Country Reports

Afghanistan

While Afghanistan is not a regional financial or banking center, its informal financial system is extremely large in scope and scale. Afghanistan is a major drug trafficking and drug producing country. Afghanistan passed anti-money laundering and terrorist financing legislation in late 2004, and efforts are being made to strengthen police and customs forces. However, there remain few resources and little expertise to combat financial crimes, or to produce meaningful financial intelligence. The most fundamental obstacles continue to be legal, cultural and historical factors that conflict with more Western-style proposed reforms to the financial sector.

The majority of the money laundering in Afghanistan is linked to the illicit narcotics trade. Afghanistan accounts for a large majority of the world's opium production, and in 2004 and 2005 its internal production of opium increased. Opium gum itself is often used as a currency, especially by rural farmers, and it is used as a store of value in prime production areas. It is estimated that one third of Afghanistan's (licit plus illicit) GDP is derived directly from narcotics activities, and proceeds generated from the drug trade have reportedly fueled a growing real estate boom in Kabul, as well as a sharp increase in capital investment in rural poppy growing areas.

Afghan opium is refined into heroin by production labs, more of which are being established within Afghanistan's borders. The heroin is then often broken into small shipments and smuggled across porous borders for resale abroad. Payment for the narcotics outside the country is facilitated through a variety of means, including through conventional trade and the hawala system (money dealers). The narcotics themselves are often used as tradable goods and as a means of exchange for foodstuffs, vegetable oils, electronics, and other goods between Afghanistan and neighboring Pakistan. Many of these goods are smuggled into Afghanistan from neighboring countries or enter through the Afghan Transit Trade without payment of customs duties or tariffs. Invoice fraud, corruption, indigenous smuggling networks, and legitimate commerce are all intertwined.

Afghanistan is widely served by the hawala system, which provides a range of financial and non-financial business services in local, regional, and international markets. Financial activities include foreign exchange transactions, funds transfers, micro and trade finance, as well as some deposit-taking activities. While the hawala network may not provide financial intermediation of the same type as the formal banking system (i.e., deposit-taking for lending and investing purposes based on the assessment, underwriting, and pricing of risk(s)), it is deeply entrenched and widely used throughout Afghanistan.

There are over 330 known hawala dealers in Kabul, with 100-300 additional dealers in each province. These dealers are organized into unions in each province and maintain a number of agent-principal and partnership relationships with other dealers throughout the country and internationally. Their record keeping and accounting practices are quite robust, extremely efficient, and take note of currencies traded, international pricing, deposit balances, debits and credits with other dealers, lending, cash on hand, etc. Hawaladars are supposed to be registered. However, consistent standards for record keeping and accounting do not exist among these dealers, further complicating the regulatory task.

In early 2004, the Central Bank of Afghanistan, Da Afghanistan Bank (DAB), worked in collaboration with the International Monetary Fund (IMF) and the United Nations Office on Drugs and Crime (UNODC) to establish the legislative framework for anti-money laundering and the suppression of the financing of terrorism. Although Afghanistan was unable to meet its initial commitment to enact both

pieces of legislation by September 30, 2004, they were both finalized and signed into law by late October 2004.

The Central Bank claims that both the Anti-Money Laundering (AML) and Proceeds of Crime and Combating the Financing of Terrorism (CFT) laws incorporate provisions that are designed to meet the recommendations of the Financial Action Task Force (FATF) and address the criminalization of money laundering and the financing of terrorism, customer due diligence, the establishment of a Financial Intelligence Unit (FIU), international cooperation, extradition, and the freezing and confiscation of funds. In fact, the AML law also includes provisions to address cross-border currency reporting, and establishes authorities to seize and confiscate monies found to be undeclared or falsely declared, or determined to be transferred for illicit purposes. However, the capability to enforce these provisions is nearly non-existent, and furthermore, these provisions are largely unknown in many parts of the country.

Under the new AML law, an FIU has been established and will function as a semi-autonomous unit within DAB. Additionally, banks are required to report suspicious transactions and all cash transactions as prescribed by DAB to the FIU, which has the legal authority to freeze assets for up to 7 days. The FIU will refer cases to the Attorney General's office which will assign it to the appropriate court. The FIU, originally set to be established in January 2005, was actually initiated in October 2005 with assignment of a General Director, office space, and other resources. However, a number of key organizational issues remain to be resolved before the FIU can be considered fully operational.

At present the formal banking sector consists of three recently re-licensed state-owned banks, five branches of foreign banks, and four additional domestic banks. With the possible exception of the foreign bank branches, these banks are equipped with only limited knowledge or technical capacity to produce financial intelligence. Many are looking to both the Central Bank and to the Ministry of Finance to provide training on requirements set forth by anti-money laundering legislation, including customer due diligence and "know your customer" provisions (KYC), record keeping, currency transaction reporting (CTRs), suspicious transaction reporting (STRs), and the establishment of internal AML/CFT controls. The DAB is working to meet these bank demands by developing its anti-money laundering regulatory regime and supporting training curricula. The DAB is not yet fully aware of the compliance capabilities of banks other than those that are state-owned.

The Supervision Department within the DAB was formed at the end of 2003, and is divided into four divisions: Licensing, General Supervision (which includes on-site and off-site supervision), Special Supervision (which deals with special cases of problem banks), and Regulation. The Department remains poorly staffed and struggles to find the appropriate talent. The Department is charged with administering the AML and CFT legislation, conducting examinations, licensing new institutions, overseeing money service providers, and liaising with the commercial banking sector generally. In 2005, two members of the Supervision Department traveled to the U.S. to receive comprehensive AML training. Three more members are scheduled to receive similar training in 2006.

In April 2004, Afghanistan issued new regulations for the licensing of foreign exchange dealers, hawaladars and other money service providers, and required them to submit quarterly transaction reports. Regulations differ for foreign exchange dealers and money service providers, with more stringent requirements placed on the latter. The regulations also require foreign exchange dealers and money service providers to take appropriate measures to prevent money laundering and terrorist financing, including the submission of suspicious transaction reports to the FIU. DAB branch managers have been trained on the licensing requirements, but to date only one entity-Western Union-has received a license. The DAB is phasing in its regulations and has little communication with the foreign exchange dealers and money service providers themselves, many of whom see the regulations as overly strict, requiring burdensome capital requirements and fees for agents in each province. The

DAB is struggling with administering the regulations and lacks the support of enforcement authorities from the Ministry of Interior, among others.

The Ministry of Interior and the Attorney General's Office are the primary financial enforcement authorities, although neither is able to conduct financial investigations, and both lack the training necessary to follow potential leads generated by an FIU, whether within Afghanistan or from international sources. Pursuant to the Central Bank law, a Financial Services Tribunal will be established to review certain decisions and orders of Da Afghanistan Bank (DAB), although there is a need for significant training for judges and administrative staff before this Tribunal can be effectively stood up. The Tribunal will review supervisory actions of DAB, but not prosecute cases of financial crime. At present, all financial crime cases are being forwarded to the Kabul Provincial Court, where there has been little or no activity in the last three years. The process to prosecute and adjudicate cases is long and cumbersome, and significantly underdeveloped. The U.S., along with other countries, is helping to develop these mechanisms and to train prosecutors and judges.

Border security continues to be a major issue throughout Afghanistan. At present there are 21 border crossings that have come under federal control, utilizing international donor assistance as well as local and international forces. However, many of the border areas continue to be un-policed and therefore susceptible to illicit cross-border trafficking and trade-based money laundering. Many regional warlords also continue to control the international borders in their provincial areas, causing major security risks. Customs authorities, with the help of outside assistance, have made significant strides, but much work remains to be done. Customs collection has also dramatically improved, but there continues to be significant leakage and corruption, as well as trade-based fraud, including false invoicing and under-invoicing. Thorough cargo inspections are currently not conducted at any gateway.

Under the Law on Combating the Financing of Terrorism, any nonprofit organization that wishes to collect, receive, grant, or transfer funds and property must be entered in the registry with the Ministry of Auqaf (Islamic Affairs). All non-profit organizations are subject to a due diligence process which includes an assessment of accounting, record keeping, and other activities. However, the capacity of the Ministry to conduct such examinations is nearly non-existent, and the reality is that any organization applying for a registration is granted one. Furthermore, because no adequate enforcement authority exists, many organizations operating under a "tax-exempt" non-profit status in Afghanistan go completely unregistered and illicit activities are suspected on the part of a number of organizations.

The Government of Afghanistan (GOA) has now become a party to 12 of the UN conventions and protocols against terrorism and is a signatory to the International Convention for the Suppression of Acts of Nuclear Terrorism. Afghanistan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime.

While the Government of Afghanistan has made strides in strengthening its overall AML/CFT regime, much work remains to be done: overseeing the informal hawala system through effective regulation; enabling bank and non-bank financial institutions to produce adequate financial intelligence; developing a fully operational and effective FIU; bolstering financial investigative capabilities; and, training prosecutors and judges on money laundering and other financial crimes. These efforts must be conducted in tandem, while at the same time combating the overwhelming narcotics trade. A concerted effort on the part of international donors and Afghan authorities is needed to empower rural farmers through effective alternative livelihoods programs and to dismantle the logistical and financial infrastructure that facilitates the opium economy generally.

Albania

As a transit country for trafficking in narcotics, arms, contraband, and humans, Albania remains at significant risk for money laundering. Major sources of criminal proceeds are drug-related crimes, robberies, customs offenses, prostitution, trafficking in weapons and automobiles, official corruption, tax crimes and fraud. Organized crime groups use Albania as a base of operations for conducting criminal activities in other countries, sending the illicit funds back to Albania. The proceeds from these activities are easily laundered in Albania because of the lack of a strong formal economy and weak government controls. Money laundering is believed to be occurring through the investment of tainted money in real estate and business development projects. Customs controls on large cash transfers are not believed to be effective, due to a lack of resources and corruption of Customs officials.

Albania's economy is primarily cash-based. Electronic and ATM transactions are relatively few in number, but are growing rapidly as more banks introduce this technology. At the end of 2004, eight banks were offering ATM service with a total of 76 ATMs all over the country. The number of ATMs rapidly expanded following the decision of the Government of Albania (GOA) to deliver salaries through electronic transfers. Until 2004, the GOA paid its own civil servants in cash, but all central government institutions are now required to convert to electronic pay systems by the end of 2005. According to the Bank of Albania (the Central Bank), 25 percent of the money in circulation is outside of the banking system, compared to an average of 10 percent in other Central and Eastern European transitioning economies. There are 17 banks in Albania, but only five of them are considered to have a significant national presence. Albania is not considered an offshore financial center, nor do its current laws facilitate such types of activity. Under current law, free trade zones are permissible, but the GOA has not pursued the implementation of free trade zones and none are currently in operation.

The Albanian economy is particularly vulnerable to money laundering activity because it is a cash economy. Estimates place the informal sector at between 30 and 60 percent of GDP. Albania collects 10 to 15 percent less of GDP in taxes than neighboring countries. Relatively high levels of foreign trade activity, coupled with weak Customs controls, presents a gateway for money laundering in the form of fake imports and exports. The Bankers Association estimates that only 20-30 percent of transactions with trading partners take place through formal banking channels, reaching only a small portion of total imports. Likewise, a significant portion of remittances enters the country through unofficial channels. It is estimated that only half of total remittances enter through banks or money transfer companies. Black market exchange is still present in the country, especially in Tirana, despite repeated efforts by GOA institutions (Ministry of Interior, Bank of Albania, and Ministry of Finance) to impede such exchanges. There have been court decisions against illegal money remitters based on information received from foreign financial intelligence units.

Albania previously criminalized all forms of money laundering in Article 287 of the Albanian Criminal Code of 1995. Law No. 8610 "On the Prevention of Money Laundering" (passed in 2000) required financial institutions to report to an anti-money laundering agency all transactions that exceed approximately $15,000 as well as those that involved suspicious activity. Law No. 8610 required financial institutions to report all cross-border transactions that exceed approximately $10,000, as well as those that involve suspicious activity. Financial institutions are required to report transactions within 48 hours if the origin of the money cannot be determined. In addition, private and state entities are required to report all financial transactions that exceed certain thresholds. However, financial institutions had no legal obligation to identify customers prior to opening an account. While most banks have internal rules mandating customer identification, Law No. 8610 only required customer identification prior to conducting transactions that exceed 2 million Albanian leke (approximately $20,000) or when there is a suspicion of money laundering.

The laws set forth an "all crimes" definition for the offense of money laundering. However, an issue of concern is the fact that the Albanian court system requires a prior or simultaneous conviction for the predicate crime before an indictment for money laundering can be issued. Albanian law also has no specific laws pertaining to corporate criminal liability. Officials, however, state that legal entities can be punished for money laundering under Article 45 of the Criminal Code as well as under Article 14 of Law No. 8610.

In June 2003, Parliament approved Law No. 9084, which strengthened the old Law No. 8610, and improved the Criminal Code and the Criminal Procedure Code. The new law redefined the legal concept of money laundering, harmonizing the Albanian definition with that of the European Union (EU) and bringing it into line with EU and international conventions. Under the revised Criminal Code many powers were expanded and improved upon. The definition of money laundering was revised, the establishment of anonymous accounts was outlawed, and the confiscation of accounts was permitted. The law also mandates the identification of beneficial owners. Banks and other institutions are required to maintain records of suspicious activity reports for ten years. All other reports are subject to a five-year record retention period. The law also covers informal value transfer systems.

In the case of intermediaries, it is the responsibility of the appropriate licensing authority to supervise such entities for compliance (e.g., Ministry of Justice for notaries, Ministry of Finance for accountants). Although regulations also cover non-bank financial institutions, their enforcement has been poor in practice. The formal banking sector reports accounts for 90 percent of suspicious activity reports filed, while the rest come from state institutions like tax and customs and foreign counterparts. Currently, no law criminalizes negligence by financial institutions in money laundering cases. However, the Bank of Albania has established a task force to confirm banks' compliance with customer verification rules. Reporting individuals and entities are protected by law with respect to their cooperation with law enforcement agencies. However, given leaks of information from other agencies, reporting entities complain that reporting requirements compromise their client confidentiality and put them into a difficult position.

Banking groups initially objected to implementation of some aspects of the law, especially with regard to what they see as onerous reporting requirements. Originally, financial institutions were required to complete a 61-question form for all transactions, including bank-to-bank transfers, exceeding $200,000. Subsequent modifications to the form, however, have somewhat reduced this reporting burden. Financial institutions that submit reports are required to do so within 72 hours. In addition to banks, bureaux de change, casinos, tax and customs authorities, accountants, notaries, postal services, insurance companies, and travel agencies are entities that are obligated to comply with the threshold reporting rules.

Law No. 8610 also mandates the establishment of an agency to coordinate the GOA's efforts to detect and prevent money laundering. The General Directorate for Coordinating the Combat of Money Laundering (DBLKPP) is Albania's financial intelligence unit (FIU). The DBLKPP falls under the control of the Ministry of Finance and evaluates reports filed by financial institutions. If the agency suspects that a transaction involves the proceeds of criminal activity, it must forward the information to the prosecutor's office. In 2005, the FIU received 30 suspicious activity reports, four of which were passed to the prosecutor's office.

Law No. 9084 clarifies and improves the role of the FIU and increases its responsibility. It has been given additional status by its designation as the national center to combat money laundering. Also, the duties and responsibilities for the FIU have been clarified. The law also establishes a legal basis for increased cooperation between the FIU and the General Prosecutor's Office, while creating an oversight mechanism to ensure that the FIU fulfills, but does not exceed, its responsibilities and authority. Previously, coordination against money laundering and terrorist financing among agencies was sporadic. The new law establishes two levels of coordination: on the policy level, an inter-

ministerial group headed by Albania's Prime Minister and including the participation of different ministers, the Central Bank Governor, and the General Prosecutor. On the technical level, a group of experts was established.

The government bodies responsible for investigating financial crimes are the Ministry of Interior (through its Organized Crime and Witness Protection Departments), the General Prosecutor's Office and the State Intelligence Service. Money laundering and terrorist financing are relatively new issues for GOA institutions, and responsible agencies are neither adequately staffed nor fully trained to handle money laundering and terrorist financing issues.

There have been seven prosecutions initiated under the new Law No. 9084. In the two years preceding that law, there were seven prosecutions brought under the old law. Of these fourteen prosecutions, ten are pending in the courts and four have yet to be brought to trial. Given the high number of drug-trafficking and fraud-related cases in Albania, the number of money laundering prosecutions is still relatively low. This is largely due to the fact that the Albanian police force still does not have a central database and investigators lack much needed training in modern financial investigation techniques. The Prosecutor's Office also lacks well-trained prosecutors to efficiently manage cases. There have been no arrests for money laundering or terrorist financing since January 2005.

Through Law No. 9084, the Code of Criminal Procedure vastly improves the Albanian confiscation regime. Prior to 2004, Albanian law did not allow for asset forfeiture without a court decision. In 2004, Albania passed legislation that made the freezing and seizure of assets much easier. First, Albania passed a comprehensive anti-Mafia law, Law No. 9284, which contains strong civil asset seizure and forfeiture provisions, subjecting the assets of suspected persons and their families and close associates to seizure. The law also places the burden to prove a legitimate source of funding for seized assets on the defendant.

Law No. 9084 criminalizes the financing of terrorism, mandating strong penalties for any actions or organizations linked with terrorism. Until 2004, the GOA used its anti-money laundering law to freeze the assets of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list. In 2004, Law No. 9258, "On Measures Against Terrorist Financing," was enacted, permitting the GOA to administratively seize assets of any terrorist designated pursuant to Security Council resolutions, as well as pursuant to certain bilateral or multilateral requests. The Ministry of Finance has already implemented this law. In addition to one freeze obtained in 2004, the GOA has frozen the assets of seven additional persons or entities in 2005.

The Ministry of Finance is the main entity responsible for issuing freezing orders, while the FIU is responsible for tracing and seizing assets. In the case of individuals or entities whose names appear on the UNSCR 1267 consolidated list, the freezing orders remain in force as long as their names remain on the list. In the case of individuals under investigation or prosecution for money laundering, properties remain frozen until a court decision to the contrary is issued (such investigative freezes may not exceed three years). If a person is found guilty, his assets are confiscated and all the proceeds transferred to the state budget. The Agency for the Administration of Sequestered and Confiscated Assets (AASCA) was established in June 2005, following a Council of Ministers decision. After a difficult start, the GOA staffed the AASCA in early December 2005.

In the past four years, the GOA has seized $4.72 million in liquid criminal and terrorist assets ($3.14 million for terrorism financing and $1.58 million for money laundering) and about $5 million in real estate ($2.3 million in 2005). Some estimates place these figures at even higher values. In 2005, the previous freezing orders were converted under the new law against terrorism financiers. In total, there have been eight freeze orders issued, involving 56 bank accounts frozen in six different commercial banks. Fifty-four of these are related to terrorist financing. Each of the eight freeze orders issued by the Ministry of Finance in relation to persons involved in terrorism financing has been referred to the Prosecutor's Office for further investigation.

Although the GOA has not passed specific legislation addressing alternative remittance systems or charitable organizations, officials state that such informal transactions are covered under recent laws. Additionally, although the GOA does not normally monitor the use of funds by charitable organizations, the Ministry of Finance has explored additional legislation that would include such oversight. Starting from 2006, charitable organizations have to present their books to the tax office. The GOA has aggressively acted against charities that are suspected of wrongdoing, resulting in the removal of three of them from the country.

Contraband smuggling generates funds that are easily laundered in Albania due to highly unregulated transaction overview, lax control in almost all institutions dealing with immovable properties, and corruption in the State Administration. By contrast, the formal banking sector is highly regulated and is continuously under the scrutiny of the Central Bank.

Albanian legislation regarding cash couriers is not yet complete. Law No. 8610 sets the maximum amount of money that individuals (both Albanian and foreign) may possess on crossing borders. Amounts in excess of $10,000 require formal declaration. Declaration forms are available at border crossing points. There have been cases of individuals sentenced for illegal transfer of money based on information from foreign FIUs. The FIU shares cash smuggling reports with its counterparts in Turkey, Bulgaria and Macedonia.

The Albanian FIU became a member of the Egmont Group in July 2003, and continues to enlarge its cooperation with regional counterparts. The FIU has the ability to enter into bilateral or multilateral information sharing agreements on its own authority and has signed MOUs with 23 countries. The FIU is also participates in personnel exchanges with regional counterparts for training purposes and has also agreed to fight corruption jointly with Italy.

Albania is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime, and became a party to the UN International Convention for the Suppression of the Financing of Terrorism on April 10, 2002. On August 21, 2002, Albania ratified the UN Convention against Transnational Organized Crime. Albania is a party to the 1988 UN Drug Convention and in December 2003 signed the UN Convention against Corruption. Albania is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and participates in the Southeastern Europe Cooperative Initiative (SECI).

The Government of Albania has taken important steps to enhance its anti-money laundering and counterterrorist financing regime; however, additional improvements can still be made. Albania should incorporate into its anti-money laundering legislation specific provisions regarding corporate criminal liability, customer identification procedures, and the adequate oversight of money remitters and charities. Albania should also amend its laws to allow authorities to obtain an indictment for money laundering without a prior conviction for a predicate offense. A central police database should be created in order to assist law enforcement in the investigation of financial crimes.

