the AMLL to covered nonbank financial institutions. The GOS should enforce anti-money laundering regulations pertaining to money service businesses and obligated nonfinancial business and professions. Serbia should complete its supervisory scheme, and enact binding implementing regulations for the insurance and securities sectors. The GOS should also enact 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 legislation needed to comply with UN Security Council resolutions regarding the freezing, seizing and confiscation of suspected terrorist assets and to require suspicions of terrorist financing to be reported to the FIU. The National Bank and other supervisory bodies need to enhance their knowledge and receive additional staff. On an operational level, law enforcement needs audit and investigative capacity to investigate the STRs that the FIU disseminates. Prosecutors and judges also need a better understanding of money laundering and terrorist financing to ensure successful prosecutions. 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 2007, there were 34,000 registered international business companies (IBCs) and 160 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, registers, licenses and regulates offshore activities. The SIBA licenses and registers agents who carry out due diligence tests when registering new companies in the Seychelles offshore sector. The SIBA also regulates activities of the Seychelles International Trade Zone.

In addition to IBCs and trusts, Seychelles permits offshore insurance companies, mutual funds, and offshore banking. In November 2006, the GOS established the Non-Bank Financial Services Authority, which is 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: 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 its 2007-2017 Strategic Plan, the Seychelles Government proposes to facilitate the development of the financial services sector as a third pillar of the economy. It plans to achieve this through actively promoting Seychelles as an internationally recognized offshore jurisdiction, with emphasis on IBCs, mutual funds, special license companies and insurance companies.

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 suspicious transactions to the Central Bank, which now houses the financial intelligence unit (FIU), 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 its implementation, 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 nonbank financial institutions, such as exchange houses, stock brokerages, insurance agencies, lawyers, notaries, accountants, and estate agents. Offshore banks are also explicitly covered. The gaming sector is also obliged to report. However, although Internet gaming is also obligated, the law does not state explicitly that offshore gaming is covered in an identical manner. 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 an STR, criminalizes tipping off, and sets safe harbor provisions. The new law also requires reporting entities to take “reasonable measures” to ascertain the purpose of any transaction in excess of Seychelles rupees 100,000 (approximately U.S. $12,500), or of rupees 50,000 (approximately U.S. $6,250) in the case of cash transactions, and the origin and destination of the funds involved in the transaction. However, it 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 rupees 50,000” (approximately U.S. $6,250); 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 rupees 3,000,000 (approximately U.S. $375,000) in penalties. While there have been 49 investigations, there have been no arrests or prosecutions for money laundering or terrorist financing since January 1,

2003. Of the 49 cases, eight were closed due to lack of evidence. In three cases, the suspects had left Seychelles, and in one case, the suspect had died. The remaining cases are still pending investigation.

The Financial Institutions Act of 2004 imposes more stringent rules on banking operations and brings the Seychelles' regulatory framework closer to compliance with international standards. The law aims to ensure greater transparency in financial transactions by regulating the financial activities of both domestic and offshore banks. Among other provisions, 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 Financial Intelligence Unit (FIU) was established under Section 16 of the 2006 AMLA. The FIU operates within the Central Bank of Seychelles. Prior to the establishment of the FIU, the Bank Supervision Division of the Central Bank of Seychelles performed the duties of the FIU. The FIU is the focal point for receiving, analyzing, and disseminating reports of transactions related to money laundering or the financing of terrorism to the appropriate law enforcement and supervisory agencies in Seychelles. To support these core functions, the FIU is authorized to collect information that it considers pertinent and is also empowered to request additional information from reporting entities, law enforcement and supervisory agencies. The law provides for the FIU to have a proactive targeting section to research trends and developments in money laundering and terrorist financing. The FIU also performs examinations of the reporting entities and, in concert with regulators, issues guidance related to customer identification, identification of suspicious transactions, and record keeping and reporting obligations. The FIU is currently in the process of updating a set of guidelines on anti-money laundering/counter-terrorist financing (AML/CTF), which dates back to 1998, for the reporting entities in accordance with the requirements of the AMLA 2006. In December 2006, the Seychelles Government established a National Anti-Money Laundering Committee to better coordinate the efforts of the various law enforcement agencies in combating financial crimes. The Committee is chaired by the FIU, and comprises representatives of the Police, the Attorney General's Office, Customs, Immigration, the Seychelles Licensing Authority, and the Seychelles International Business Authority.