Algeria

Algeria is not a regional financial center or an offshore financial center. The extent of money laundering through formal financial institutions is thought to be minimal due to stringent exchange control regulations and an antiquated banking sector. The partial convertibility of the Algerian dinar enables the Bank of Algeria (Algeria's Central Bank) to monitor all international financial operations carried out by public and private banking institutions.

Algeria first criminalized terrorist financing through the adoption of Ordinance 95.11 on February 24, 1994, making the financing of terrorism punishable by five to ten years of imprisonment. On February 5, 2005, Algeria enacted public law 05.01, entitled "The Prevention and Fight Against Money

Laundering and Financing of Terrorism." The law aims to strengthen the powers of the Cellule du Traitement du Renseignement Financier (CTRF), an independent financial intelligence unit (FIU) within the Ministry of Finance (MOF) created in 2002. This law seeks to bring Algerian law into conformity with international standards and conventions. It offers guidance for the prevention and detection of money laundering and terrorist financing, institutional and judicial cooperation, and penal provisions.

Algerian financial institutions, as well as Algerian customs and tax administration agents, are required to report any activities they suspect of being linked to criminal activity, money laundering, or terrorist financing to CTRF and comply with subsequent CTRF inquiries. They are obligated to verify the identity of their customers or their registered agents before opening an account; they must furthermore record the origin and destination of funds they deem suspicious. In addition, these institutions must maintain confidential reports of suspicious transactions and customer records for at least five years after the date of the last transaction or the closing of an account.

The new legislation extends money laundering controls to specific, non-bank financial professions such as lawyers, accountants, stockbrokers, insurance agents, pension managers, and dealers of precious metals and antiquities. Provided information is shared with the CTRF in good faith, the law offers immunity from administrative or civil penalties for individuals who cooperate with money laundering and terrorist finance investigations. Under the law, assets may be frozen for up to 72 hours on the basis of suspicious activity; such freezes can only be extended with judicial authorization. Financial penalties for non-compliance range from 50,000 to 5 million Algerian dinars.

The law also provides significant authority to the Algerian Banking Commission, the independent body established under authority of the Bank of Algeria to supervise banks and financial institutions, to inform the CTRF of suspicious or complex transactions. The law furthermore gives the Algerian Banking Commission, CTRF, and the Algerian judiciary wide latitude to exchange information with their foreign government counterparts in the course of money laundering and terrorist finance investigations, provided confidentiality for suspected entities is insured. A clause excludes the sharing of information with foreign governments in the event legal proceedings are already underway in Algeria against the suspected entity, or if the information is deemed too sensitive for national security reasons.

On November 14, 2005, the Government of Algeria issued Executive Decree 05-442, establishing a ceiling for cash transactions conducted in Algeria. Effective September 1, 2006, any payments in excess of 50,000 Algerian dinars must be made by check, wire transfer, payment card, bill of exchange, promissory note, or other official bank payment. While non-residents are exempt from this requirement, they must (like all travelers to and from the country) report their foreign currency to the Algerian Customs Authority.

The Ministry of Interior is charged with registering foreign and domestic non-governmental organizations in Algeria, although some probably operate beneath its notice. While the Ministry of Religious Affairs legally controls the collection of funds at mosques for charitable purposes, some of these funds probably escape the notice of government monitoring efforts.

In November 2004, Algeria became a member of the Middle East and North Africa Financial Action Task Force (MENA FATF). Algeria is a party to the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the 1988 UN Drug Convention. In addition, Algeria is a signatory to various UN, Arab, and African conventions against terrorism, trafficking in persons, and organized crime. It has also established an interagency council to oversee money laundering and terrorist financing investigations and form a commission that will evaluate all pending cases. The Ministry of Justice is expected to create a pool of judges trained in financial matters.

Over the last two years, Algeria has taken significant steps to enhance its statutory regime against anti-money laundering and terrorist financing. It must now move forward with implementation of those laws, including the coming into force of the law limiting the size of cash transactions.

Angola

Angola is not a regional or offshore financial center and has not prosecuted any known cases of money laundering. The laundering of funds derived from continuous and widespread high-level corruption is a concern, as is the use of diamonds as a vehicle for money laundering. However, the Government of Angola (GOA) has taken steps to guard against money laundering in the diamond industry by participating in the "Kimberley Process," an international certification scheme designed to halt trade in "conflict" diamonds in countries such as Angola. Angola has implemented a control system in accordance with the Kimberley Process. However, through the process of "mixing parcels" of licit and illicit diamonds, the Kimberly certification process can be compromised. Angola's long and porous borders further facilitate smuggling and the laundering of diamonds.

Angola currently has no comprehensive laws, regulations, or other procedures to detect money laundering and financial crimes, although some related crimes are addressed through other provisions of the criminal code. Reportedly, additional laws are in draft form. Legislation governing foreign exchange controls allows the Central Bank's Supervision Division, the governmental entity charged with money laundering issues, to exercise some authority against illicit banking activities. The Central Bank of Angola has the authority to freeze assets, but Angola does not presently have an effective system for identifying, tracing, or seizing assets. Instead, such crimes are addressed through other provisions of the criminal code. For example, Angola's counternarcotics laws criminalize money laundering related to narcotics trafficking. One of three draft laws to reform the banking sector specifically targets money laundering. The money laundering bill, which has not yet been approved by the Angolan Parliament, was drafted with the assistance of the World Bank. The GOA expects the money laundering law to be promulgated in 2006.

The high cash flow in Angola makes its financial system a potentially attractive site for money laundering. Because of a lack of a domestic interbank dollar clearing system, even dollar transfers between domestic Angolan banks are logged as "international" transfers, thus creating an incentive to settle transfers in cash. The local banking system imports approximately $200-300 million in net cash per month, largely in dollars, without a corresponding cash outflow. Reportedly, local bank representatives have noted that clients have walked into banks with up to $2 million in a briefcase to make a deposit. These massive cash flows occur in a banking system ill equipped to detect and report suspicious activity. The Central Bank has no workable data management system and only rudimentary analytic capability. It cannot develop suspicious transaction reports (STRs), much less analyze them and search for patterns.

Angola is party to the 1988 UN Drug Convention. Angola has signed but not yet ratified the UN Convention against Transnational Organized Crime. Angola has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Angola should pass its pending legislation and criminalize money laundering (beyond drug offenses) and terrorist financing. As part of the legislation, the GOA should establish a system of financial transparency reporting requirements. The GOA should then move quickly to implement the legislation and bolster the capacity of law enforcement to better investigate financial crimes. The GOA should become a party to both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. The GOA should increase efforts to combat official corruption.

Antigua and Barbuda

Antigua and Barbuda has comprehensive legislation in place to regulate its financial sector, but remains susceptible to money laundering because of its offshore financial sectors and Internet gaming industry. Money laundering in the region is related to both narcotics and fraud schemes, as well as to other crimes, but money laundering appears to occur more often in the offshore sector than in the domestic financial sector.

The International Business Corporations Act of 1982 as amended (IBCA) is the governing legal framework for offshore businesses in Antigua and Barbuda. Antigua and Barbuda has 16 licensed offshore banks in operation, one offshore trust, one offshore insurance company, and 8,000 offshore companies. Bearer shares are not permitted. The license application requires disclosure of the names and addresses of directors (who must be natural persons), the activities the corporation intends to conduct, the names of shareholders, and number of shares they will hold. Registered agents or service providers are required by law to know the names of beneficial owners. Failure to provide information or give false information is punishable by a fine of $50,000. All licensed institutions are required to have a physical presence, which means presence of at least a fulltime senior officer and availability of all files and records. Shell companies are not permitted.

In 2002, the IBCA was amended to create the Financial Services Regulatory Commission (FSRC), which replaced the previous entity, the International Financial Sector Regulatory Authority. The FSRC is responsible for the regulation and supervision of all institutions licensed under the act to include offshore banking and all aspects of offshore gaming. The FSRC is autonomous and is financed by the revenue generated from registration fees and licensing fees of IBCs. The FSRC is supervised by a four-member Board comprised of public officials and is presently chaired by the Solicitor General. Responsibilities of the FSRC include issuing licenses for international business corporations (IBCs) and maintaining the register of all corporations. The FSRC conducts examinations and on-site and off-site reviews of the country's offshore financial institutions, and of some domestic financial entities, such as insurance companies and trusts. Proposed 2005 amendments to the IBCA seek to authorize the FSRC to decline to incorporate a corporation if it has reason to suspect that the corporation may be used for criminal purposes.

In September 2002, the Government of Antigua and Barbuda (GOAB) issued anti-money laundering guidelines for financial institutions, requiring banks to establish the true identities of account holders and to verify the nature of an account holder's business and beneficiaries. The GOAB has not chosen to initiate a unified regulatory structure or uniform supervisory practices for its domestic and offshore banking sectors. Currently, the Eastern Caribbean Central Bank (ECCB) supervises Antigua and Barbuda's domestic banking sector. The amended Banking Act 2004 enables the ECCB to share information directly with foreign regulators if a memorandum of understanding is established.

The Money Laundering (Prevention) Act (MLPA) of 1996 as amended is the operative legislation addressing money laundering. The Office of National Drug Control and Money Laundering Policy (ONDCP), which is the financial intelligence unit (FIU), directs the GOAB's anti-money laundering efforts in coordination with the FSRC. The ONDCP is a department in the Prime Minister's office, and has primary responsibility for the enforcement of the MLPA. The ONDCP Act of 2003 establishes the FIU as an independent organization and the Director of ONDCP as the supervisory authority under the MLPA. Additionally, the ONDCP Act of 2003 authorizes the Director to appoint officers to investigate narcotics trafficking, fraud, money laundering, and terrorist financing offenses. Auditors of financial institutions review their compliance program and submit a report to the ONDCP for analysis and recommendations. Memoranda of understanding have been drafted to cover all aspects of the ONDCP's relationship with the Royal Antigua and Barbuda Police Force, Customs, Immigration, and the Antigua and Barbuda Defense Force. Through November 2005, the ONDCP received 21 suspicious activity reports of which 20 were investigated. A training program and information kit on

anti-money laundering for magistrates and other judicial officers was developed, and training was conducted in 2004. In 2005, a number of GOAB civilian and law enforcement officials received anti-money laundering training.

The 2000 and 2001 amendments to the MLPA broadened its definition of supervised financial institutions to include all types of gambling entities and to set financial limits above which customer identification and source of funds information are required. Antigua and Barbuda has five domestic casinos, which are required to incorporate as domestic corporations. Internet gaming operations are required to incorporate as IBCs; as such they are required to have physical presence. Internet gaming sites are considered to have a physical presence when the primary servers and the key person are resident in Antigua and Barbuda. Official sources indicate there are 33 Internet gambling entities, with 14 operating licenses granted in 2005. The GOAB expects to grant 10 new licenses for online gambling companies in 2006. The GOAB receives approximately $2.8 million per year from license fees and other charges related to the internet gaming industry. Casinos and sports book-wagering operations in Antigua and Barbuda's Free Trade Zone are supervised by the ONDCP and the Directorate of Offshore Gaming (DOG), housed in the FSRC. The DOG has 13 employees. Antigua and Barbuda has five domestic casinos, which are required to incorporate as domestic corporations. In 2001, the GOAB adopted regulations for the licensing of interactive gaming and wagering, in order to address possible money laundering through client accounts of Internet gambling operations. Furthermore, the FSRC and DOG have issued Internet gaming technical standards and guidelines. Internet gaming companies are required to enforce know-your-customer verification procedures and maintain records relating to all gaming and financial transactions of each customer for six years. The FSRC recently mandated Internet gaming sites must submit quarterly financial statements in addition to annual statements. Suspicious activity reports from domestic and offshore gaming entities are sent to the ONDCP and FSRC.

In October 2001, the GOAB enacted the Prevention of Terrorism Act, which empowers the ONDCP to nominate any entity as a "terrorist entity" and to seize and forfeit terrorist funds. The law covers any finances in any way related to terrorism. The proposed Prevention of Terrorism Act 2005 requires financial institutions to report possession of assets of persons declared by the Attorney General to be a terrorist. It is also illegal for a financial organization to deal with property belonging to a terrorist or a terrorist organization. Under the Act, the Attorney General may revoke or deny the registration of a charity or non-profit organization if it is believed funds from the organization are being used for financing terrorism. The GOAB circulates lists of terrorists and terrorist entities to all financial institutions in Antigua and Barbuda. No known evidence of terrorist financing has been discovered in Antigua and Barbuda to date. The GOAB does not believe indigenous alternative remittance systems exist in country.

Amendments to the MLPA in 2000, 2001, and 2002 enhanced international cooperation, strengthened asset forfeiture provisions, and created civil forfeiture powers. In 2005, two arrests were made on money laundering charges. Despite the comprehensive nature of the law, Antigua and Barbuda has yet to prosecute a money laundering case on its own.

The GOAB continues its bilateral and multilateral cooperation in various criminal and civil investigations and prosecutions. In 1999, a Mutual Legal Assistance Treaty and an Extradition Treaty with the United States entered into force. An extradition request related to a fraud and money laundering investigation remains pending under the treaty. The GOAB signed a Tax Information Exchange Agreement with the United States in December 2001 that allows the exchange of tax information between the two nations. Because of such assistance, the GOAB has benefited through an asset sharing agreement with Canada and has received asset sharing revenues from the United States. The GOAB is currently working on asset forfeiture agreements with other jurisdictions. Regardless of its own civil forfeiture laws, currently the GOAB can only provide forfeiture assistance in criminal forfeiture cases. In the past few years, the GOAB has frozen approximately $6 million in Antigua and

Barbuda financial institutions as a result of U.S. requests and has repatriated approximately $4 million. The GOAB has frozen, on its own initiative, over $90 million that it believed to be connected to money laundering cases still pending in the United States and other countries. In 2005, the GOAB cooperated extensively with U.S. law enforcement in an investigation that resulted in a seizure of $1,022,000.

Antigua and Barbuda is a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD), and the Caribbean Financial Action Task Force (CFATF), of which it chaired in 2004. The GOAB underwent its second round CFATF Mutual Evaluation in October 2002. The CFATF found that Antigua and Barbuda's anti-money laundering framework was consistent with international standards and is being enforced. Antigua and Barbuda is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. The ONDCP joined the Egmont Group in June 2003.

The Government of Antigua and Barbuda should continue its international cooperation, and rigorously implement and enforce all provisions of its anti-money laundering legislation. Antigua and Barbuda should vigorously enforce its anti-money laundering laws by actively prosecuting money laundering and asset forfeiture cases.

Argentina

Argentina is neither an important regional financial center nor an offshore financial center. Money laundering related to narcotics trafficking, corruption, contraband, and tax evasion is believed to occur throughout the financial system, in spite of the efforts of the Government of Argentina (GOA) to stop it. The financial sector's slow recovery from the 2001-02 financial crisis and post-crisis capital controls may have reduced the incidence of money laundering through the banking system. However, transactions conducted through non-bank sectors and professions, such as the insurance industry, financial advisors, accountants, notaries, trusts, and companies, real or shell, remain viable mechanisms to launder illicit funds. Tax evasion is the predicate crime in roughly two thirds of all Argentine money laundering investigations. Argentina has a long history of capital flight and tax evasion, and Argentines hold billions of dollars offshore, much of it legitimately earned money that was never taxed.

The GOA took several important steps to further combat money laundering and terrorist financing in 2005, including the ratification of the UN International Convention for the Suppression of the Financing of Terrorism and the Inter-American Convention Against Terrorism, and regulatory changes to improve its anti-money laundering and counterterrorist financing systems. Over 100 cases of suspected money laundering have now been passed to prosecutors by the Unidad de Informacion Financiera (UIF), Argentina's financial intelligence unit (FIU). The Central Bank of Argentina (BCRA) established a specialized bank examination unit devoted specifically to money laundering, and expanded its requirements for financial institutions to check transactions against the terrorism lists of the United States, European Union, Great Britain, and Canada, in addition to the UN 1267 Sanctions Committee consolidated list. The two chambers of Congress passed different versions of a law that would lift all bank secrecy and some fiscal secrecy provisions that have prevented the UIF from obtaining information needed for its investigations.

Argentina's primary anti-money laundering legislation is Law 25.246 of May 2000. Law 25.246 expands the predicate offenses for money laundering to include all crimes listed in the Penal Code, sets a stricter regulatory framework for the financial sectors, and creates an FIU, the Unidad de Informacion Financiera (UIF), under the Ministry of Justice and Human Rights. This law lay down requirements for customer identification, record keeping, and reporting of suspicious transactions by all financial entities and businesses supervised by the Central Bank, the Securities Exchange

Commission (Comisión Nacional de Valores or CNV), and the Superintendence of Insurance (Superintendencia de Seguros de la Nación or SSN). The law forbids the institutions to notify their clients when filing suspicious financial transactions reports, and provides a safe harbor from liability for reporting such transactions. Reports that are deemed by the UIF to warrant further investigation are forwarded to the public prosecutors' office. As of November 2005, the UIF had received 1416 reports of suspicious or unusual activities, forwarded 102 suspected cases of money laundering to prosecutors for review, and assisted prosecutors with 79 cases.

The UIF, which began operating in June 2002, has issued resolutions widening the range of institutions and businesses required to report of suspicious or unusual transactions to the UIF beyond those identified in Law 25.246. Obligated entities include the tax authority (Administracion Federal de Ingresos Publicos or AFIP), banks, currency exchange houses, casinos, securities dealers, dealers in art, antiques, and precious metals, insurance companies, postal money transmitters, accountants, and notaries public. The resolutions issued by the UIF also provide guidelines for identifying suspicious or unusual transactions. In 2005, the UIF eliminated a previous resolution requiring that obligated entities only report suspicious or unusual transactions that exceeded 50,000 pesos (approximately $16,400); UIF Resolution 4/2005 now requires entities to report all suspicious or unusual transactions regardless of their amount. Suspicious or unusual transactions are now reported directly to the UIF; prior to 2004, all suspicious transactions below a 500,000 peso threshold were first reported to the appropriate supervisory body for pre-analysis due to budget constraints at the UIF. Obligated entities are required to maintain a database of all information related to client transactions, including suspicious or unusual transaction reports, for at least five years and must respond to requests from the UIF for further information within 48 hours.

The Central Bank requires by resolution that all banks maintain a database of all transactions exceeding 10,000 Argentine pesos (approximately $3,350). This data is submitted on a periodic basis to the BCRA. Some banks make this information available to the UIF on request; others do not, citing financial secrecy laws. Law 25.246 requires banks to make available to the UIF upon request records of transactions involving the transfer of funds (outgoing or incoming), cash deposits, or currency exchanges that are equal to or greater than 10,000 pesos (approximately $3,300).

The UIF further receives copies of the declarations to be made by all individuals (foreigners or Argentine citizens) entering or departing Argentina with over $10,000 in currency or monetary instruments. These declarations are required by Resolutions 1172/2001 and 1176/2001 issued by the Argentine Customs Service in December 2001. A law (Law 22.415/25.821) that would have provided for the immediate fine of 25 percent of the undeclared amount, and for the seizure and forfeiture of the remaining undeclared currency and/or monetary instruments, passed the Argentine Congress in 2003, but was vetoed by the President due to alleged conflicts with Argentina's commitments to MERCOSUR (Common Market of the Southern Cone).

Argentina's Narcotics Law of 1989 authorizes the seizure of assets and profits, and provides that these or the proceeds of sales will be used in the fight against illegal narcotics trafficking. Law 25.246 provided that proceeds of assets forfeited under this law can also be used to fund the UIF.

The Financial Action Task Force (FATF) conducted a mutual evaluation of Argentina in October 2003. The mutual evaluation report was accepted at the FATF plenary in June 2004 and at the plenary meetings of the Financial Action Task Force for South America (GAFISUD) in July 2004. While the evaluation of Argentina showed the UIF to be functioning satisfactorily, it identified some weaknesses in Argentina's current anti-money laundering legislation, as well as the lack of terrorist financing legislation or a national coordination strategy. There have been only two money laundering convictions in Argentina since money laundering was first criminalized in 1989, and none since the passage of Law 25.246 in 2000. Under a strict interpretation of the law, a prior conviction for the predicate offense is required in order to obtain a conviction for money laundering.

Although Law 25.246 of 2000 expands the number of predicate offenses for money laundering beyond narcotics-related offenses and created the UIF, it limits the UIF's role to investigating only money laundering arising from six specific crimes. The law also defines money laundering as an aggravation after the fact of the underlying crime. A person who commits a crime cannot be prosecuted for laundering money obtained from the crime; only someone who aids the criminal after the fact in hiding the origins of the money can be guilty of money laundering. Another impediment to Argentina's anti-money laundering regime is that only transactions (or a series of related transactions) exceeding 50,000 pesos can constitute money laundering; transactions below 50,000 pesos can constitute only concealment, a lesser offense.

The strict interpretation of the secrecy provisions of Law 25.246 also inhibits the UIF's ability to request additional information from obligated entities. Although Law 25.246 provides that the UIF is able to request information from obligated entities if this information is deemed useful to the UIF in carrying out its functions, it fails to resolve conflicts with strict "banking, fiscal, and professional" confidentiality provisions in other laws that require court orders to request information not directly related to a suspicious transaction report. Several government authorities, such as AFIP (the tax authority, which is responsible for overseeing the customs agency and dealing with tax fraud and other economic crimes), reportedly have been uncooperative in responding to the UIF's requests for assistance, citing these confidentiality provisions. An exception is the Central Bank, which generally cooperates with the UIF by providing regulatory information needed for money laundering investigations. As of November 2005, the UIF had requested additional information from the AFIP in 419 cases and from the Central Bank in 310 cases.

Legislation that would lift all banking secrecy restrictions and partially lift fiscal secrecy restrictions passed both houses of the Congress in 2005—but in different forms. The two bills need to be reconciled and the legislation must be signed by the President before becoming law. The passage of this law would lift or reduce many restrictions that have prevented the UIF from obtaining information needed for money laundering investigations.

Terrorism and terrorist acts are not specifically criminalized under Argentine law. Because these acts are not autonomous offenses, terrorist financing is not a predicate offense for money laundering. In 2005, Argentina ratified the UN International Convention for the Suppression of the Financing of Terrorism and the Inter-American Convention Against Terrorism, but it has not yet passed domestic legislation. Several bills have been introduced in the Congress to implement the provisions of those treaties under Argentine law, but there have not yet been votes on any of these draft laws and the GOA has not yet indicated which, if any, of these bills it will support. In an attempt to close this gap, the Central Bank issued Circular 4863 in 2005 that requires banks to report any detected instances of the financing of terrorism. However, bankers have complained that the regulation is not backed by any legal definition of what constitutes terrorist financing in Argentina, and that the absence of domestic legislation means that they are not protected from lawsuits by clients if they report suspected cases of terrorist financing.

The Central Bank of Argentina issued Circular B-6986 in 2004, instructing financial institutions to identify and freeze the funds and financial assets of the individuals and entities listed on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. It modified this circular with Resolution 319 in October 2005, which expands Circular B-6986 to require financial institutions to check transactions against the terrorist lists of the United Nations, United States, European Union, Great Britain, and Canada. No assets have been identified or frozen to date.

Working with the United States Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Argentina began the process of establishing a Trade Transparency Unit (TTU) that will examine anomalies in trade data that could be indicative of customs fraud and trade-based money laundering. This is also a positive step towards complying with FATF Special

Recommendation VI on Terrorist Financing via alternative remittance systems. Trade- based systems such as hawala often use fraudulent trade documents and over and under invoicing schemes to provide counter valuation in value transfer and settling accounts.

The GOA remains active in multilateral counternarcotics and international anti-money laundering organizations. It is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering, the FATF, and GAFISUD. The GOA 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, and the UN Convention against Transnational Organized Crime, and has signed but not yet ratified the UN Convention Against Corruption. Argentina has been a member of the Egmont Group since July 2003 and participates in the "3 Plus 1" Counter-Terrorism Dialogue between the United States and the Triborder Area countries (Argentina, Brazil and Paraguay). The UIF has signed memoranda of understanding regarding the exchange of information with a number of financial intelligence units, including Australia, Belgium, Bolivia, Brazil, Chile, Colombia, El Salvador, Guatemala, Honduras, Panama, Paraguay, Peru, Romania, Spain, and Venezuela. The GOA and the USG have a Mutual Legal Assistance Treaty that entered into force in 1993, and an extradition treaty that entered into force in 2000. With strengthened mechanisms available under the Law 25.246, the ratification of the UN International Convention for the Suppression of the Financing of Terrorism, and increased reporting requirements issued by the UIF, Argentina seems poised to prevent and combat money laundering effectively. However, several legislative and regulatory changes would significantly improve the anti-money laundering/counterterrorism finance regime in Argentina, particularly the passage of domestic legislation that criminalizes the financing of terrorism. To comply with the latest FATF recommendation on the regulation of bulk money transactions, Argentina also will need to review the legislation vetoed in 2003 to find a way to regulate such transactions consistent with its MERCOSUR obligations.

To comport with international standards established by the Financial Action Task Force to which Argentina, as a member of the FATF, is committed to honor, the Government of Argentina needs to amend its anti-money laundering legislation to state that any person who commits a crime and then launders the illicit proceeds of that crime is prosecuted for money laundering. The final passage of pending legislation should reduce disputes over information sharing between the UIF, the financial sector, the Central Bank, the tax agency (AFIP), and other regulatory agencies. In doing so, the Government of Argentina will need to balance the concerns of the UIF and judicial authorities for quick and efficient access to such information in aid of legitimate investigations of suspected money laundering, and the need to stringently protect that information from disclosure or use for other purposes, which remains a major concern of the financial sector. Other issues need to be resolved for anti-money laundering efforts to succeed. The lack of coordination and cooperation between GOA agencies, and the lack of a national strategy on money laundering that would link and coordinate GOA resources devoted to intelligence and to counternarcotics and anti-financial crime efforts hinders the separate efforts of the different agencies. There are also needs for forceful sanctioning of officials and institutions that fail to comply with the reporting requirements of the law, the pursuit of a training program for all levels of the criminal justice system, and the provision of the necessary resources to the UIF to carry out its mission. Additionally, there is a need for increased public awareness of the problem of money laundering and its connection to narcotics, corruption, and terrorism.

Aruba

Aruba is an autonomous, largely self-governing Caribbean island under the sovereignty of the Kingdom of the Netherlands. Due to its geographic location and excellent infrastructure Aruba is both attractive and vulnerable to money launderers and narcotics trafficking. Aruba has four commercial and two offshore banks, one mortgage bank, two credit unions, an investment bank, a finance

company, 11 credit institutions, and 11 casinos. The island also has six registered money transmitters, two exempted U.S. money transmitters (Money Gram and Western Union), eight life insurance companies, 14 general insurance companies, two captive insurance companies, and 11 company pension funds. As of November 30, 2004, there were 5,526 limited liability companies (NVs), of which 493 were offshore limited liability companies or offshore NVs. In addition, there are approximately 4,014 offshore tax-exempt companies referred to as Aruba Exempt Companies (AECs), which mainly serve as vehicles for tax minimization, corporate revenue routing, and asset protection and management.

The offshore NV and the AEC are the primary methods used for international tax planning in Aruba. The offshore NV pays a small percentage tax and is subject to more regulation than the AEC. The AEC is tax exempt as long as all business income arises outside of Aruba and as long as the company is not controlled directly or indirectly by Aruban residents. AECs cannot participate in the economy of Aruba; therefore, no transactions with onshore companies or residents are allowed. AECs are also exempt from several obligations including currency restrictions, filing of annual financial statements, and from disclosure of financial condition and beneficial owners. AECs pay an annual registration fee of approximately $280, and must have minimum authorized capital of approximately $6,000. Both offshore NVs and AECs can issue bearer shares. A local managing director is required for offshore NVs. AECs must have a local registered agent, which must be a trust company.

In 2001 the Government of Aruba (GOA) made a commitment to the Organization for Economic Cooperation and Development (OECD), in connection with the Harmful Tax Practices initiative, to modernize its fiscal legislation in line with OECD standards. In 2003 the GOA introduced a New Fiscal Regime (NFR) that contains a dividend tax and imputation credits. As a result of the introduction of the NFR, Aruba no longer has an offshore regime (grandfathered until 2007/2008). As of July 1, 2003, the incorporation of low tax offshore NVs was halted. The NFR contains a specific exemption for the AEC; nevertheless, commitments have been made to the OECD that the AEC will be amended before the end of 2005. The amendments will for the major part relate to transparency and the requirement of a yearly audited financial statement.

Aruba currently has three areas designated as free zones: Oranjestad Free Zone, Bushiri Free Zone, and the Barcadera Free Zone. The free zones of Aruba are managed and operated by Free Zone Aruba (FZA) NV, a government limited liability company. Originally, only companies involved in trade or light industrial activities (which include the servicing, repairing and maintenance of goods with a foreign destination) could be licensed to operate within the Free Zone. However, the State Ordinance Free Zones 2000 extended licensing to service-oriented companies (excluding financial services). Before admittance to operate in the free zone, companies must submit a business plan; submit personal data of managing directors, shareholders, and ultimate beneficiaries; and establish a limited liability company founded under Aruban law that is exclusively intended for free zone operations. Aruba took the initiative in the Caribbean Financial Action Task Force (CFATF) to develop regional standards for free zones, in an effort to control trade-based money laundering. The guidelines were adopted at the CFATF Ministerial Council in October 2001. Free Zone Aruba NV is continuing the process of implementing and auditing the standards that have been developed.

The Central Bank of Aruba is the supervisory/regulatory authority for credit institutions, insurance companies, company pension funds, and money transfer companies. The State Ordinance on the Supervision of Insurance Business (SOSIB) and the Implementation Ordinance on SOSIB brought insurance companies under the supervision of the Central Bank and require those established after July 1, 2001, to obtain a license from the Central Bank. The State Ordinance on the Supervision of Money-Transfer Companies became effective August 12, 2003, and places money transfer companies under the supervision of the Central Bank. Quarterly reporting requirements became effective in 2004. A State Ordinance on the supervision of trust companies, which will designate the Central Bank as the supervisory authority, is being drafted.

The anti-money laundering legislation in Aruba extends to all crimes, including tax offenses, in which the underlying offense must have a potential penalty of more than four years' imprisonment. All financial and non-financial institutions are obligated to report suspicious transactions to Aruba's financial intelligence unit, the Meldpunt Ongebruikelijke Transacties (MOT). On July 1, 2001, a State Ordinance was issued that extends reporting and identification requirements to casinos and insurance companies. The MOT is authorized to inspect all banks, money remitters, casinos, insurance companies, and brokers for compliance with the unusual reporting requirements and the identification requirements for financial transactions.

The MOT is staffed by 12 employees. In 2004, the MOT received 7,460 suspicious transaction reports (STRs) with 87 investigations conducted and 27 cases transferred to the appropriate authorities. For 2005, the MOT received 6,956 STRs with 60 investigations conducted, 27 cases transferred, and 10 cases still to be worked. In June 2000, Aruba enacted a State Ordinance making it a legal requirement to report the importation and exportation via harbor and airport of currency in excess of 20,000 Aruban guilders (approximately $11,000) to the Customs Department. The law also applies to express courier mail services. Reports generated are forwarded to the MOT to review. In 2005 approximately 872 reports were submitted to the MOT.

The MOT shares information with other national government departments. On April 2, 2003, the MOT signed an information exchange agreement with the Aruba Tax Office, which is in effect and being implemented. Recently, the MOT and the Central Bank signed an information exchange memorandum of understanding (MOU) that is effective January 2006. The MOT is not linked electronically to the police or prosecutor's office. The MOT is a member of the Egmont Group, and is authorized by law to share information with members of the Egmont Group through a memorandum of understanding. The United States and the MOT signed such an MOU in November 2005.

Aruba signed a multilateral directive with Colombia, Panama, the United States, and Venezuela to establish an international working group to fight money laundering that occurs through the Black Market Peso Exchange (BMPE). The final set of recommendations on the BMPE was signed on March 14, 2002. The working group developed policy options and recommendations to enforce actions that will prevent, detect, and prosecute money laundering through the BMPE. The GOA is in the process of implementing the recommendations.

Aruba participates in the FATF through the Netherlands, and therefore, participates in the FATF mutual evaluation program. The GOA has a local FATF committee, comprised of officials from different departments of the Aruban Government that work together under the leadership of the MOT, to oversee the implementation of the FATF recommendations. The local FATF committee reviewed the GOA anti-money laundering legislation and proposed, in accordance with the nine FATF Special Recommendations on Terrorist Financing, amendments to existing legislation, and introduction of new laws. In 2004, the Penal Code of Aruba was modified to criminalize terrorism, the financing of terrorism, and related criminal acts. Aruba is in compliance with seven of the nine FATF Special Recommendations. Aruba will introduce the Sanctions Ordinance to become fully compliant with the Special Recommendations. The GOA and the Netherlands formed a separate committee in 2004 to ensure cooperation of agencies within the Kingdom of the Netherlands in the fight against cross-border organized crime and international terrorism.

Aruba is a member of CFATF and served as its Chairman in 2001. In 1999, the Netherlands extended application of the 1988 UN Drug Convention to Aruba. The Mutual Legal Assistance Treaty between the Netherlands and the United States applies to Aruba, though it is not applicable to requests for assistance relating to fiscal offenses addressed to Aruba. The Tax Information Exchange Agreement with the United States signed in November 2003 became effective in September 2004.

The Government of Aruba has shown a commitment to combating money laundering by establishing a solid anti-money laundering regime that is generally consistent with the recommendations of the

FATF and the CFATF. Aruba should immobilize bearer shares under its fiscal framework and should enact its long-pending ordinance addressing the supervision of trust companies.

Australia

Australia is one of the major centers for capital markets in the Asia-Pacific region. Annual turnover across Australia's over-the-counter and exchange-traded financial markets was AUD82 trillion (approximately $61.50 trillion) in 2005. Australia's total stock market capitalization is over $500 billion (approximately $375 billon), making it the ninth largest market in the world, and the second largest in the Asia-Pacific region behind Japan. Australia's foreign exchange market is ranked seventh in the world by turnover; with the U.S. dollar and the Australian dollar the fourth most actively traded currency pair globally. While narcotics offences provide a substantial source of proceeds of crime, the majority of illegal proceeds are derived from fraud-related offences. One Australian Government estimate suggested that the amount of money laundered in Australia ranges between AUD2-3 billion (approximately $1.5-$2,25 billion) per year.

The Government of Australia (GOA) has maintained a comprehensive system to detect, prevent, and prosecute money laundering. The major sources of illegal proceeds are fraud and drug trafficking. The last three years have seen a noticeable increase in activities investigated by Australian law enforcement agencies that relate directly to offenses committed overseas. Australia's system has evolved over time to address new money laundering and terrorist financing risks identified through continuous consultation between government agencies and the private sector.

In March 2005, the Financial Action Task Force (FATF) conducted its on-site Mutual Evaluation (FATFME) of Australia's anti-money laundering/counterterrorism financing (AML/CTF) system. Australia is one of the first member countries to be evaluated under FATF's revised recommendations. The FATF's findings from the mutual evaluation of Australia were published in October 2005 and Australia was found to be compliant or largely complaint with just over half of the FATF Recommendations. The FATFME noted that although Australia "has a comprehensive money laundering offense… the low number of prosecutions …indicates…that the regime is not being effectively implemented".

In response, the GOA has committed to reforming Australia's AML/CTF system to implement the revised FATF Forty plus Nine recommendations. The Attorney General's Department (AGD) is coordinating this process, which is expected to significantly reshape Australia's current AML/CTF regime in line with current international best practices. In December 2003, the Australian Government confirmed its intention to implement the revised FATF standards and an extensive process of consultation with industry has been underway since then.

Australia criminalized money laundering related to serious crimes with the enactment of the Proceeds of Crime Act 1987. This legislation also contained provisions to assist investigations and prosecution in the form of production orders, search warrants, and monitoring orders. It was superseded by two acts that came into force on January 1, 2003 (although proceedings that began prior to that date under the 1987 law will continue under that law). The Proceeds of Crime Act 2002 provides for civil forfeiture of proceeds of crime as well as for continuing and strengthening the existing conviction-based forfeiture scheme that was in the Proceeds of Crime Act 1987. The Proceeds of Crime Act 2002 also enables freezing and confiscation of property used in, intended to be used in, or derived from, terrorism offenses. It is intended to implement obligations under the UN International Convention for the Suppression of the Financing of Terrorism and resolutions of the UN Security Council relevant to the seizure of terrorism-related property. The Act also provides for forfeiture of literary proceeds where these have been derived by a person from commercial exploitation by the person of notoriety gained from committing a criminal offense.

The Proceeds of Crime (Consequential Amendments and Transitional Provisions) Act 2002 (POCA 2002), repealed the money laundering offenses that had previously been in the Proceeds of Crime Act 1987 and replaced them with updated offenses that have been inserted into the Criminal Code. The new offenses are graded according both to the level of knowledge required of the offender and the value of the property involved in the activity constituting the laundering. As a matter of policy all very serious offenses are now gradually being placed in the Criminal Code. POCA 2002 also enables the prosecutor to apply for the restraint and forfeiture of property from proceeds of crime. POCA 2002 further creates a national confiscated assets account from which, among other things, various law enforcement and crime prevention programs may be funded. Recovered proceeds can be transferred to other governments through equitable sharing arrangements. It also authorizes the seizure and forfeiture of property used in, intended to be used in, or derived from, terrorist offenses. It is intended to implement obligations relating to property that arise under the UN International Convention for the Suppression of the Financing of Terrorism.

Underneath the framework of offenses, the Financial Transaction Reports Act (FTR Act) of 1988 was enacted to combat tax evasion, money laundering, and serious crimes. The FTR Act requires banks and non-banking financial entities (collectively referred to as cash dealers) to verify the identities of all account holders and signatories to accounts, and to retain the identification record, or a copy of it, for seven years after the day on which the relevant account is closed. A cash dealer, or an officer, employee, or agent of a cash dealer, is protected against any action, suit, or proceeding in relation to the reporting process. The FTR Act also establishes reporting requirements for Australia's financial services sector. Required to be reported are: suspicious transactions, cash transactions in excess of Australian $10,000 (approximately $7,500), and all international funds transfers into or out of Australia, regardless of value. The FTR Act also obliges any person causing an international movement of currency of Australian $10,000 (or a foreign currency equivalent) or more, into or out of Australia, either in person, as a passenger, by post or courier to make a report of that transfer.

FTR Act reporting also applies to non-bank financial institutions such as money exchangers, money remitters, stockbrokers, casinos and other gambling institutions, bookmakers, insurance companies, insurance intermediaries, finance companies, finance intermediaries, trustees or managers of unit trusts; issuers, sellers, and redeemers of travelers checks, bullion sellers, and other financial services licensees. Solicitors (lawyers) also are required to report significant cash transactions. Accountants do not have any FTR Act obligations. However, they do have an obligation under a self-regulatory industry standard not to be involved in money laundering transactions.

The FTR Act established the Australian Transaction Reports Analysis Centre (AUSTRAC). Australia's financial intelligence unit (FIU). AUSTRAC collects, retains, compiles, analyzes, and disseminates FTR information. AUSTRAC is Australia's AML/CTF regulator, ensuring compliance with the FTR ACT.AUSTRAC also provides advice and assistance to revenue collection and law enforcement agencies, and issues guidelines to cash dealers in terms of their obligations under the FTR Act and regulations. As such, AUSTRAC plays a central role in Australia's AML system both domestically and internationally. Between 2004 and 2005, AUSTRAC's FTR information was used in 2,224 investigations. Of these, 578 matters identified FTR information as being very valuable to investigation outcomes. Results from the Australian Taxation Office shows that the FTR information contributed to more that AUD61.65 million (approximately $45 million) in Australian Taxation Office assessments during the year. By November 2005, AUSTRAC received a total of 12,575,531 financial transaction reports, with 99.5 percent of the reports submitted electronically through the EDDS Web system. AUSTRAC received 17,212 suspect transaction reports (SUSTRs), an increase of 49.9 percent from the precious year.

In 2005, there was a significant increase in the total number of financial transaction reports received by AUSTRAC. Significant cash transactions reports (SCTRs) account for 18 percent of the total number of FTRs reported to AUSTRAC each year and are reported by cash dealers and solicitors. In

2005, AUSTRAC received 2,288,373 SCTRs, an increase of 11.3 percent from the previous year. Cash dealers are required to report all international funds transfer instructions (IFTIs) to AUSTRAC. Cash deakers reported 10,243,774 IFTIs to AUSTRAC—a 17.9 percent increase from 2004. The remittances generated 1,229,592 IFTI reports—a 76 percent increase in number from the previous year. International currency transfer reports (ICTR) are primarily declared to the Australian Customs Service by individuals when they enter or depart from Australia. AUSTRAC received 26,172 ICTRs—a 2.3 percent increase from the previous year. In April 2005, the Minister for Justice and Customs launched AUSTRAC's AML eLearning application. This application has been well received by cash dealers as a tool in providing basic education on the process of money laundering, the financing of terrorism, and the role of AUSTRAC in identifying and assisting investigations of these crimes

AUSTRAC expanded its involvement in the fight against financial crimes by signing agreements for using AUSTRAC's financial transaction data with Centrelink (an Australian public assistance agency) and the Child Support Agency in an effort to reduce welfare fraud and related criminal conduct. The information available to Centrelink officers will relate specifically to significant cash transaction reports, international currency transfer reports, suspect transaction reports, and international funds transfer instructions.

APRA is the prudential supervisor of Australia's financial services sector. AUSTRAC regulates anti-money laundering/counterterrorist financing (AML/CTF) compliance. AUSTRAC's powers include criminal, but not administrative sanctions for non-compliance. AUSTRAC has conducted very few compliance audits in recent years and places a great deal of emphasis on educating and continuously engaging the private sector regarding the evolution of AML/CTF regime and the attendant reporting requirements. The FATFME noted that a comprehensive system for AML/CTF compliance for the entire financial sector needed to be established by the GOA, as does an administrative penalty regime for AML/CTF non-compliance.