The FIU 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. 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; however, the report has not been presented to the plenary body or finalized. The Seychelles is a party to the 1988 UN Drug Convention, the UN Convention Against Corruption, 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 with its FIU to ensure it has the training and resources needed for outreach, analysis and dissemination, and comports with the membership criteria of the Egmont Group of FIUs. 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 participate more actively in ESAAMLG, and when the mutual evaluation report is finalized, address any further identified deficiencies.

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.

Former President Kabbah 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 for obliged entities. There is a currency reporting requirement for deposits larger than 25 million leones (approximately U.S. $8,330) and no minimum for suspicious transaction reporting. The law requires that international financial transfers over U.S. $10,000 use formal financial channels. The AMLA also institutes cross-border currency reporting requirements for cash or securities in excess of U.S. $10,000. The law designates the Governor of the Bank of Sierra Leone as the national Anti-Money Laundering Authority.

Subject to the AMLA reporting requirements are 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. The AMLA also imposes reporting requirements on designated nonfinancial businesses and professions such as casinos, realtors, dealers in precious metals and stones, notaries, legal practitioners, and accountants.

A financial intelligence unit (FIU) exists but lacks the capacity to effectively monitor and regulate financial institution operations, and in particular lacks the technological capability necessary to maintain databases, track actors and patterns, and monitor online transactions. Law enforcement and customs authorities 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 training workshop with the United Nations Office on Drugs and Crime and Intergovernmental Group for Action Against Money Laundering (GIABA) on strategy development for anti-money laundering and combating financing of terrorism. Workshop participants recommended that the Bank of Sierra Leone draft a national anti-money laundering strategy and regulatory regime for reporting suspicious transactions to the FIU. Other recommendations focused on the FIU itself, including developing regulations for the operations of the FIU and establishing a system for the receipt, analysis, and dissemination of financial disclosures. Preparation of Sierra Leone's strategy paper has been delayed because new individuals are now involved with implementing the AMLA following the August 2007 parliamentary elections. As of late 2007, the Bank of Sierra Leone prepared the draft and recommended improving governance, setting up robust AMLA enforcement, reforming the financial sector and improving cooperation among local and regional institutions with regard to monitoring and reporting money laundering activities

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

Sierra Leone is member of the Inter-Governmental Action Group against Money Laundering and Terrorist Financing in West Africa (GIABA), a FATF-style regional body (FSRB). The mutual evaluation report for Sierra Leone was conducted by the World Bank and discussed at the GIABA Plenary in June 2007. The GOSL is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Sierra Leone is number 150 of 180 countries listed in Transparency International's 2007 Corruption Perception Index.

President Ernest Bai Koroma was elected in September 2007 and came into office pledging to fight corruption. If the President succeeds in creating an environment and legal framework to combat corruption, there will be a positive impact on the enforcement of laws against money laundering. Although the Government of Sierra Leone has passed anti-money laundering legislation, it remains to be effectively 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 must increase the level of awareness of money laundering issues throughout the country and allocate the necessary resources to facilitate the development of its anti-money laundering and counter-terrorist financing regime. Sierra Leone needs to develop implementing regulations for its legislation, institute a reporting regime, and strengthen its FIU through both training and technical assistance. The Sierra Leonean FIU should work toward membership in the Egmont Group. The GOSL should ensure that its counter-terrorist financing measures adhere to international standards. The GOSL should work to ensure that the UNSCR 1267 Sanctions Committee's consolidated list is distributed to financial institutions regularly. It needs to ratify the UN Convention against Transnational Organized Crime. Sierra Leone should also continue its efforts to counter the smuggling of diamonds and take steps to combat corruption at all levels of commerce and government.