In June 2002, Australia passed the Suppression of the Financing of Terrorism Act 2002 (SFT Act). The aim of the SFT Act is to restrict the financial resources available to support the activities of terrorist organizations. This legislation criminalizes terrorist financing and substantially increases the penalties that apply when a person uses or deals with suspected terrorist assets that are subject to freezing. The SFT Act enhances the collection and use of financial intelligence by requiring cash dealers to report suspected terrorist financing transactions to AUSTRAC, and relaxes restrictions on information sharing with relevant authorities regarding the aforementioned transactions. The SFT Act also addresses commitments Australia has made with regard to the UNSCR 1373 and is intended to implement the UN International Convention for the Suppression of the Financing of Terrorism. Under this Act three accounts related to an entity listed on the UNSCR 1267 Sanction Committee's consolidated list, the International Sikh Youth Federation, were frozen in September 2002. There have been no arrests or prosecutions under this legislation. The Security Legislation Amendment (Terrorism) Act 2002, also inserted new criminal offenses in the Criminal Code for receiving funds from, or making funds available to, a terrorist organization

The Anti-Terrorism Act (No.2) 2005 (AT Act) recently amended offenses related to the funding of a terrorist organization in the Criminal Code so that they also cover the collection of funds for or on behalf of a terrorist organization. The AT Act also inserted a new offense of financing a terrorist. The SFT Act amendments to the FTR Act were a significant milestone in the enhancement of AUSTRAC's international efforts. These amendments gave the Director of AUSTRAC the right to establish agreements with international counterparts to directly exchange intelligence, spontaneously and upon request. A review of the FTR Act is currently being undertaken to improve procedures, implement international best practices, and address further aspects of terrorist financing, including alternative remittance systems.

Investigations of money laundering reside with the Australian Federal Police (AFP) and Australian Crime Commission (Australia's only national multi- jurisdictional law enforcement agency). The AFP is the primary law enforcement agency for the investigation of money-laundering and terrorist-financing offences in Australia at the Commonwealth level and has both a dedicated Financial Crimes Unit and Financial Investigative Teams (FIT) consisting of 44 members with primary responsibility for asset identification/restraint and forfeiture under the POCA 2002. The Commonwealth Director of Public Prosecutions (CDPP) prosecutes offences against Commonwealth law and to recover proceeds of Commonwealth crime. The main cases prosecuted by the CDPP involve drug importation and money laundering offences. No convictions for money laundering have been reported for 2005.

In April 2003, the AFP established a Counter Terrorism Division to undertake intelligence-led investigations to prevent and disrupt terrorist acts. Eleven Joint Counter Terrorism Teams (JCTT), including investigators and analysts with financial investigation skills and experience, are conducting a number of investigations specifically into suspected terrorist financing in Australia. The AFP also works closely with overseas counterparts in the investigation of terrorist financing, and has worked closely with the FBI on matters relating to terrorist financing structures in South East Asia.

A draft AML/CTF Bill developed by the AGD and a package of draft AML/CTF Rules, developed by AUSTRAC, have recently been released for public comment. The package of draft legislation and rules will form the basis of further consultations on proposed enhancements to current customer due diligence, reporting and record keeping obligations, and deficiencies in regulatory coverage identified in Australia's FATF Mutual Evaluation Report. The consultation package represents a first tranche of reforms, which would apply to financial services, including when provided by professionals such as lawyers and accountants, gambling services and bullion sellers. Businesses providing these designated services would be required to, amongst other obligations, verify the identity of customers, report suspicious matters, keep appropriate records, and maintain rigorous internal AML/CTF Programs.

The release of the draft bill and AML/CTF Rules followed the passing of interim legislation in the form of Anti-Terrorism Act (No 2) 2005 (AT Act). The AT Act contains a range of measures to improve Australia's compliance with the FATF Special Recommendations on Terrorist Financing VI, VII and IX:

- Special Recommendation VI-providers of remittance services (including alternative remittance dealers) will be required to register with AUSTRAC.
- Special Recommendation VII-businesses that send international funds transfers on behalf of customers will be required to include customer information with the funds transfer instructions.
- Special Recommendation IX-travelers will be required to declare bearer negotiable instruments (e.g., travelers checks) that they are bringing into or taking out of Australia, at the request of a Customs or police officer.

The Australian Government will consider a second tranche of reforms, extending to real estate agents, jewelers, and specified non-financial legal and accounting services once the first tranche of AML/CTF reforms are implemented. The proposed legislative framework provides scope for operational detail to be settled in AML/CTF Rules, which will be developed by (AUSTRAC) in consultation with industry.

Australia is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime and its protocol on migrant smuggling. In September, 1999, a Mutual Legal Assistance Treaty between Australia and the United States entered into force. Australia participates actively in a range of international fora including the Financial Action Task Force, a member of the Pacific Islands Forum, and the Commonwealth Secretariat. Through its funding and hosting of the Secretariat of the Asia/Pacific Group on Money Laundering, of which it serves as permanent co-chair, the GOA has

elevated money laundering and terrorist financing issues to a priority concern among countries in the Asia/Pacific region. AUSTRAC is an active member of the Egmont Group of Financial Intelligence Units. AUSTRAC has signed Memoranda of understanding (MOUs) allowing the exchange of financial intelligence with FinCEN and the FIUs of 40 other countries.

Following the bombings in Bali in October 2002, the Australian Government announced an ADOL AUD 10 million (approximately $7.5 million) initiative managed by AusAID, to assist in the development of counterterrorism capabilities in Indonesia. As part of this initiative, the AFP has established a number of training centers such as the Joint Centre for Law Enforcement Cooperation. As part of Australia's broader regional assistance initiatives, AUSTRAC has embarked on a long-term technical assistance program to help Indonesia in developing an effective Financial Intelligence Unit (FIU). AUSTRAC is exploring similar assistance to other regional FIUs, with AUD 7.8 million (approximately $5,85 million) in funding over the next four years under the Southeast Asia Counter-Terrorism Technical Assistance and Training Package. AUSTRAC has provided training and other technical assistance to developing FIUs in Southeast Asia, including the Philippine FIU and regional training provided by AUSTRAC through the Malaysian Government's South East Asian Regional Centre for Counter Terrorism. In the Pacific region, AUSTRAC has developed and provided unique software to six nascent Pacific island FIUs to fulfill their domestic obligations and share information with foreign analogs. The AGD received a grant of AUD 7.7 million (approximately $5.75) to develop an a four year program AML/CTF regimes for the Pacific island jurisdictions. The AGD's program will work cooperatively with the U.S. Department of State funded Pacific Islands Anti-Money Laundering Program (PAPL). The PALP, projected to be a four-year program, will be managed by the Pacific Islands Forum (PIF) and will employ residential mentors to develop or enhance existing AML/CTF regimes in the fourteen non-FATF member states of the PIF.

Simultaneously, the GOA continues to pursue a comprehensive, anti-money laundering/counterterrorist financing regime to meets the objectives of the revised FATF Forty Recommendations and Nine Special Recommendations on Terrorist Financing. To enhance its AML regime, as noted in FATFME, AUSTRAC should conduct more on-site compliance audits and be enabled to levy administrative sanctions for non-compliance with AML/CTF laws and regulations. Additionally, the GOA should consider coordinating all regulatory agencies of its financial, securities and insurance sectors. It should also continue its exemplary leadership role in emphasizing money laundering/terrorist finance issues and trends within the Asia/Pacific region and its commitment to providing training and technical assistance to the jurisdictions in that region.

Austria

Austria is not an important regional financial center, offshore tax haven, or banking center. There is no hard evidence that Austria is a major money laundering country; however, like any highly developed financial marketplace, Austria's financial and non-financial institutions are vulnerable to money laundering. The Austrian Interior Ministry's crime statistics show mixed developments regarding financial crime in Austria in 2004, with a significant increase in serious fraud. The percentage of undetected organized crime is believed to be enormous, with much of it coming from the former Soviet Union. Organized crime is involved in money laundering in connection with narcotics trafficking and trafficking in persons, but apparently not in connection with contraband smuggling.

Money laundering occurs within the Austrian banking system as well as in non-bank financial institutions and businesses. Many of the former-Soviet crime groups are trying to launder money in Austria by investing in real estate, exploiting existing business contacts, and trying to establish new contacts in politics and business. Criminal groups seem increasingly to use money transmitters and informal money transfer systems to launder money. The Internet and offshore companies also play an important role in such crime.

Austria criminalized money laundering in 1993. Predicate crimes are listed and include terrorist financing and many financial and other serious crimes. Regulations are stricter for money laundering by criminal organizations and terrorist "groupings," because in such cases no proof is required that the money stems directly or indirectly from prior offenses.

Amendments to the Customs Procedures Act and the Tax Crimes Act, effective May 1, 2004, address the problem of cash couriers and international transportation of illegal-source currency and monetary instruments. Austrian customs authorities do not automatically screen all persons entering Austria for cash or monetary instruments. However, if asked, anyone carrying more than 15,000 euros (approximately $17,800) must declare the funds and provide information on their source and use. Spot checks for currency at border crossings will continue. Customs has authority to seize suspect cash at the border.

In implementing the new EU regulation on controls of cash entering or leaving the Community, the Government of Austria (GOA) in 2006 plans to amend the Customs Procedures Act and the Tax Crimes Act to introduce a declaration obligation for anyone carrying cash of 10,000 euros (approximately $12,000) or more.

Adoption of the Banking Act of 1994 creates customer identification, record keeping, and staff training obligations for the financial sector. Entities subject to the Banking Act include banks, leasing and exchange businesses, safe custody services, and portfolio advisers. The Insurance Act of 1997 includes similar regulations for insurance companies underwriting life policies. The Banking Act requires identification of all customers when entering an ongoing business relationship, i.e., in all cases of opening a checking account, a passbook savings account, a securities deposit account, etc. In addition, customer identification is required for all transactions of more than 15,000 euros for customers without a permanent business relationship with the bank. Banks and other financial institutions are required to keep records on customers and account owners. Bankers are protected with respect to their cooperation with law enforcement agencies. They are also not liable for damage claims resulting from delays in completing suspicious transactions. There is no requirement for banks to report large currency transactions, unless they are suspicious. The Austrian Financial Intelligence Unit (AFIU) is, however, providing information to banks to raise awareness of large cash transactions.

Since October 2003, financial institutions have adopted tighter identification procedures, requiring all customers appearing in person to present an official photo identification card. These procedures also apply to trustees of accounts, who are now required to disclose the identity of the account beneficiary. However, the procedures still allow customers to carry out non-face-to-face transactions, including Internet banking, on the basis of a copy of a picture identification card.

Some years ago the Financial Action Task Force (FATF) and the European Union (EU) criticized the GOA for permitting anonymous numbered passbook savings accounts. The Austrians temporarily "grandfathered" existing accounts, but they have now nearly all been closed. Since 2000, new passbook savings accounts and deposits to existing accounts require customer identification.

The Banking Act includes a due diligence obligation, and individual bankers are held legally responsible if their institutions launder money. In addition, banks have signed a voluntary agreement to prohibit active support of capital flight. On November 26, 2001, the Federal Economic Chamber's Banking and Insurance Department, in cooperation with all banking and insurance associations, published an official Declaration of the Austrian Banking and Insurance Industries to Prevent Financial Transactions in Connection with Terrorism.

The 2003 Amendments to the Austrian Gambling Act, the Business Code, and the Austrian laws governing lawyers, notaries, and accounting professionals, introduced money laundering regulations regarding identification, record keeping, and reporting of suspicious transactions for dealers in high-

value goods such as precious stones or metals, or works of art, auctioneers, real estate agents, casinos, lawyers, notaries, certified public accountants, and auditors.

Since 2002, the AFIU, the central repository of suspicious transaction reports, has been a section of the Austrian Interior Ministry's Bundeskriminalamt (Federal Criminal Intelligence Service). During the first eleven months of 2005, the AFIU received 372 suspicious transaction reports from banks, and fielded 417 requests for information from Interpol, Europol, the Egmont Group, and other authorities. This represents an increase from the 373 suspicious transactions (349 of them from banks) reported in 2004, which led to five convictions for money laundering. Criminals are often convicted for other crimes, however, with money laundering serving as additional grounds for conviction.

Legislation implemented in 1996 allows for asset seizure and the forfeiture of illegal proceeds. The banking sector generally cooperates with law enforcement efforts to trace funds and seize illicit assets. The distinction between civil and criminal forfeiture in Austria is different from that in the U.S. legal system. However, Austria has regulations in the Code of Criminal Procedure that are similar to civil forfeiture, which is a form of forfeiture through an independent procedure. Courts may freeze assets in the early stages of an investigation. While in previous years there had been little evidence of enforcement, as law enforcement units tend to be understaffed, in the first eleven months of 2005, Austrian courts froze assets worth 98.3 million euros (approximately $117 million), nearly four times as much as the 25.4 euros (approximately $29.8 million) seized in the equivalent period of 2004.

The amended Extradition and Judicial Assistance Law provides for expedited extradition, expanded judicial assistance, and acceptance of foreign investigative findings in the course of criminal investigations, as well as enforcement of foreign court decisions. Austria has strict banking secrecy regulations, though bank secrecy can be lifted for cases of suspected money laundering. Moreover, bank secrecy does not apply in cases when banks and other financial institutions are required to report suspected money laundering. Such cases are subject to instructions of the authorities (i.e., AFIU) with regard to processing such transactions.

The Criminal Code Amendment 2002, effective October 1, 2002, introduced the following new criminal offense categories: terrorist "grouping," terrorist criminal activities, and financing of terrorism. "Financing of terrorism" is defined as a separate criminal offense category in the Criminal Code, punishable in its own right. Terrorism financing is also included in the list of criminal offenses subject to domestic jurisdiction and punishment, regardless of the laws where the act occurred. Further, the money laundering offense is expanded to terrorist "groupings." The law also gives the judicial system the authority to identify, freeze, and seize terrorist financial assets. With regard to terrorist financing, forfeiture regulations cover funds collected or held available for terrorist financing, and permit freezing and forfeiture of all assets that are in Austria, regardless of the place of the crime and the whereabouts of the criminal.

The Austrian authorities have circulated to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224.or designated by the EU. According to the Ministry of Justice and the AFIU, no accounts found in Austria ultimately showed any links to terrorist financing. After September 11, 2001, the AFIU froze several accounts on an interim basis, but in the course of trying to establish evidence, only two accounts were designated for seizure. Both later turned out to be cases of mistaken identity.

During the first 11 months of 2005, the AFIU and a sister agency received 24 reports on suspected terrorism financing transaction reports, of which 15 were from banks, 7 from foreign authorities, and 2 from domestic. No assets were frozen. The increase from the 14 suspicious transactions in 2004 is due to improved control mechanisms in banks and better international cooperation. None of the 2004 reports resulted in a conviction—with many cases being due to mistaken identity.

Since January 1, 2004, money remittance businesses require a banking license from the Financial Market Authority (FMA) and are subject to supervision. Informal remittance systems like hawala exist in Austria, but are subject to administrative fines for carrying out banking business without a license.

The GOA has undertaken important efforts that may help thwart the misuse of charitable and/or non-profit entities as conduits for terrorist financing. A new law on responsibility of associations, effective January 1, 2006, introduces criminal responsibility for all legal entities, general and limited commercial partnerships, registered partnerships, and Europe economic interest groupings. The law covers all crimes listed in the criminal code, including corruption, money laundering, and terrorist financing. The earlier law on associations (Vereinsgesetz, published in Federal Law Gazette No. I/66 of April 26, 2002) came into force on July 1, 2002, and covers charities and all other nonprofit associations in Austria (including religious associations, sports clubs, etc.). This law is similar to its predecessor, but it calls for record keeping and auditing on the part of non-profit entities. The 2002 Vereinsgesetz regulates the establishment of associations, bylaws, organization, management, association register, appointment of auditors, and detailed accounting requirements. The Ministry of Interior's responsibility is limited to approving the establishment of associations, regardless of the purpose of the association, unless it violates legal regulations.

There are no regular or routine checks made on associations established in Austria. Only in case of complaints does the Interior Ministry start investigations and, in case of serious violations of laws, it may officially prohibit the association from operating. Reportedly, the GOA has generally implemented the FATF's Special Recommendations on Terrorist Financing, except for certain aspects of the recommendation regarding non-profit organizations.

Adoption of the new EU regulation on wire transfers is imminent. The European Commission hopes the regulation will enter into force on January 1, 2007, at which time it will be immediately and directly applicable in Austria. In 2006 the GOA will start working on domestic implementation of the EU's third money laundering directive (Directive 2005/60/EC on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing), which involves a number of legal changes, including of the Banking Act, Insurance Act, Gambling Act, Business Code, and several other laws. During Austria's EU presidency in the first half of 2006, the GOA in various EU committees and bodies will also work to implement guidelines for the third money laundering directive, proceed with implementing the FATF's Special Recommendation Seven on Wire-Transfers, host a workshop on a code of conduct for non-profit organizations, and, together with the U.S. Government, host another workshop on terrorist financing.

Austria has not enacted legislation that provides for sharing forfeited narcotics-related assets with other governments. However, mutual legal assistance treaties (MLATs) can be used as an alternative vehicle to achieve equitable distribution of forfeited assets. Ratification of bilateral protocols to update the bilateral MLAT, which has been in force since August 1, 1998, and the bilateral extradition treaty, which has been in force since January 1, 2000, and bring them in line with the twin U.S.-EU agreements on extradition and mutual legal assistance, is underway. In addition to the exchange of information with home country supervisors permitted within the EU, Austria has defined this information exchange more precisely in agreements with nine other EU members (France, Germany, Italy, Netherlands, United Kingdom, the Czech Republic, Hungary, Slovakia, and Slovenia).

The International Monetary Fund's spring 2004 Financial System Stability Assessment (FSAP) stated that Austria has made significant progress in the past few years in bringing its anti-money laundering and counterterrorism financing regime into compliance with international standards. The FSAP notes that the overall legal and institutional framework currently in place is comprehensive and that Austria has achieved a good level of compliance with the FATF Recommendations. The FMA has created an internal Task Force on Money Laundering, and in following up on suggestions for further

improvements, started to publish on its homepage circulars with additional guidance for banks and other financial institutions on fighting money laundering and terrorist financing.

Austria is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Austria ratified the UN Convention against Transnational Organized Crime on September 23, 2004, and the UN International Convention for the Suppression of the Financing of Terrorism on April 15, 2002. Austria is a party to the UN Convention against Corruption. Austria is a member of the FATF and the EU. The AFIU is a member of the Egmont Group.

The Government of Austria has criminalized money laundering for all serious crime, and passed additional legislation necessary to construct a viable anti-money laundering regime. Austria is generally cooperative with U.S. authorities in money laundering cases. But some improvements could still be made. There remains a need for identification procedures for customers in non-face-to-face banking transactions. The criminal code should be amended to penalize negligence in reporting money laundering and terrorist financing transactions. The AFIU and law enforcement should be provided with sufficient resources to adequately perform their functions. AFIU and other government personnel should be protected against damage claims because of delays in completing suspicious transactions. Additionally, Austria should adequately regulate its charitable and non-profit entities to reduce their vulnerability to misuse by criminal and terrorist organizations and their supporters.

Bahamas

The Commonwealth of the Bahamas is an important regional and offshore financial center. Second to tourism, the economy depends on its financial services sector. Financial services account for approximately 15 percent of the gross domestic product. The U.S. dollar circulates freely in the Bahamas, and is accepted everywhere on par with the Bahamian dollar. Money laundering in the Bahamas is related to financial fraud and the proceeds of drug trafficking. Illicit proceeds from drug trafficking usually take the form of cash or are quickly converted into cash. The strengthening of anti-money laundering laws has made it increasingly difficult for most drug traffickers to deposit large sums of cash. As a result, a new trend has developed of storing extremely large quantities of cash in security vaults at properties deemed to be safe houses. Other money laundering trends include the purchase of real estate, large vehicles, and jewelry, and the processing of money through a complex national or international web of legitimate businesses and shell companies.

The Bahamas has two 24 hour casinos in Nassau and one in Freeport/Lucaya, with a fourth scheduled to open in 2006. Cruise ships that overnight in Nassau may operate casinos. Reportedly, there are over ten Internet gaming sites based in the Bahamas, although none are licensed with Bahamian authorities. Under Bahamian law, Bahamian residents are prohibited from gambling.

The Central Bank of the Bahamas is responsible for the licensing, regulation, and supervision of banks and trust companies operating in and from within the Bahamas. The Central Bank Act 2000 (CBA) and The Banks and Trust Companies Regulatory Act 2000 (BTCRA) enhanced the supervisory powers of the Central Bank. The CBA gives the Central Bank extensive information gathering powers including on-site inspection of banks and provides for enhanced cooperation between overseas regulatory authorities and the Central Bank. The BTCRA expands the licensing criteria for banks and trust companies, enhances the supervisory powers of the Inspector of Banks and Trust Companies, and enhances the role of the Central Bank's Governor including the right to deny licenses to banks or trust companies he/she deems unfit to transact business in the Bahamas. In 2001, The Central Bank enacted a physical presence requirement that means "managed banks" (those without a physical presence but which are represented by an agent such as a lawyer or another bank) must either establish a physical presence in the Bahamas (an office, separate communications links, and a resident director) or cease operations. The transition to full physical presence was largely complete for all affected banks and

trust companies by the end of 2004. The physical presence requirement is thought to have led to a gradual decline in banks and trusts from 301 in 2003 to 253 in 2005.

The International Business Companies Act 2000 and 2001 (Amendments) enacted provisions that abolish bearer shares, require international business companies (IBCs) to maintain a registered office in the Bahamas, and require a copy of the Register of the names and addresses of the Directors and Officers and a copy of the Shareholders Register to be kept at the registered office. A copy of the Register of Directors and Officers must also be filed with the Registrar General's office. Only banks and trust companies licensed under the BTCRA and financial and corporate service providers licensed under the Financial Corporate Service Providers Act (FCSPA) may provide registration, management, administration, registered agent, registered office, nominee shareholders, and officers and directors for IBCs.

The Financial Transaction Reporting Act 2000 (FTRA) requires financial institutions (such as banks and trusts, insurance companies, real estate brokers, casino operators, and others which hold or administer accounts for clients) to verify the identity of account holders, and to report suspicious transactions (STRs) to the FIU and the police. The FTRA also establishes "know your customer" (KYC) requirements. By December 31, 2001, financial institutions were obliged to verify the identities of all their existing account holders and of customers without an account who conduct transactions over $10,000. All new accounts established in 2001 or later have to be in compliance with KYC rules before they are opened. As of September 2005, the Central Bank reports greater than 95 percent compliance with KYC requirements. KYC requirements initially caused complaints by Bahamians who were unable to produce adequate documentation when attempting to open accounts in domestic banks. (The absence of house numbers on most Bahamian streets, the prevailing practice of utility companies' issuing bills only in the name of landlords rather than tenants, and the scarcity of photo identification among Bahamians contribute to these documentation problems.) In October 2002, the Minister of Financial Services and Investments lamented that the rigid, overly prescriptive requirements of the KYC rules had caused financial institutions to harass longstanding, well-known clients for documents, and observed that those rules had been applied to accounts of low-risk customers, including pensioners, whose opportunities for money laundering were minimal. The Government of the Commonwealth of the Bahamas (GCOB) declined banking officials' recommendations to apply a risk-based approach to "grandfather" Bahamas-based accounts considered to be in compliance, and instead extended the compliance deadline to June 2006.

Established by the FIU Act 2000, the Bahamas FIU operates as an autonomous body under the Office of the Attorney General. The FIU is the responsible agency for receiving, analyzing, and disseminating suspicious transaction reports (STRs). The FIU has the administrative power to issue an injunction to stop anyone from completing a transaction for a period of up to three days upon receipt of an STR. From January to May 2005, the FIU received 67 STRs of which 55 were being analyzed, and 8 were forwarded to the police for investigation. The Bahamas FIU has signed several memoranda of understanding with other FIUs for the exchange of information. As a result of the Financial Intelligence Unit (Amendment) Act 2001, the FIU is able to cooperate and assist foreign FIUs. The FIU became a member of the Egmont Group in 2001.

The eight-member Tracing and Forfeiture/Money Laundering Investigation Section of the Drug Enforcement Unit of the RBPF is the primary financial law enforcement agency in the Bahamas, with the responsibility for investigating STRs received from the FIU, all reports of money laundering received from law enforcement agencies or the public, and matters of large cash seizures. It also investigates local drug-traffickers and other serious crime offenders, to determine whether they benefited from their criminal conduct. As a matter of law, the GCOB seizes assets derived from international drug trade and money laundering. Over the years, joint U.S./GCOB investigations have resulted in the seizure of cash, vehicles and boats. The seized items are in the custody of the GCOB. Some are in the process of confiscation while some remain uncontested.

The Bahamas has a Mutual Legal Assistance Treaty with the United States, which entered into force in 1990, and agreements with the United Kingdom and Canada. The Attorney General's Office for International Affairs manages multilateral information exchange requests. In December 2004, the Bahamas signed an agreement for future information exchange with the U.S. Securities and Exchange Commission to ensure that requests can be completed in an efficient and timely manner.

In November 2004, the Anti-Terrorism Act was passed to implement the provisions of the UN International Convention for the Suppression of the Financing of Terrorism. In addition to formally criminalizing terrorism and making it a predicate crime for money laundering, the law provides for the seizure and confiscation of terrorist assets, reporting of suspicious transactions related to terrorist financing, and strengthening of existing mechanisms for international cooperation. The Bahamas also ratified the UN International Convention for the Suppression of the Financing of Terrorism on November 1, 2005. The Bahamas signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. The Bahamas is a party to the 1988 UN Drug Convention. The Bahamas is a member of the Caribbean Financial Action Task Force and was Chair in 2003.

The GCOB has enacted substantial reforms that could reduce its financial sector's vulnerability to money laundering; however, it must steadfastly and effectively implement those reforms. The Bahamas should provide adequate resources to its law enforcement and prosecutorial/judicial personnel to ensure that investigations and prosecutions are satisfactorily completed, and requests for international cooperation are efficiently processed.

Bahrain

Bahrain has one of the most diversified economies in the Persian Gulf and the Gulf Cooperation Council (GCC), which consists of Bahrain, Saudi Arabia, United Arab Emirates, Kuwait, Qatar, and Oman. Though the government depends on oil and petroleum processing for nearly 70 percent of its revenue, Bahrain's oil reserves are dwindling. In contrast to the economies of many of its neighbors, oil accounted for just 15.4 percent of Bahrain's gross domestic product (GDP) in 2004. Its financial sector, in contrast, accounted for 24.2 percent. Bahrain has promoted itself as an international financial center in the Gulf region and sees the sector as vital to its future. As of December 2005, the Bahrain Monetary Agency (BMA)—Bahrain's Central Bank and sole regulator for the financial sector—had issued a total of 358 licenses, including 169 banks, of which 51 are offshore banking units (OBUs), 39 are investment banks, 25 are commercial banks, and 32 are representative offices of international banks. In addition, there are 19 money changers, 22 locally operating insurance companies (of which 12 are locally incorporated) and 73 insurance exempt companies (the bulk of whose operations are in Saudi Arabia). With so many financial institutions, and a geographic location in the Middle East as a transit point along the Gulf and into southwest Asia, Bahrain may attract money laundering activities. However, it is thought that the greatest risk of money laundering is not illegal money generated in Bahrain, but rather Bahrain's financial institutions being used to layer illegal foreign money by transiting it through Bahrain.

In January 2001, the Government of Bahrain (GOB) enacted an anti-money laundering (AML) law that criminalizes the laundering of proceeds derived from any predicate offense. The law stipulates punishment of up to seven years imprisonment and a fine of up to one million Bahraini dinars (BD) (about $2.65 million) for convicted launderers and those aiding or abetting them. If organized criminal affiliation, corruption, or disguise of the origin of proceeds is involved, the minimum penalty is a fine of at least 100,000 dinars (approximately $265,000) and a prison term of not less than five years. Notably, the AML law allows Bahrain to prosecute a money laundering violation regardless of whether the act is a crime in Bahrain. For example, there is no income tax in Bahrain, yet someone engaging in illicit financial transactions for the purpose of evading another nation's tax system may be prosecuted for money laundering in Bahrain.

Following enactment of the law, BMA, as the principal financial sector regulator, issued regulations requiring financial institutions to file suspicious transaction reports (STRs), to maintain records for a period of five years, and to provide ready access for law enforcement officials to account information. Immunity from criminal or civil action is given to those who report suspicious transactions. There is no minimum threshold required to file an STR.

The law also provides for the formation of an interagency committee to oversee Bahrain's anti-money laundering regime. Accordingly, in June 2001, the Anti-Money Laundering Policy Committee was established and assigned the responsibility for developing anti-money laundering policies and guidelines. The committee, which is under the chairmanship of the Undersecretary of Finance, includes members from the BMA, the Bahrain Stock Exchange, and the Ministries of Finance, Interior, Justice, Industry & Commerce, Labor and Social Affairs, and Foreign Affairs. The law further provides for the confiscation of assets and allows for greater international cooperation. This committee had an initial duration of three years, but its mandate was renewed in March 2005 for an additional three years. In the process of reinstating the committee in 2005, representatives from the Directorate of Customs Inspections, the Terrorist Financing Unit of the National Security Agency, and the Office of the Public Prosecutor were also added to the committee.

In addition, the law provides for the creation of the Anti-Money Laundering Unit (AMLU) as Bahrain's financial intelligence unit (FIU). The AMLU, which is housed in the Ministry of Interior, is empowered to: receive reports of money laundering offenses, conduct preliminary investigations, implement procedures relating to international cooperation under the provisions of the law, and execute decisions, orders, and decrees issued by the competent courts in offenses related to money laundering. The AMLU became a member of the Egmont Group of FIUs in July 2003.

The AMLU receives suspicious transaction reports (STRs) from banks and other financial institutions, investment houses, broker/dealers, money changers, insurance firms, real estate agents, gold dealers, financial intermediaries, and attorneys. Financial institutions must also file STRs with the BMA, which supervises these institutions. In March 2005, the BMA started receiving STRs from banks and financial institutions via a secure website. Non-financial institutions are required under a Ministry of Industry & Commerce (MOIC) directive to also file STRs with that ministry. The BMA analyzes the STRs, of which it receives copies, as part of its scrutiny of compliance by financial institutions with anti-money laundering and combating terrorist financing (AML/CFT) regulations, but it does not independently investigate the STRs (responsibility for investigation rests with the AMLU). The BMA may assist the AMLU with its investigations, where special banking expertise is required.

In 2003, the MOIC published new anti-money laundering guidelines, which govern all non-financial institutions. The MOIC system of requiring dual STR reporting to both it and the AMLU mirrors the BMA's system. Good cooperation exists between MOIC, BMA, and AMLU, with all three agencies describing the double filing of STRs as a backup system. The AMLU, MOIC, and BMA's compliance units analyze the STRs and work together on identifying weaknesses or criminal activity, but it is the AMLU that conducts a preliminary investigation and then forwards cases of suspected money laundering and terrorist financing for investigation to the Office of Public Prosecutor. The AMLU works with the Office of the Public Prosecutor, which under Bahrain's trial system is the body responsible for gathering and assessing evidence for trial.

From January to December 2005, the AMLU received and investigated 219 STRs. This is a dramatic increase over the 294 STRs received between June 2001 and February 2005. The AMLU attributes this to increased awareness of the need to file STRs within the Bahrain financial and designated non-financial sectors. In 2005, four cases were forwarded to the Office of the Public Prosecutor after preliminary investigation, and are currently undergoing investigation by the public prosecutor, in anticipation of referral to the courts for trial. The AMLU has obtained three court orders to freeze bank accounts of suspected money launderers.

The AMLU has been notably public in its crackdown on narcotics and financial crimes. The AMLU has announced money laundering and narcotics arrests and issued fraud and scam warnings. This activity is significant because it demonstrates strong public action against financial crimes—in a region where most countries are either not targeting financial crimes or do not make their efforts highly public. Despite being hampered by an overburdened criminal court system and a lack of specialized prosecutors and judges, Bahrain has managed to bring four money laundering cases before the courts for prosecution. However, none of these cases has yet reached the trial stage. Nonetheless, members of the Office of the Public Prosecutor recently attended U.S.-sponsored AML/CFT courses, and the Government of Bahrain is contemplating the establishment of a special court to try financial crimes. The Ministry of Justice has also sent Bahraini judges abroad for specialized training to handle such crimes.

There are 51 BMA-licensed offshore banking units (OBUs), representing both international and regional banks, active mainly in commercial and wholesale banking (e.g., project and corporate finance). OBUs are prohibited from accepting deposits from citizens and residents of Bahrain, and from undertaking transactions in Bahraini dinars (with certain exemptions, such as dealings with other banks and government agencies). In all other respects, OBUs are regulated and supervised in the same way as the domestic banking sector. They are subject to the same regulations, on-site examination procedures, and external audit and regulatory reporting obligations. OBUs are required to maintain a substantive physical presence in Bahrain, including resident management.

Bahrain's Commercial Companies Law (Legislative Decree 21 of 2001) does not permit the registration of offshore companies or international business companies (IBCs). All companies must be resident and maintain their headquarters and operations in Bahrain. Capital requirements vary, depending on the legal form of the company, but in all cases the amount of capital required must be sufficient for the nature of the activity to be undertaken. In the case of financial services companies licensed by BMA, various minimum and risk-based capital requirements are also applied (in addition to a variety of other prudential requirements), in line with international standards of the Basel Committee's Core Principles for Effective Banking Supervision.

In January 2002, the BMA issued a circular implementing the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing as part of the BMA's AML regulations, and subsequently froze two accounts designated by the UNSCR 1267 Sanctions Committee and one account listed under U.S. Executive Order 13224. However, the Government of Bahrain has not yet passed its law criminalizing terrorist financing or issued new regulations concerning the FATF Special Recommendation Nine on cash couriers. The amendments to the AML law to create specific antiterrorist financing offenses and offenses to combat cash couriers are currently before the National Assembly, together with a new antiterrorism law that would add to and expand the scope of the predicate offenses of terrorism already contained in the Bahrain penal code.

Regulation No. 1 of 1994 requires all persons or entities providing money exchange and remittance and currency transfer services to be licensed by BMA as money changers. BMA Circular BC/1/2002 states that money changers may not transfer funds for customers in another country by any means other than Bahrain's banking system. In addition, all BMA licensees are required to include details of the originator's information with all outbound transfers. With respect to incoming transfers, licensees are required to maintain records of all originator information and to carefully scrutinize inward transfers that do not contain the originator's information, as they are presumed to be suspicious transactions. Licensees that suspect, or have reasonable grounds to suspect, that funds are linked or related to suspicious activities—including terrorist financing—are required to file suspicious transaction reports (STRs). Licensees must maintain records of the identity of their customers in accordance with the BMA's anti-money laundering regulations, as well as the exact amount of transfers. During 2004, the BMA consulted with the industry on changes to its existing AML/CFT regulations, to reflect revisions by the FATF to its Forty plus Nine Recommendations. These updates

were issued to banks and insurance companies during the course of 2005. Those for remaining licensees are scheduled to be implemented in early 2006.

Legislative Decree No. 21 of 1989 governs the licensing of non-profit organizations. The Ministry of Social Development (MSD) is responsible for licensing and supervising charitable organizations in Bahrain. In February 2004, as part of its efforts to strengthen the regulatory environment and fight potential terrorist financing, MLSA issued a Ministerial Order regulating the collection of donated funds through charities and their eventual distribution, to help confirm the charities' humanitarian objectives. The regulations are aimed at tracking money that is entering and leaving the country. These regulations require organizations to keep records of sources and uses of financial resources, organizational structure, and membership. Charitable societies are also required to deposit their funds with banks located in Bahrain and may have only one account in one bank. The MSD has the right to inspect records of the societies to insure their compliance with the laws. Additionally, banks are required to have a registration certificate from the MSD to open an account for a charity, and banks must report to the BMA any transaction by a charitable institution that exceeds BD 3,000 (approximately $7,950), a reduction from the original BD 20,000 ceiling.

Bahrain is a leading Islamic finance center in the region. The sector has grown considerably since the licensing of the first Islamic bank in 1979. Bahrain has 26 Islamic banks and financial institutions. Given the large share of such institutions in Bahrain's banking community, the BMA has developed a framework for regulating and supervising the Islamic banking sector, applying regulations and supervision the same way as it does with respect to conventional banks. In March 2002, the BMA introduced a comprehensive set of regulations for Islamic banks called the Prudential Information and Regulatory Framework for Islamic Banks (PIRI). The framework was designed to monitor certain banking aspects, such as capital requirements, governance, control systems, and regulatory reporting.

In March 2004, Bahrain issued a Legislative Decree ratifying the Convention against Transnational Organized Crime. In June 2004, Bahrain published two Legislative Decrees ratifying the UN International Convention for the Suppression of the Financing of Terrorism, and the UN International Convention for the Suppression of Terrorist Bombings. Bahrain is now a party to 11 of the 12 UN conventions on terrorism. Bahrain is also a party to the Arab Convention for the Suppression of Terrorism and the Convention of the Organization of the Islamic Conference on Combating International Terrorism. In December 2005, Bahrain ratified the GCC Agreement to Combat Terrorism.

Bahrain is also the headquarters for the Middle East and North Africa Financial Action Task Force (MENAFATF) secretariat. MENAFATF held its inaugural meeting in November 2004 and its first plenary in April 2005 in Bahrain. As a FATF-style regional body, MENAFATF promotes best practices on AML/CFT issues, conducts mutual evaluations of its members against the FATF standards, and works with its members to comply with international standards and measures.

Bahrain has shown progress in investigating and publicizing financial crimes. The AMLU has openly published information on narcotic arrests and its actions against financial crimes. The BMA has upgraded its regulatory requirements in line with developments in international standards and has significantly tightened its reporting requirements for charitable transfers. However, the lack of capacity within the Office of the Public Prosecutor and the judiciary has prevented the AMLU from bringing these complicated cases to trial.

Despite the achievements of the AMLU and the BMA, the Bahraini Government has not yet passed a law to combat terrorist financing and the problem of cash couriers. The Bahraini Government should continue its battle against money launderers and terrorist financiers by enacting such laws, by aggressively enforcing both the new laws and the existing AML law and regulations, and by enhancing the prosecutorial and judicial ability to successfully try financial crimes.

Bangladesh

Bangladesh is not an important regional or offshore financial center.

There are no indications that substantial funds are laundered through the official banking system. The principal money laundering vulnerability remains the widespread use of the underground hawala or "hundi" system to transfer value outside the formal banking network. The vast majority of hundi transactions in Bangladesh are used to repatriate wages from Bangladeshi workers abroad. However, as elsewhere, the hundi system is also used to avoid taxes, customs duties and currency controls and as a compensation mechanism for the significant amount of goods smuggled into Bangladesh. Traditionally, trade goods provide counter valuation in hundi transactions.

An estimated $1 billion dollars worth of dutiable goods is smuggled every year from India into Bangladesh. A comparatively small amount of goods is smuggled out of the country into India. Instead, hard currency and other assets flow out of Bangladesh to support the smuggling networks.

Corruption is a major area of concern in Bangladesh. The non-convertibility of the local currency (the taka) coupled with intense scrutiny on foreign currency transactions in formal financial institutions also contribute to the popularity of both hundi and black market money exchanges.

Money exchanges outside the formal banking system are illegal. During the last year, there has been a significant increase in the amount of money transferred through the formal banking system as a result of the efforts by the Government of Bangladesh (GOB) to increase the efficiency of the process.

Bangladeshis are not allowed to carry cash outside of the country in excess of 3,000 taka (approximately $50). There is no limit as to how much currency can be brought into the country, but amounts over $5,000 must be declared. Customs is primarily a revenue collection agency, accounting for 40-50 percent of annual Bangladesh government income.

Since 2004, the Central Bank (CB), Bangladesh Bank, has conducted training for every bank's headquarters around the county in "know your customer" practices. Since Bangladesh does not have a national identify card and because most Bangladeshis do not have a passport, there are difficulties in enforcing customer identification requirements. In most cases, banking records are maintained manually with little support technology, although this is changing, especially in head offices. Accounting procedures used by the CB may not in every respect achieve international standards. In 2004, the Bangladesh Bank issued "Guidance Notes on Prevention of Money Laundering" and designated effective anti-money laundering compliance programs as a "core risk" subject to the annual bank supervision process of the Bangladesh Bank. Banks are required to have an anti-money laundering compliance unit in their head office and a designated anti-money laundering compliance officer in each bank branch. The Bangladesh Bank conducts regular training programs for compliance officers based on the Guidance Notes. In December 2005, the CB called all compliance officers to Dhaka for a discussion about their obligations and heightened police interest in money laundering and terrorist financing.

Currently, Bangladesh does not have a Financial Intelligence Unit (FIU) per se. However, under the 2002 Money Laundering Prevention Act (MLPA), the Anti-Money Laundering Unit (AMLU) of Bangladesh Bank acts as a de facto FIU and has authority to freeze assets without a court order and seize them with a court order. The Bangladesh Bank has received 45 suspicious transaction reports in 2005 to make a total of 193 suspicious transaction reports since the MLPA was passed in 2002. By 2004, 134 were resolved without further action. The remaining reports were transferred from the now defunct Bureau of Anti-Corruption to the newly created Anti-Corruption Commission (ACC). The ACC has advised the bank that it will not investigate these cases and stated it would send the files back to the CB by December 31, 2005. Currently, there are 29 cases pending with the Criminal Investigation Division of Bangladesh Police Headquarters that Bangladesh Bank referred to them after the ACC abruptly refused to investigate.

There have been important developments in 2005 in the anti-money laundering and terrorist financing arena. A new law, The Anti-Money Laundering and Terrorist Financing Act 2005 (AMLTF), has been drafted to replace the MLPA from 2002. The new legislation was to have been presented to the cabinet for approval in mid-December 2005. After Cabinet approval it will be vetted by the Law Ministry and then presented to Parliament. Reportedly, the current draft addresses most of the shortcomings in prior legislation noted in last year's INCSR report.

The AMLTF, if enacted, would criminalize terrorist financing. It would provide powers required for a FIU to meet international recommendations set forth by the Egmont Group, including sharing information with law enforcement at home and abroad. The draft legislation also provides for the establishment of a Financial Investigation and Prosecution Office wherein law enforcement investigators and prosecutors will work as a team from the beginning of the case to trial. The 2005 draft legislation also addresses asset forfeiture and provides that assets, substitute assets (without proving the relation to the crime) and instrumentalities of the crime can be forfeited. The draft legislation does not address the nuts and bolts of asset forfeiture that the CB asserts can be addressed administratively and via regulatory procedures.

In 2003, Bangladesh froze a nominal sum in an account of a designated entity on the UNSCR 1267 Sanctions Committee's Consolidated List and identified an empty account of another entity. In 2004, following investigation of the accounts of an entity listed on the UNSCR 1267 consolidated list, Bangladesh Bank fined two local banks for failure to comply with Bangladesh Bank regulatory directives. In 2005, the GOB became a party to the UN International Convention for the Suppression of the Financing of Terrorism and is now a party to twelve UN Conventions on Terrorism. The GOB is a party to the 1988 UN Drug Convention but is not a signatory to the Convention against Transnational Organized Crime. Bangladesh is a member of the Asia/Pacific Group on Money Laundering.

Despite advancements to address shortcomings in the money laundering and terrorist financing regime, the GOB's anti-money laundering/terrorist financing regimes need to be strengthened to comport with international standards, including standards for the criminalization of terrorist finance, for the provision of safe harbor in order to protect reporting individuals, for the conduct of due diligence, and for banker negligence legislation that would make individual bankers responsible under certain circumstances if their institutions launder money. While a lack of training, resources and computer technology, including computer links with the outlying districts, continue to hinder necessary progress, the GOB remains as the most corrupt government on Transparency International's Index.

Barbados

As a transit country for illicit narcotics, Barbados is both attractive and vulnerable to money launderers. The Government of Barbados (GOB) has taken a number of steps in recent years to strengthen its anti-money laundering legislation. As of December 31, 2005, the Barbados offshore sector includes 4,635 international business companies (IBCs), 413 exempt insurance companies, three trust companies, 11 finance companies, and 53 offshore banks. The Central Bank regulates and supervises, offshore banks, trust companies and finance companies and the other entities are regulated by the Ministry of Industry and International Business. According to the Central Bank, it is estimated that there is approximately $32 billion worth of assets in Barbados's offshore banks. Barbados has no Foreign Sales Corporations (FSCs) and no free trade zones.

The GOB initially criminalized drug money laundering in 1990 through the Proceeds of Crime Act, No. 13, which also authorizes asset confiscation and forfeiture, permits suspicious transaction disclosures to the Director of Public Prosecutions, and exempts such disclosures from civil or criminal liability. The Money Laundering (Prevention and Control) Act 1988 (MLPCA) criminalizes the

laundering of proceeds from unlawful activities that are punishable by at least one year's imprisonment. The MLPCA makes money laundering punishable by a maximum of 25 years in prison and a maximum fine of 2 million Barbadian dollars (BDS) (approximately $1 million).

The MLPCA applies to a wide range of financial institutions, including domestic and offshore banks, IBCs, and insurance companies. In 2001 the MLPCA was amended to bring non-traditional financial institutions under the supervision of the AMLA including "any person whose business involves money transmission services, investment services or any other services of a financial nature." These institutions are required to identify their customers, cooperate with domestic law enforcement investigations, report and maintain records of all transactions exceeding 10,000 BDS (approximately $5,000), and establish internal auditing and compliance procedures. Financial institutions must also report suspicious transactions to the Anti-Money Laundering Authority (AMLA). The AMLA was established in August 2000 to supervise financial institutions' compliance with the MLPCA and issue training requirements and regulations for financial institutions.

The International Business Companies Act (1992) provides for general administration of IBCs. The Ministry of Industry and International Business vets and grants licenses to IBCs after applicants register with the Registrar of Corporate Affairs. Bearer shares are not allowed, and financial statements of IBCs are audited if total assets exceed $500,000. To enhance due diligence efforts, the 2001 International Business (Miscellaneous Provisions) Act requires the provision of more information than was previously provided with IBC license applications or renewals.

The Barbados Central Bank's 1997 Anti-Money Laundering Guidelines for Licensed Financial Institutions were revised in 2001. The revised "know your customer" guidelines were issued in conjunction with the AMLA, and provide detailed guidance to financial institutions regulated by the Central Bank. The Central Bank conducts off-site surveillance and undertakes regular on-site examinations of licensees and applies a comprehensive methodology that seeks to assess the level of compliance with legislation and guidelines.

The Ministry of Finance issues banking licenses after the Central Bank receives and reviews applications, and recommends applicants for licensing. The Offshore Banking Act (1985) gives the Central Bank authority to supervise and regulate offshore banks, in addition to domestic commercial banks. The International Financial Services Act replaced the 1985 Act in June 2002, in order to incorporate fully the standards established in the Basel Committee's Core Principles for Effective Banking Supervision. The 2002 law provides for on-site examinations of offshore banks. This allows the Central Bank to augment its off-site surveillance system of reviewing anti-money laundering policy documents and analyzing prudential returns. Additionally, offshore banks must submit quarterly statements of assets and liabilities and annual balance sheets to the Central Bank. The Central Bank may also refer suspicious activity reports (SARs) to the Barbados Financial Intelligence Unit (FIU).

The FIU, located within the AMLA, was established in September 2000. The FIU was first established by administrative order, but subsequently implemented in statute by the MLPCA (Amendment) Act, 2001. The FIU is fully operational. By the end of December 2005, the FIU had received 84 SARs. The FIU forwards information to the Financial Crimes Investigation Unit of the police if it has reasonable grounds to suspect money laundering.

The MLPCA also provides for asset seizure and forfeiture. In November 2001, the GOB amended its financial crimes legislation to shift the burden of proof to the accused to demonstrate that property in his or her possession or control is derived from a legitimate source. Absent such proof, the presumption is that such property was derived from the proceeds of crime. The law also enhances the GOB's ability to freeze bank accounts and to prohibit transactions from suspect accounts.

The Barbados Anti-Terrorism Act, 2002-6, Section 4, gazetted on May 30, 2002, criminalizes the financing of terrorism. The GOB circulates the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. In 2005, the GOB found no evidence of terrorist financing. Intelligence suggests that a small amount of money is leaving Barbados via an alternative remittance system. However, the GOB has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and nonprofit entities. The GOB is considering amending the Money Laundering and Financing of Terrorism (Prevention and Control) Act.

Barbados has bilateral tax treaties that eliminate or reduce double taxation, with the United Kingdom, Canada, Finland, Norway, Sweden, Switzerland, and the United States. The United States and the GOB ratified amendments to their bilateral tax treaty in 2004. The treaty with Canada currently allows IBCs and offshore banking profits to be repatriated to Canada tax-free after paying a much lower tax in Barbados. A Mutual Legal Assistance Treaty (MLAT) and an Extradition Treaty between the United States and the GOB each entered into force in 2000.

Barbados is a member of the Offshore Group of Banking Supervisors, the Caribbean Financial Action Task Force, and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The FIU was admitted to the Egmont Group in 2002. The Barbados Association of Compliance Professionals, along with the Compliance Associations from Trinidad and Tobago, the Bahamas, the Cayman Islands, and the British Virgin Islands, formed the Caribbean Regional Compliance Association in October 2003.

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

Although the GOB has strengthened anti-money laundering legislation, it should consider adopting civil forfeiture and asset sharing legislation. Barbados must steadfastly enforce the laws and regulations it has adopted. The GOB should be more aggressive in conducting examinations of the financial sector and maintaining strict control over vetting and licensing of offshore entities. In 2005, there was a disproportionate number of SARS reported compared to the number of financial institutions. The GOB should ensure adequate supervision of non-governmental organizations and charities. It should also work to improve information sharing between regulatory and enforcement agencies. Additionally, Barbados should continue to provide adequate resources to its law enforcement and prosecutorial personnel, to ensure Mutual Legal Assistance Treaty requests are efficiently processed. The GOB should adequately staff its FIU as a first step toward bolstering its ability to prosecute anti-money laundering cases.

Belarus

Belarus is not a regional financial center. A general lack of transparency in industry and banking sectors makes it difficult to assess the level of or potential for money laundering and other financial crimes. Belarus faces problems with organized crime and therefore is vulnerable to money laundering. Due to inflation, excessively high taxes, and the dollarization of the economy, a significant volume of foreign-currency cash transactions eludes the banking system. Shadow incomes from offshore companies, filtered through small local businesses, constitute a significant portion of foreign investment. Casinos and gambling establishments are prevalent.

Economic decision-making in Belarus is highly concentrated within the top levels of government and has become even more so after the President issued Decree 520 "On Improving Legal Regulation of Certain Economic Relations" in November 2005. This decree gives the president broader powers over

the entire economy—including the power to manage, dispose of, and privatize all state owned property—while taking away authority from Parliament, the National Bank of Belarus, and even market forces. The decree also states that any legislation that contradicts the decree will expire in June 2006. From that date, the president will be above the law when it comes to economic regulation. In addition, by the power of the "golden share rule," government agencies have broad powers to intervene in the management of public and private enterprises, which they often do.

Since the President issued decree 114 "On free economic zones on the territory of the Republic of Belarus" in 1996, Belarus has established six free economic zones (FEZs). The president creates FEZs upon the recommendation of the Council of Ministers and can dissolve or extend the existence of a FEZ at will. The Presidential Administration, the State Control Committee (SCC), and regional and Minsk city authorities supervise the activities of companies in the FEZs. According to the SCC, applying organizations are fully vetted before they are allowed to operate in an FEZ in an effort to prevent money laundering and terrorism finance.

Belarus' "Law on Measures to Prevent the Laundering of Illegally Acquired Proceeds" (AML Law) was amended in 2005. It establishes the legal and organization framework to prevent money laundering and terrorism financing. The measures described in the AML Law apply to all entities that conduct financial transactions in Belarus. Such entities include: bank and non-bank credit and financial institutions; stock and currency exchanges; investment funds and other professional dealers in securities; insurance and reinsurance institutions; dealers' and brokers' offices; notary offices (notaries); casinos and other gambling establishments; pawn shops; and other organizations conducting financial transactions.

The AML Law makes individuals and businesses, government entities, and entities without legal status criminally liable for drug and non-drug related money laundering, although the punishments for laundering money or financing terrorism are not explicitly stated in the law. However, Article 235 of the Belarusian criminal code ("Legalization of illegally acquired proceeds") stipulates that money laundering crimes may be punishable by fine or prison terms of up to ten years. The law defines "illegally acquired proceeds" as money (Belarusian or foreign currency), securities or other assets, including property rights and exclusive rights to intellectual property, obtained in violation of the law.

The AML Law authorizes the following government bodies to monitor financial transactions for the purpose of preventing money laundering: the State Control Committee (Department of Financial Monitoring); the Securities Committee; the Ministry of Finance; the Ministry of Justice; the Ministry of Communications and Information; the Ministry of Sports and Tourism; the Committee on Land Resources; and other state bodies.

In December 2005, Parliament approved a series of amendments to the AML Law to enhance the current legislation on money laundering prevention. The amendments state that individual and corporate financial transactions exceeding approximately $27,000 and $270,000, respectively, are subject to special inspection. The amendments, however, exempt most government transactions and transactions sanctioned by the President from extraordinary inspection.

In January 2005, the President signed a decree on the regulation of the gambling sector. The owners of gambling businesses will be subject to stricter tax regulations. Gamblers will have to produce a passport or other identification in order to receive a money prize, a provision intended to combat money laundering.

The Belarusian banking sector consists of 31 banks. Within this number, 27 have foreign investors and nine banks are foreign owned. The state-owned BelarusBank is the largest and most influential bank in Belarus. Four other state banks and one private bank comprise the majority of the remaining banking activities in the country. In addition, 12 foreign banks have representative offices in Belarus in order to facilitate business cooperation with their Belarusian clients.

In 2003, Belarus established the Department of Financial Monitoring (DFM)—the Belarusian equivalent of a Financial Intelligence Unit—within the State Control Committee and named the DFM as the primary government agency responsible for gathering, monitoring and disseminating financial intelligence. The DFM analyzes information it receives for evidence of money laundering to pass to law enforcement officials for prosecution. The DFM also has the power to penalize those who violate money laundering laws. The DFM cooperates with its counterparts in foreign states and with international organizations to combat money laundering. Belarus' DFM is not a member of the Egmont Group, but it has applied for membership. Russia has agreed to sponsor Belarus' membership and to represent Belarus while the DFM's membership application is pending.

Financial institutions are obligated to register with the DFM transactions subject to special monitoring, such as: transactions whose suspected purpose is money laundering or terrorism finance; cases where the person performing the transaction is a known terrorist or controlled by a known terrorist; cases in which the person performing the transaction is from a state that does not cooperate internationally to prevent money laundering and terrorism financing; and finally, transactions exceeding approximately $27,000 for individuals and $270,000 for businesses that involve cash, property, securities, loans or remittances. Belarusian law stipulates that a one-time transaction that exceeds predetermined amounts for individuals and businesses set by the government must be registered in accordance with the law. If the total value of transactions conducted in one month exceeds the set thresholds and there is reasonable evidence to suggest that the transactions are related, then all the transaction activity must be registered.

Financial institutions conducting transfers subject to special monitoring are required to submit information about such transfers in written form to the DFM within one business day of the reported transaction. Financial institutions should identify the individuals and businesses ordering the transaction or the person on whose behalf the transaction is being placed, disclose information about the beneficiary of a transaction, and provide the account information and document details used in the transaction, including the type of transaction, the name and location of the financial institution conducting the transfer, and the date, time and value of the transfer. The law provides a "safe harbor" for banks and other financial institutions that provide otherwise confidential transaction data to investigating authorities, provided the information is given in accordance with the procedures established by law. Under the State Control Committee (SCC), the Department of Financial Investigations, in conjunction with the Prosecutor General's Office, has the legal authority to investigate suspicious financial transactions.

Failure to register and transmit the required information on financial transactions may subject a bank or other financial institution to criminal liability. The National Bank of Belarus is the relevant monitoring agency for the majority of transactions conducted by banking and other financial institutions. According to the National Bank, information on suspicious transactions should be reported to the Bank's Department of Bank Monitoring. Although the banking code stipulates that the National Bank has primary regulatory authority over the banking sector, in practice, the Presidential Administration exerts significant influence on central and state commercial bank operations, including employment. Any member of the Board of the National Bank may be removed from office by the president with a simple notification to the National Assembly.

Terrorism is a crime in Belarus. The AML Law establishes measures to prevent terrorism finance. Belarus' law on counterterrorism also states that knowingly financing or otherwise assisting a terrorist group constitutes terrorist activity. Under the Belarusian Criminal Code, the willful provision or collection of funds in support of terrorism by nationals of Belarus or persons in its territory constitutes participation in the act of terrorism itself in the form of aiding and abetting. In December 2005, the Belarusian Parliament amended the Criminal Code to stiffen the penalty for the financing of terrorism and thus bring Belarusian regulations into compliance with the International Convention for the Suppression of the Financing of Terrorism. The amendments explicitly define terrorist activities and

terrorism finance and carry an eight to twelve year prison sentence for those found guilty of sponsoring terrorism.

The seizure of funds or assets held in a bank requires a court decision, a decree issued by a body of inquiry or pre-trial investigation, or a decision by the tax authorities. A 2002 directive issued by the Board of Governors of the National Bank prohibits all transactions with accounts belonging to terrorists, terrorist organizations and associated persons. This directive also outlines a process for circulating to banks the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list. The National Bank is required to disseminate to banks the updates to the consolidated list and other information related to terrorist finance as it is received from the Ministry of Foreign Affairs. The directive gives banks the authority to freeze transactions in the accounts of terrorists, terrorist organizations and associated persons. Through 2005, Belarus has not identified any assets as belonging to individuals or entities included on the UNSCR 1267 Sanctions Committee's consolidated list.

Belarus has signed bilateral treaties on law enforcement cooperation with Bulgaria, Lithuania, the People's Republic of China, Poland, Romania, Turkey, the United Kingdom, and Vietnam. Belarus is also a party to five agreements on law enforcement cooperation and information sharing among CIS member states, including the Agreement on Cooperation among CIS Member States in the Fight against Crime and the Agreement on Cooperation among Ministries of Internal Affairs in the Fight against Terrorism. In 2004, Belarus joined the newly organized Eurasian Regional Group (EAG) Against Money Laundering and the Financing of Terrorism, a FATF-style regional body. The EAG has observer status in FATF.

Belarus has acceded to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Belarus is a party to the 1988 UN Drug Convention and twelve of the thirteen conventions on counterterrorism. In 2004, Belarus signed the UN Convention against Corruption. On September 15, 2005, Belarus became a signatory to the UN International Convention for the Suppression of Acts of Nuclear Terrorism. Following that accession and in an effort to promote international cooperation in the fight against terrorism, the lower house of Parliament ratified a bill for the Civil Law Convention on Corruption in December 2005. The bill aims to protect those who suffer from acts of corruption and makes the state or appropriate authority liable to compensate individuals affected by a corrupt official, as well as invalidating all scandalous contract agreements.

The Government of Belarus has taken positive and concrete steps to construct an anti-money laundering and counterterrorist financing regime. Belarus should increase the transparency of its business and banking sectors. It should extend the application of its current anti-money laundering legislation to cover more of the governmental transactions that are currently exempted under the law. It should provide adequate resources to its FIU so that it can operate effectively and further improve the coordination between agencies responsible for enforcing anti-money laundering measures.

Belgium

As a member of the Financial Action Task Force (FATF), Belgium was the subject of a mutual evaluation report in June 2005. The report examined Belgium's efforts to combat money laundering and the financing of terrorism. Belgium was found compliant with most of FATF's Forty Recommendations and Nine Special Recommendations. Efforts are now being made to address weaknesses that were identified in the evaluation.

With strong legislative and oversight provisions in place in the formal financial sector, Belgian officials have noted that criminals are increasing their use of the non-financial professions to facilitate access to the official financial sector. For example, the strong presence of the diamond trade within

Belgium leaves the nation vulnerable to money laundering. Ninety percent of crude diamonds and 50 percent of cut diamonds pass through Belgium. Authorities have transmitted a number of cases relating to diamonds to the public prosecutor, and they are examining the sector closely in cooperation with local police and diamond industry officials. Additionally, the Kimberley certification process (a joint government, international diamond industry, and civil society initiative designed to stem the flow of illicit diamonds) has helped to introduce some much-needed transparency into the global diamond trade.

The Government of Belgium (GOB) recognizes the particular importance of the diamond industry, as well as the potential vulnerabilities it presents to the financial sector. As such, the GOB has distributed typologies outlining its experiences in pursuing money laundering cases involving the diamond trade, especially those involving the trafficking of African conflict diamonds. The Belgian financial intelligence unit (FIU), known in French as Cellule de Traitement des Informations Financières and in Flemish as Cel voor Financiële Informatieverwerking (CTIF-CFI), is active in this area. It has initiated several meetings with the Belgian Ministry of Economic Affairs and the High Council for Diamonds in order to clarify the obligations of diamond traders with respect to anti-money laundering and antiterrorist financing laws. The Belgian FIU also initiated a sector-wide inquiry in order to verify how diamond traders apply this legislation.

Money launderers in Belgium often use notaries to create front companies or buy real estate. Selling property below market value, making significant investments on behalf of foreign nationals with no connections to Belgium, making client property transactions with values disproportionate to the socio-economic status of the client, and creating a large number of companies in a short timeframe are common indicators of money laundering in Belgium. While fraud involving claims for fictitious transactions for value-added tax (VAT) reimbursements has also been of concern, VAT fraud has decreased significantly since 2001 as a result of more aggressive investigation.

A growing problem, according to government officials, is the proliferation of illegal underground banking activities. Beginning in 2004, Belgian police made a series of raids on "phone shops"—small businesses where customers can make inexpensive phone calls and access the Internet. In some phone shops, authorities uncovered money laundering operations and hawala-type banking activities. Authorities believe that approximately 5,000-6,000 phone shops are operating in Belgium. Just 1,500 of these shops are formally licensed, and Belgian authorities are considering enforcing a stricter licensing regime. Some Brussels communes have also proposed heavy taxes on these types of shops in an effort to dissuade illegitimate commerce.

Money laundering in Belgium is illegal through the Law of January 11, 1993, "On Preventing Use of the Financial System for Purposes of Money Laundering." It is criminalized by Article 505 of the Penal Code, which sets penalties of up to five years' imprisonment. In January 2004, Belgian domestic legislation implementing Council Directive 2001/97/EC on prevention of the use of the financial system for money laundering (2nd EU Money Laundering Directive) entered into force, broadening the scope of money laundering predicate offenses beyond drug-trafficking to include the financing of terrorist acts or organizations.

For the purposes of money laundering and terrorist financing, Belgian financial institutions are supervised by the Belgian Banking and Finance Commission (CBFA), which also supervises exchange houses, stock brokerages, and insurance companies. The Belgian Gaming Commission oversees casinos, and CTIF-CFI oversees some professions not supervised by CBFA or other authorities.

Belgian law mandates reporting of suspicious transactions by a wide variety of financial institutions and non-financial entities, including notaries, accountants, bailiffs, real estate agents, casinos, cash transporters, external tax consultants, certified accountant-tax experts, and lawyers. An association of Belgian lawyers has appealed the law to Belgium's court of arbitration on the grounds that it violates

basic principles of the independence of the lawyer and of professional secrecy. A decision from the court of arbitration is pending.

The January 2004 legislation imposes prohibitions on cash payments for real estate, except for an amount not exceeding 10 percent of the purchase price or 15,000 euros (approximately $17,700), whichever is lower. Cash payments over 15,000 euros for goods are also illegal.

Entities with reporting obligations must also submit to the FIU information on transactions involving individuals or legal entities domiciled, registered, or established in a country or territory for which FATF has recommended countermeasures. A law passed on May 3, 2002, gives the GOB the authority to invoke countermeasures against countries or territories included on the FATF list of non-cooperative countries and territories (the NCCT List) The FIU regularly submits the NCCT List to its financial institutions.

Belgian financial institutions are required to comply with "know your customer" principles, regardless of the transaction amount. Institutions must maintain records on the identities of clients engaged in transactions that are considered suspicious, or that involve an amount equal to or greater than 10,000 euros (approximately $11,790). During the summer of 2005, Fortis Bank blocked 150,000 accounts in Belgium due to insufficient customer identifiers. Records of suspicious transactions that are required to be reported to the FIU must be kept for at least five years.

Financial institutions are required to train their personnel in the detection and handling of suspicious transactions that could be linked to money laundering. Financial institutions or other entities with reporting requirements are also liable for illegal activities occurring under their control. Failure to comply with the anti-money laundering legislation, including failure to report, is punishable by a fine of up to 1.25 million euros (approximately $1.47 million).

The financial sector cooperates actively with CTIF-CFI to guard against illegal activity. No civil, penal, or disciplinary actions can be taken against institutions, or their employees or representatives, for reporting transactions in good faith to CTIF-CFI. Legislation also exists to protect witnesses, including bank employees, who report suspicions of money laundering or who come forward with information about money laundering crimes. Belgian officials have imposed sanctions on institutions or individuals that knowingly permitted illegal activities to occur.

Belgium had long permitted the issuance of bearer bonds ("titres au porteur"), widely used to transfer wealth between generations and to avoid taxes. In late 2005 the Belgian federal parliament adopted a law to phase out bearer bonds by 2008.

Currently, Belgium has no reporting requirements on cross-border currency movements. In October 2005, the European Parliament and Council of the European Union issued Regulation (EC) No 1889/2005 on controls of cash entering or leaving the Community. Belgium is required to implement this regulation by June 15, 2007.

November 2005 was also marked by the issuance of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (3rd EU Money Laundering Directive), which EU member states, including Belgium, must implement by December 15, 2007. In another recent EU-wide initiative, the European Commission launched a consultation on the single European payments area. Stakeholder input is being sought to address a licensing/registration regime for alternative remittances. The Commission may introduce draft legislation on this topic sometime in 2006. As for non-profit organizations, the European Commission adopted a communication on non-profit organizations on November 29, 2005. This communication includes recommendations for EU member states and a framework for a code of conduct for the sector.

Belgium's FIU, CTIF-CFI, was created in 1993. CTIF-CFI's mission is to receive and analyze all suspicious transaction reports submitted by regulated entities. Operating as a filter between these

subjects and judicial authorities, CTIF-CFI reports possible money laundering or terrorist financing transactions to the public prosecutor. The FIU is an autonomous and independent public administrative authority, supervised by the Ministries of Justice and Finance. Institutions and persons subject to the reporting obligations fund the FIU. Although these contributions are compulsory, the contributing entities do not exercise any formal control over the FIU.

In terms of personnel, the CTIF-CFI is composed of eight financial experts, including three magistrates (public prosecutors) appointed by the King. A magistrate presides over the body. Terms of service are for six years and may be renewed. Decisions are taken on a majority basis, with the President of the unit holding the power to break a tie. In addition to 20 staff members providing administrative and legal support, the investigative department consists of 11 inspectors/analysts. There are also three liaison police officers, one customs officer, and one officer of the Belgian intelligence service who maintain contacts with the various law enforcement agencies in Belgium.

From its founding in 1993 until the end of 2004, the CTIF-CFI had received 94,389 disclosures and has transmitted 6,430 cases to the public prosecutor aggregating 11.7 billion euros (approximately $13.8 billion). In 2004, the FIU opened 3,163 new cases and transmitted 664 cases to the public prosecutor, down from 783 cases in 2003. A majority of the notifications generating these cases resulted from disclosures made by banks and foreign exchange offices, with less than 3 percent of notifications originating from non-financial institutions.

Belgium's FIU and federal police both transmit suspected money laundering cases to the public prosecutor. In 2004, the federal police transmitted a total of 1,815 cases to the public prosecutor. The main offenses were: narcotics (31 percent); trafficking in persons (15 percent); money laundering, fraud, and corruption (14 percent); organized crime (13 percent); armed robbery (12 percent); and vehicle theft (11 percent). Terrorism cases accounted for just over one percent of all cases forwarded to the public prosecutor by federal police.

Under Belgium's 1993 anti-money laundering and terrorist finance law (most recently amended in 2004), bank accounts can be frozen on a case-by-case basis if there is sufficient evidence that a money laundering crime has been committed. The FIU has the legal authority to suspend a transaction for a period of up to two working days in order to complete its analysis. If criminal evidence exists, the FIU forwards the case to the public prosecutor. In 2004, CTIF-CFI temporarily froze assets in 32 cases, representing 112.34 million euros (approximately $132 million).

In 2004, the federal police created a terrorist financing unit within its economic crimes department, ECOFIN. Subsequently the ECOFIN personnel were transferred to the federal police's counterterrorism department. The federal police enjoy good cross-border cooperation with other police and investigative services. The federal police and the specialized services of the Central Office for the Fight against Organized Economic and Financial Crimes utilize a number of tactics to uncover money laundering operations, including investigating significant capital injections into businesses, examining suspicious real estate transactions, and conducting random searches at all international airports. In 2004, Project Cash Watch, carried out under the auspices of the federal police at international airports and other transit venues, netted seizures of more than 1.1 million euros (approximately $1.3 million) at Belgian airports and 241,042 euros (approximately $284,067) in other locations.

Since the creation of CTIF-CFI in 1993, Belgian courts have convicted 1,085 individuals for money laundering on the basis of cases forwarded by the FIU. These convictions have yielded combined total sentences of 2,248 years and combined total fines of 29.82 million euros (approximately $35 million). Belgian authorities have confiscated more than 517 million euros (approximately $609 million) connected with money laundering crimes. The majority of convictions in relation to money laundering are based upon disclosures made by the financial institutions and others to CTIF-CFI.

In January 2004, the Belgian legislature passed domestic legislation implementing the EU Council's Framework Decision on Combating Terrorism, which criminalizes terrorist acts and material support (including financial support) for terrorist acts, allowing judicial freezes on terrorist assets. The Ministry of Finance can administratively freeze assets of individuals and entities associated with Al Qaeda, the Taliban and Usama Bin Laden on the UN 1267 Sanctions Committee's consolidated list and/or is covered by an EU asset freeze regulation. Seized assets are transferred to the Ministry of Finance. If an entity appears on the UN 1267 Sanctions Committee's consolidated list, but not on the EU list, then the GOB can pass a ministerial decree to freeze assets in order to comply with the UN requirement. Assets of entities appearing on the EU list are automatically subject to a freeze without additional legislative or executive procedures. However, Belgium lacks the legislation to administratively freeze terrorist assets in the absence of a judicial order or UN or EU designation. Belgian officials have noted that modifications in the legislation are underway in order to allow Belgium to establish a national freezing mechanism for assets related to terrorism.

Under the 2004 law, the Ministry of Justice can freeze assets related to terrorist crimes. However, the burden of proof in such cases is relatively high. In order for an act to constitute a criminal offense, authorities must demonstrate that the support was given with the knowledge that it would contribute to the commission of a crime by the terrorist group. Further, as the law does not establish a national capacity for designating foreign terrorist organizations, Belgian authorities must demonstrate in each case that the group that was lent support actually constitutes a terrorist group.

Belgium is a party to the 1988 UN Drug Convention, and in August 2004, the GOB ratified the UN Convention against Transnational Organized Crime. Belgium has signed, but not yet ratified, the UN Convention against Corruption. In 2001, Belgium became a party to the UN Convention for the Suppression of the Financing of Terrorism. A mutual legal assistance treaty between Belgium and the United States has been in force since May 2000. An extradition treaty between Belgium and the United States has been in force since September 1997. Bilateral instruments amending and supplementing these treaties, in implementation of the U.S.-EU Extradition and Mutual Assistance Agreements, were signed with Belgium in December 2004. Belgium's FIU is active among its European colleagues in sharing information. CTIF-CFI and its U.S. counterpart, FinCEN, have signed a memorandum of understanding that governs their collaborative work. CTIF-CFI heads the secretariat of the Egmont Group from 2005 to 2006.

With the January 2004 anti-money laundering legislation, Belgium has a strong anti-money laundering regime. The Government of Belgium should continue to pursue a tougher and faster independent asset-freezing capability. One obstacle is a widespread perception that once a person is placed on a UN or EU terrorist financing list, it is difficult to remove him from the list.

The Government of Belgium should continue to exert vigilance with regard to uncovering, investigating, and prosecuting illegal banking operations related to its diamond sector. Similar attention should be paid to the informal financial sector and non-bank financial institutions. Belgium should also institute stringent reporting requirements for cross-border currency movements. Finally, Belgium may need to devote more resources, including investigative personnel, to key Belgian agencies that work on money laundering, terrorist financing, and other financial crimes.

Belize

Belize is not a major regional financial center. In an attempt to diversify Belize's economic activities, authorities have encouraged the growth of offshore financial activities and have pegged the Belizean dollar to the U.S. dollar. Belize continues to offer financial and corporate services to nonresidents. Presently, there are eight licensed offshore banks, approximately 38,471 registered international business companies (IBCs), one licensed offshore insurance company and one mutual fund company operating in Belize.

Currently, there are 23 trust companies and agents operating in Belize, and there are also a number of undisclosed Internet gaming sites operating from within the country. These gaming sites are currently unregulated. Currently there are no offshore casinos operating from within Belize. Belizean officials suspect that money laundering occurs primarily within the country's offshore financial sector. The local casas de cambios (money exchange houses), which were suspected of money laundering, were closed effective July 11, 2005. Money laundering, primarily related to narcotics trafficking and contraband smuggling, also occurs through banks operating in Belize. Criminal proceeds laundered in Belize are derived primarily from foreign criminal activities. There is no evidence to indicate that money laundering proceeds are primarily controlled by local drug-trafficking organizations, organized criminals or terrorist groups. Allegedly, there is a significant black market for smuggled goods in Belize. However, there is no evidence to indicate that the smuggled goods are significantly funded by narcotics proceeds, or evidence to indicate significant narcotic-related money laundering. The funds generated from contraband are undetermined. Belizean officials have reported an increase in financial crimes, such as bank fraud, cashing of forged checks, and counterfeit Belizean and United States currency. The Central Bank of Belize has engaged in public awareness activities and trainings to regulate counterfeit currency.

There is one free trade zone presently operating in Belize, at the border with Southern Mexico. There are designated free trade zones in Punta Gorda, Belize City, and Benques Viego, but they are not operational. Data Pro Ltd. is designated as an Export Processing Zone (EPZ) and is regulated in accordance with the EPZ Act, Chapter 278, and revised edition 2000. Commercial Free Zone (CFZ) businesses are allowed to conduct business within the confines of the CFZ provided they have been approved by the Commercial Free Zone Management Agency (CFZMA) to engage in business activities. All merchandise, articles, or other goods entering the CFZ for commercial purposes are exempted from the national customs regime. However, any trade with the national customs territory of Belize is subject to the national Customs and Excise law. The CFZMA is the supervisory authority of the free zone. The CFZMA, in collaboration with the Customs Department and the Central Bank of Belize, monitors the operations of CFZ business activities. The Commercial Free Zone Act, Chapter 278 of the Laws of Belize, prescribes the establishment, functioning, and responsibilities of the CFZMA. There is no indication that the CFZ is presently being used in trade-based money laundering schemes or by the financiers of terrorism.

The Money Laundering (Prevention) Act (MLPA), in force since 1996, criminalizes money laundering related to many serious crimes, including drug-trafficking, forgery, terrorism, blackmail, arms trafficking, kidnapping, fraud, illegal deposit taking, false accounting, counterfeiting, extortion, robbery, and theft. The minimum penalty for a money laundering offense as defined by the MLPA is three years imprisonment. Additional legislation has been enacted to discourage individuals from engaging in money laundering, and there have been two arrests for money laundering in 2005. The effectiveness of the anti-money laundering regime in Belize remains unclear.

Offshore banks, international business companies and trusts are authorized to operate from within Belize, although shell banks are prohibited within the jurisdiction. The Offshore Banking Act, 1996 governs activities of Belize's offshore banks.

The Central Bank of Belize supervises and examines financial institutions for compliance with anti-money laundering/counterfinancing of terrorism laws and regulations. The banking regulations governing offshore banks are different from the domestic banking regulations in terms of capital requirements. Banks are not permitted to issue bearer shares. Nevertheless, all licensed financial institutions in Belize (onshore and offshore) are governed by the same anti-money laundering legislation and must adhere to the same anti-money laundering requirements. To legally operate from within Belize all offshore banks must be licensed by the Central Bank and be registered with IBCs. Before the Central Bank issues the license, the Central Bank must verify shareholders' and directors' backgrounds, ensure the adequacy of capital, and review the bank's business plan. The legislation

governing the licensing of offshore banks does not permit directors to act in a nominee (anonymous) capacity.

The International Business Companies Act of 1990 and its 1995 and 1999 amendments govern the operation of IBCs. The 1999 amendment to the Act allows IBCs to operate as banks and insurance companies. The International Financial Services Commission regulates the rest of the offshore sector. All IBCs must be registered. Registered agents of IBCs must satisfy the International Financial Services Commission that they conduct due diligence background checks before IBCs are allowed to register. Although IBCs are allowed to issue bearer shares, the registered agents of such companies, must know the identity of the beneficial owners of the bearer shares. In addition, registered agents must satisfy certain criteria to obtain licenses in order to perform offshore services. Belize's legislation on IBCs allows for the appointment of nominee directors. The legislation for trust companies, the Belize Trust Act, 1992, is not as stringent as the legislation for other offshore financial services and does not preclude the appointment of nominee trustees.

The Central Bank issued Supporting Regulations and Guidance Notes in 1998. Licensed banks and financial institutions are required to know their customers. Furthermore, Belizean laws require that licensed banks and financial institutions are required to monitor their customers' activities and report any suspicious transaction to the Financial Intelligence Unit (FIU). Belize law obligates banks and other financial institutions to maintain records of all large currency transactions for at least five years. Money laundering controls are applicable to non-bank financial institutions such as exchange houses, insurance companies, lawyers, and accountants. The International Financial Services Commission regulates such entities for compliance. An important exception is that of casinos. Financial institution employees are exempted from civil, criminal, or administrative liability for cooperating with regulators and law enforcement authorities in investigating money laundering or other financial crimes.

Belize does not have any bank secrecy legislation that prevents disclosure of client and ownership information. There is no impediment preventing authorities from obtaining information pertaining to financial crimes. Also, the reporting of all cross-border currency movement is mandatory. All individuals entering or departing Belize with more than BZ $20,000 ($10,000) in cash or negotiable instruments, are required to file a declaration with the authorities at the Customs, the Central Bank and the FIU.

As of September 30, 2005, the FIU had received 33 Suspicious Transaction Reports (STRs). Of the 33 STRs filed, 26 became the subject of investigations.

Current laws provide for the establishment of a FIU but not for funding of the same. The FIU has to apply to the Ministry of Finance for funds. The funding allocated to the FIU for fiscal year 2005 was BZ$400,000 ($200,000). Due to financial constraints, the FIU is not adequately staffed and the existing staff lacks sufficient training and experience. On November 5, 2005 the director of the FIU resigned, leaving the FIU with only four employees. The Director of the Public Prosecutions Office and the Belizean Police Department are responsible for investigating all crimes. However, the FIU is specifically in charge of financial crimes investigations, including money laundering and the financing of terrorism.

The FIU has access to records and databanks of other government entities and financial institutions. There are no formal mechanisms for the sharing of information with domestic regulatory and law enforcement agencies. The FIU is empowered to share information with FIUs in other countries.

Belize criminalized terrorist financing via amendments to its anti-money laundering legislation (The Money Laundering (Prevention) (Amendment) Act, 2002). Belizean authorities have circulated to all banks and financial institutions in Belize the names of suspected terrorists and terrorist organizations

listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224.

There are no indications that charitable and/or non-profit entities in Belize have acted as conduits for the financing of terrorist activities. Consequently, the country has not taken any measures to prevent the misuse of charitable and non-profit entities from aiding in the financing of terrorist activities. Belize has signed the UN International Convention for the Suppression of the Financing of Terrorism.

Belizean authorities acknowledge the existence and use of indigenous alternative remittance systems that bypass, in whole or part, financial institutions. Such systems are illegal in Belize. However, Belizean authorities, aware of illegal remittances, monitor such activities at both the border with Mexico and Guatemala.

Belizean law makes no distinctions between civil and criminal forfeitures. All forfeitures resulting from money laundering are treated as criminal forfeitures. The banking community cooperates fully with enforcement efforts to trace funds and seize assets. The FIU and the Belize Police Department are the entities responsible for tracing, seizing, and freezing assets. Currently, Belize's legislation does not specify the length of time assets can be frozen. The Ministry of Finance can confiscate frozen assets. With prior court approval, Belizean authorities have the power to identify, freeze, and seize terrorist finance or money laundering related assets. This includes vehicles, vessels, aircraft, and other means of transportation or communication. It would also include any property, tangible or intangible, which may be related to money laundering or is shown to be from the proceeds of money laundering, including legitimate businesses. There are no limitations to the kinds of property that may be seized, and all seized items become the property of the Government of Belize. However, law enforcement lacks the resources necessary to trace and seize assets. The Misuse of Drugs Act (MDA) has provisions for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets. The Director of the Public Prosecutions Office and the Belize Police Department are the agencies responsible for enforcing the MDA. New legislation is currently being considered to strengthen the appropriate provisions for identifying, tracing freezing, seizing and forfeiting narcotics-related assets.

The authorities are considering the enactment of a Proceeds of Crime law, which will address the seizure or forfeiture of assets of narcotics traffickers, financiers of terrorism, or organized crime. The Belize Police Department reported that during the past year, the dollar amount of assets forfeited and/or seized amounted to just over BZ$240,000 (approximately $120,000). Assets forfeited and/or seized in 2004 totaled BZ$16,664,850 (approximately $8,332,425).

No laws have been enacted specifically for the sharing of seized narcotics assets, or of proceeds of other serious crimes, including the financing of terrorism. However, the Government of Belize actively cooperates with the efforts of foreign governments to trace or seize assets relating to financial crimes.

Belize has signed a Mutual Legal Assistance Treaty, which provides for mutual legal assistance in criminal matters with the United States. Amendments to the MLPA preclude the necessity of a Mutual Legal Assistance Treaty for exchanging information or providing judicial and legal assistance in matters pertaining to money laundering and other financial crimes to authorities of other jurisdictions. On several occasions, the FIU has cooperated with the United States Department of Justice, the Financial Crimes Enforcement Network (FinCEN), the Federal Bureau of Investigation (FBI), the Internal Revenue Service (IRS), the Drug Enforcement Administration (DEA), and the Food and Drug Administration (FDA).

Belize is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention. Belize is also a member of the Organization of American States (OAS) and its FIU is a member of the Egmont Group.

The Government of Belize should increase resources to law enforcement and should provide adequate training to those responsible for enforcing both Belize's anti-money laundering/counterterrorist financing laws and its asset forfeiture regime. Belize should take steps to address the vulnerabilities in its supervision of its offshore sector, particularly the lack of supervision of the gaming sector, including Internet gaming facilities. Belize should immobilize bearer shares and mandate suspicious activity reporting for the offshore financial sector.

Bermuda

An overseas territory of the United Kingdom (UK), Bermuda is a major offshore financial center, and has a strong reputation internationally for the integrity of its financial regulatory system. The Government of Bermuda (GOB) cooperates with the United States and the international community to counter money laundering and terrorist financing, and continues to update its legislation and procedures in conformance with international standards. In March 2003, Bermuda welcomed the external review of offshore financial centers by the International Monetary Fund (IMF), published in early 2005. Overall, the report was positive about the Government of Bermuda's (GOB) implementation of financial regulations and anti-money laundering procedures, although it did identify a number of areas requiring action. Many of those points have since been addressed through legislation, and the GOB has committed to introducing additional amendments to address the remaining issues.

As of June 30, 2005, records indicate that 13,996 international businesses were registered in Bermuda, compared to 3,072 local companies. The majority of international businesses (12,768) are exempted companies, which means they are exempt from Bermuda laws that apply to local entities including the restriction that at least 60 percent of local entities must be owned by Bermudan residents. Like local companies, an exempt company is not subject to currency controls or capital controls and is free from all forms of direct taxation on income and capital gains. Therefore, exempt companies are normally prohibited from doing business in the local economy. In addition, there are 612 exempted partnerships, 596 nonresident international companies (incorporated elsewhere to do business in Bermuda), and 19 nonresident insurance companies. These businesses operate in a fashion similar to and are subject to the same rules as an exempt company. The majority of Bermuda's exempt companies are shell companies with no physical presence on the island. Local directors (generally a local lawyer and secretary) are designated to manage corporate affairs in Bermuda. Before exempted companies can be established or any shares transferred between nonresidents, the owners and controllers must be vetted by the Bermuda Monetary Authority (BMA), the sole regulatory body for financial services.

As of December 2005, Bermuda has 1,421 international insurers and reinsurers; 1,031 of those are captive insurance companies. The term "captive" refers to companies formed primarily to insure the risks of their parent companies or affiliates. The United States is the biggest single source of captive business for Bermuda, accounting for 63 percent of the island's insurance formations. There are also 1,031 mutual fund companies, and 21 unit trusts in Bermuda. There are 4 banks in Bermuda; offshore banking is not permitted. There are no free trade zones in Bermuda.

The GOB first passed specific money laundering legislation in 1997, enacting the Proceeds of Crime Act (PCA) to apply money laundering controls to financial institutions such as banks, deposit companies, and trust companies. Subsequent amendments added investment businesses, including broker-dealers and investment managers to the list. Amendments in 2000 expanded the scope of the legislation to cover the proceeds of all indictable offenses. The PCA established the National Anti-Money Laundering Committee (NAMLC) for the purpose of advising the Minister of Finance on efforts to combat money laundering domestically and internationally, as well as to issue Guidance Notes. The committee is comprised of government officials from the Ministry of Finance, the Ministry of Labor, Home Affairs and Public Safety, Attorney General's Chambers, Department of Public

Prosecutions, Her Majesty's Customs, Registrar of Companies, Bermuda Monetary Authority, and the Bermuda Police Service-Financial Investigation Unit (FIU). The NAMLC revised the guidance notes and it is expected that the notes, along with amendments to the PCA and the PCA Regulations, will become effective in 2006. The amendments broaden the scope of the PCA regulations to include gatekeepers such as lawyers and accountants.

The PCA includes "know your customer" (KYC) requirements and provides for the monitoring of accounts for suspicious activity. Furthermore, Bermuda performs due diligence on persons seeking to undertake business on the island. The vetting process is undertaken when an entity is incorporated. A personal declaration form must be submitted for beneficial owners of international businesses prior to incorporation. Similar requirements apply to proposals to transfer shares. Additionally, a company must detail its business plan and maintain a register of shareholders at its registered office.

The Bermuda Monetary Authority (BMA) is the sole regulatory body for financial services and is responsible for the licensing, supervision, and regulation of financial institutions including those conducting deposit-taking, insurance, investment and trust business in Bermuda. The BMA Amendment Act 2002 formalized the BMA's responsibilities to include assisting with the detection and prevention of financial crime. The BMA conducts on-site reviews and detailed compliance testing of financial institutions' anti-money laundering controls. The BMA engages in active perimeter policing responsibilities and has legal powers to undertake investigations of unlicensed persons suspected of breaching the regulations, although the BMA has not found it necessary to use these legal powers extensively.

The Banks and Deposit Companies Act 1999 implements the Core Principles for Effective Banking Supervision issued by the Basel Committee. Banks and other financial institutions are required to retain records for a minimum of five years. Bermuda has not adopted bank secrecy laws, but like the UK, recognizes a banker's common-law duty of client confidentiality. Bankers and others are protected by law with respect to their cooperation with law enforcement officials. The Insurance Amendment Act 2004 implemented a number of changes to Bermuda's insurance regime pursuant to the International Association of Insurance Supervisors' (IAIS) adoption of revised core principles for supervision, as well as to the comments made by the IMF in their report on Bermuda's insurance provisions. A further series of more substantive amendments to the Insurance Act is currently in preparation and expected to be introduced into Parliament in the spring of 2006, which should complete the overhaul of the island's insurance legislation, consistent with new international standards for this sector.

The amended Investment Business Act 2003 enhances the regulatory powers of the BMA through stronger intervention powers and clarifying certain provisions, such as the BMA's ability to cooperate with foreign regulatory bodies. Other provisions include measures to strengthen criminal and regulatory penalties. The Act also brought the Bermuda Stock Exchange (BSX) under the regulation of the BMA. In 2004 provisions were added to the Criminal Code Amendment Act to create specific offenses of insider trading and market manipulation in securities markets. Fines up to $100,000 and prison terms of five years are in place for market manipulation and up to $175,000 and seven years jail time for insider trading. These provisions are in addition to existing regulations of the Bermuda Stock Exchange (BSX) that prohibit members from insider trading and market manipulation, on penalty of sanctions, including expulsion from the BSX.

Collective investment schemes (CISs) are regulated by the BMA, and fund administrators are regulated persons for the purposes of the PCA. To strengthen regulation, CISs, including hedge funds, will be the subject of new legislation anticipated for the spring 2006 session of Parliament. The proposed legislation will expand the definition of collective investment schemes to include, in addition to mutual funds and unit trusts, other business vehicles that pool and manage investment monies. It will require the licensing of fund administrators to be subject to minimum standards and a code of

practice. The BMA will also be able to conduct compliance checks of PCA procedures as carried out by CIS administrators. However, the BMA will continue to apply differentiated requirements involving lighter regulation of schemes catering to institutional and sophisticated investors, with greater reliance on transparency and disclosure.

The Bermuda Police Service's Financial Investigation Unit (FIU) serves as the island's financial intelligence unit. The FIU's mandate includes including criminal tax investigations. The FIU is the designated recipient of suspicious activity reports (SARs). In the past, the majority of SARs were related primarily to conversion of suspected local drug profits to U.S. dollars via the island's Western Union money transmission service, which ceased operations in Bermuda on October 31, 2002. Because Bermuda law requires money transmission services to be conducted in association with a licensed deposit-taker, conversion of funds is subject to bank reporting standards. SAR statistics reflect the closure of Western Union: In 2001, 2,827 SARs were filed with the FIU, decreasing to 2,570 in 2002, 275 in 2003, and 162 in 2004. The downward trend reversed in 2005 with 181 SARs posted through mid-December. From 2001-2003 a total of 16 arrests were made on money laundering charges; however, Bermuda's first and only money laundering conviction was prosecuted in 2004. Involving $136,000, the conviction resulted in an 18-month suspended sentence due to mitigating circumstances. Ten arrests were made in 2005 for money laundering.

The PCA establishes procedures for identifying, tracing, and freezing the proceeds of narcotics trafficking and other indictable offenses, including money laundering, tax evasion, corruption, fraud, counterfeiting, stealing, and forgery. Additionally, the PCA provides for forfeiture upon criminal conviction if it is proven that benefit was gained from a criminal act. Under the PCA, there is no provision for seizure of physical assets unless intercepted leaving the island. However, the Supreme Court may issue a confiscation order pursuant to which the convicted person must satisfy a monetary obligation. The amount paid is placed into the Confiscated Assets Fund and may be shared with other jurisdictions at the direction of the Minister of Finance. Under the Misuse of Drugs Act, physical assets can be seized if used at the time the offense was committed. During 2004, the courts issued two successful confiscation orders, for a total amount of $52,335. Forfeitures under the Misuse of Drugs Act are holding steady, with six forfeitures in 2004 amounting to $17,529, compared to the $13,908 forfeited in three separate 2003 cases. Cash seized in 2004 under PCA detention orders exceeded $56,600, and in 2005 there were two cash seizures worth $57,761; both 2004 and 2005 represented a considerable a drop from the $173,000 seized in 2003. Three restraining orders still in place from 2003/2004 are valued at approximately $1.5 million. One new restraining order was issued in 2005 for approximately $621,000. Three cash seizures from 2004 were forfeited under the PCA during 2005 amounting to $47,561.

The Bermuda Police Service, through the FIU and the courts, enforces existing drug-related asset tracing/seizure/forfeiture laws. The PCA will likely be amended in 2006 to strengthen measures to detect/monitor cross-border transportation of cash. At present, the PCA provides for the seizure of cash imported into and exported from Bermuda believed to be the proceeds of criminal activity. Proposed amendments will address cash movements not attributable to criminal activity. Other amendments will widen mandatory reporting requirements relating to the suspicion of money laundering, to cover gatekeepers, such as attorneys and accountants. Currently, if there are reasonable grounds for suspicion, Her Majesty's Customs is authorized to seize cash and instruments; monies can also be seized if travelers fail to report the transportation of cash in excess of $10,000.

The Criminal Justice (International Co-Operation) (Bermuda) Act 1994, as amended in 1996, authorizes the provision of assistance to foreign entities upon their request in connection with foreign criminal proceedings, including securing of evidence in Bermuda and overseas. The BMA Amendment (No. 3) Act 2004 clarifies the power of the BMA to cooperate with other overseas authorities. Its passage follows challenges in Bermuda courts on a specific case in which the BMA was assisting the U.S. Securities and Exchange Commission. Other Bermuda laws also authorize the

sharing of information with overseas regulators: the Banks and Deposit Companies Act 1999, the Trusts (Regulation of Trust Business) Act 2001 and the Investment Business Act 2003.

Bermuda is a member of the Caribbean Financial Action Task Force (CFATF), and its FIU is a member of the Egmont Group. Bermuda is also a member of regulatory standard-setting bodies for banking, insurance and investment business. Through the UK by extension, Bermuda is a party to the 1988 UN Drug Convention and the U.S./UK Extradition Treaty. The GOB enacted the Anti-Terrorism (Financial and Other Measures) Act 2004 that introduced specific provisions criminalizing terrorist financing and provided the framework to ensure implementation of the FATF Special Recommendations on Terrorist Financing. It makes it an offense to raise funds for terrorism, creates specific offenses relating to the raising, use, or possession of funds for purposes of terrorism, imposes a duty to report suspicious activity, and provides for the forfeiture of terrorist cash. The effect is to parallel the provisions already in place under the PCA for money laundering and the proceeds of other serious crimes. Financial institutions had previously been asked to conduct full reviews of their clients against officially published lists of terrorist suspects. There has been no known identified evidence of terrorist financing in Bermuda.

The Government of Bermuda should continue its efforts to update its financial services legislation relating to anti-money laundering and counterterrorism. It should also enact the proposed measures to strengthen provisions relating to the cross-border transportation of cash and monetary instruments and to include gatekeepers, such as accountants and attorneys, as covered entities under its anti-money laundering laws.

Bolivia

Bolivia is not an important regional financial center, but it occupies a geographically significant position in the heart of South America. Bolivia is a major drug producing and drug-transit country. Most money laundering in Bolivia is related to public corruption, contraband smuggling, and narcotics trafficking. Bolivia's long tradition of bank secrecy and the lack of a government entity with effective oversight of non-bank financial activities facilitate the laundering of the profits of organized crime and narcotics trafficking, the evasion of taxes, and laundering of other illegally obtained earnings.

Bolivia's anti-money laundering regime is based on Law 1768 of 1997. Law 1768 modifies the penal code; criminalizes money laundering related only to narcotics trafficking, organized criminal activities and public corruption; provides for a penalty of one to six years for money laundering; and defines the use of asset seizure beyond drug-related offenses. Law 1768 also created Bolivia's financial intelligence unit, the Unidad de Investigaciones Financieras (UIF), within the Office of the Superintendence of Banks and Financial Institutions. The attributions and functions of the unit are defined under Supreme Decree 24771.

Although Law 1768 established the UIF as an administrative financial intelligence unit in 1997, the UIF did not become operational until July 1999. The UIF currently has more than 20 staff members, including the director. The director of the UIF is not a political appointee. The Superintendence of Banks and the Superintendence of Securities and Insurance elect the director to his/her position for a five-year term. The director can only be re-elected once. In January 2004, the term of the UIF's first director ended; he was not re-elected, and the UIF's second director took over the operations of the UIF in February 2004.

The UIF is responsible for collecting and analyzing data on suspected money laundering and other financial crimes, forwarding cases that warrant further information to the Public Ministry, and requesting specific information from the financial sector on behalf of the Public Ministry prosecutors. Under Decree 24771, obligated entities—which include banks, insurance companies and securities brokers—are required to identify their customers, retain records of transactions for a minimum of ten

years, and report to the UIF all transactions that are considered unusual (without apparent economic justification or licit purpose) or suspicious (customer refuses to provide information or the explanation and/or documents presented are clearly inconsistent or incorrect). Under the current law, there is no requirement for obligated entities to report cash transactions above a certain threshold, as is commonplace in many countries' anti-money laundering regimes. Although by law Bolivian Customs is permitted to share information with the UIF regarding the movement of currency into or out of Bolivia, it generally does not do so.

After analyzing suspicious transaction reports and any other relevant information it may receive, the UIF reports all detected criminal activity to the Public Ministry. The UIF also has the ability to request additional information from obligated financial institutions in order to assist the prosecutors of the Public Ministry with their investigations. In 2005 the UIF received 45 reports of suspicious or unusual transactions and sent seven cases to the Public Ministry for further investigation. The UIF is also responsible for implementing anti-money laundering controls, and may request that the Superintendence of Banks sanction obligated institutions for noncompliance with reporting requirements. In 2004, the UIF began on-site inspections of obligated entities in order to review their compliance with the reporting of suspicious transactions.

In 2002, the Special Group for Investigation of Economic Financial Affairs (GIAEF) was created within Bolivia's Special Counter-Narcotics Force (FELCN) to investigate narcotics-related money laundering. The UIF, the Public Ministry, the National Police, and FELCN have established mechanisms for the exchange and coordination of information, including formal exchange of bank secrecy information. The full range of possibilities inherent in this mechanism has yet to be exploited.

Corruption is a serious issue in Bolivia. Traditionally, allegations against high-ranking law enforcement officials were routinely dismissed or forgotten. However, recently created anticorruption task forces have increased the effectiveness of investigations and prosecutions, and the number of convictions related to the crime of corruption is growing. For instance, several major convictions occurred in December 2004: three high-ranking police officials and one judge were convicted on charges related to narcotics trafficking and consorting with narcotics traffickers. In the case of the convicted judge, a report created in part by the UIF detailing financial transactions related to the case led to the formal charges.

In spite of advances in combating money laundering, Bolivia's anti-money laundering system still has many weaknesses. In spite of recommendations by both the International Monetary Fund (IMF) and the Financial Action Task Force for South America (GAFISUD), the Government of Bolivia (GOB) has done little to strengthen the UIF. Limitations in its reach and weaknesses in its basic legal and regulatory framework continue to hamper the UIF's effectiveness as a financial intelligence unit. The GOB's anti-money laundering regime is also undermined by the lack of support—both legal and bureaucratic—for money laundering investigations carried out by law enforcement officials. In order to prosecute a money laundering case, Bolivian law requires that the crime of money laundering be tied to an underlying illicit activity. At present, the list of these underlying crimes is extremely restrictive and inhibits money laundering prosecution. Although the Public Ministry is the office responsible for prosecuting money laundering offenses, it does not have a specialized unit dedicated to the prosecution of these cases. Judges trying these cases are challenged to understand their complexities. To date, there has been only one conviction that involved money laundering. The case is under appeal.

There are also serious deficiencies in Bolivia's legal framework with regard to civil responsibility. Under Bolivian law, there is no protection for judges, prosecutors, or police investigators who make good-faith errors while carrying out their duties. If a case is lost initially or on appeal, or if a judge rules that the charges against the accused are unfounded, the accused can request compensation for damages, and the judges, prosecutors, or investigators can be subject to criminal charges for

misinterpreting the law. This is particularly a problem for money laundering investigations, as the law is full of inconsistencies and contradictions and is open to wide interpretation. For these reasons, prosecutors are often reluctant to pursue these types of investigations.

Several entities that move money in Bolivia remain unregulated. Hotels, currency exchange houses, illicit casinos, cash transporters, and wire transfer businesses (such as Western Union) are all unregulated and can be used to transfer money freely into and out of Bolivia. Informal exchange businesses, particularly in the department of Santa Cruz, are also used to transmit money in order to avoid law enforcement scrutiny.

While traditional asset seizure continues to be employed by counternarcotics authorities, until recently the ultimate forfeiture of assets was problematic. Prior to 1996, Bolivian law permitted the sale of property seized in drug arrests only after the Supreme Court confirmed the conviction of a defendant. A 1995 decree permitted the sale of seized property with the consent of the accused and in certain other limited circumstances. The Directorate General for Seized Assets (DIRCABI) is responsible for confiscating, maintaining, and disposing of the property of persons either accused or convicted of violating Bolivia's narcotics laws. DIRCABI, however, has been poorly managed for years, and has only auctioned confiscated goods sporadically. The UIF, with judicial authorization, may freeze accounts for up to 48 hours in suspected money laundering cases; this law has only been applied on one occasion.

Although terrorist acts are criminalized under the Bolivian Penal Code, the GOB currently lacks legislation that specifically addresses terrorist financing. Bolivia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and has signed the Organization of American States (OAS) Inter-American Convention Against Terrorism. However, there are no explicit domestic laws that criminalize the financing of terrorism or grant the GOB the authority to identify, seize, or freeze terrorist assets. Nevertheless, the UIF distributes the terrorist lists of the United Nations and the United States, receives and maintains information on terrorist groups, and can freeze suspicious assets under its own authority for up to 48 hours, as it has done in counternarcotics cases. A draft terrorist financing law was created by the UIF and presented to the Superintendence of Banks. However, because of a lack of political will due to the recent presidential elections, the bill has not yet been presented to Congress. There have been no cases of terrorist financing to date.

In order to address the problems faced by Bolivia's anti-money laundering regime, the UIF has proposed various changes that will amend Law 1768 and the UIF regulations. A set of draft laws was presented to Congress in 2004, which—if passed—would make money laundering an autonomous crime, penalized by a minimum prison term of fifteen years; increase the number of predicate offenses for money laundering, as well as the number of entities obligated to file financial reports with the UIF; and allow for the seizure of assets and the use of certain special investigative techniques. These draft laws would also require financial institutions to report cash transactions above a certain threshold and require the customs authority to provide the UIF with information regarding the physical movement of cash or monetary instruments into or out of Bolivia.

The GOB remains active in multilateral counternarcotics and international anti-money laundering organizations. Bolivia is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the South America Financial Action Task Force (GAFISUD), and is due to undergo its second mutual evaluation by GAFISUD in 2006. Bolivia is a party to the 1988 UN Drug Convention and the UN Convention for the Suppression of the Financing of Terrorism. In 2005, the GOB ratified the UN Convention Against Corruption and the UN Convention Against Transnational Organized Crime. The GOB has signed, but not yet ratified, the OAS) Inter-American Convention Against Terrorism. The UIF has been a member of the Egmont Group of financial intelligence units since 1999 and has signed memoranda of understanding with several other financial intelligence units, including Argentina, Brazil, Chile, Colombia, Ecuador,

France, Guatemala, Honduras, Korea, Mexico, Panama, Paraguay, Peru, Portugal, Slovakia, Spain and Venezuela. The GOB and the United States signed an extradition treaty in June 1995, which entered into force in November 1996.

The Government of Bolivia should strengthen its anti-money laundering regime by improving its current money laundering legislation so that it conforms to the standards of the Financial Action Task Force and GAFISUD. Bolivia should adopt new laws making money laundering a separate offense without requiring a connection to other illicit activities, expand the list of predicate offenses, criminalize terrorist financing, and enable the blockage of terrorist assets. These changes are necessary for an effective anti-money laundering and counterterrorist financing regime. As recommended by the IMF and GAFISUD, the jurisdiction of the UIF should also be expanded to cover reporting by non-banking financial institutions. Bolivia should continue to strengthen the relationships and cooperation between all government entities involved in the fight against money laundering.

Bosnia and Herzegovina

Bosnia and Herzegovina (BiH) is neither an international, regional, nor offshore financial center. International observers believe the laundering of illicit proceeds from criminal activity through existing financial institutions, as well as the laundering of proceeds from official corruption, is widespread. Other major sources of laundered money include tax evasion, corruption, and smuggling. Money laundering is not related primarily to narcotics proceeds. The economy of BiH is primarily cash-based, and recent studies indicate that as much as 40-60 percent of the economic activity in BiH is in the gray market.

Due to its porous borders and weak rule of law capacities, BiH is a significant market and transit point for illegal commodities including cigarettes, firearms, fuel oils, and trafficking in persons. It is likely that at least some of the proceeds from illicit activities are laundered through the banking system, though supervisory entities have made progress in requiring banks to improve controls of suspect transactions. BiH authorities have had some success in clamping down on money laundering through the formal banking system, especially on the part of suspect non-governmental organizations using direct cash transfers from abroad as a source of funding. Financial crimes overall are not seen to be increasing, though renewed attention from investigators and prosecutors means that more cases are receiving public attention. Governmental authorities throughout BiH are primarily concerned with tax and customs evasion.

There are multiple jurisdictional levels in Bosnia and Herzegovina: the State (or national) level; the entity level, which includes two entities, the Federation of Bosnia and Herzegovina (Federation) and Republika Srpska (RS) plus the Brcko District; cantons in the Federation; and, municipal governments in both entities and the Brcko District. Each jurisdiction has its own (for the most part) parallel institutions, criminal codes, criminal procedure codes, supporting laws and regulations, and enforcement bodies. The Entity, Brcko District, and State-level criminal and criminal procedure codes were harmonized in 2003. Although State level institutions are becoming more firmly grounded and are gaining increased authority, jurisdictional matters between the entities and State-level institutions remain confused.

Money laundering is a criminal offense in all State and entity criminal codes. New criminal procedure (CPC) and criminal codes were enacted at the State and entity levels in 2003, with tougher provisions against money laundering. Terrorist financing was criminalized in Article 202 of the CPC. The law on the Prevention of Money Laundering came into force on December 28, 2004, and determines the measures and responsibilities for detecting, preventing, and investigating money laundering and terrorist financing. It also prescribes measures and responsibilities for international cooperation and mandates the establishment of the Financial Intelligence Department (FID), the financial intelligence unit (FIU) for BiH. The FID is part of the recently created State Investigative and Protection Agency

(SIPA). The law requires that data on money laundering and terrorist financing offenses be shared by the prosecutor's office with the FIU. The FIU became a member of the Egmont Group in 2005. The FIU is a hybrid body, tasked with performing both analytic and criminal investigative functions. The FIU has no regulatory responsibilities. The FIU receives, collects, records, analyzes, investigates, and forwards to the State prosecutor information and documentation related to money laundering and terrorist financing. It also provides expert support to the prosecutor regarding financial activities and is responsible for international cooperation on money laundering issues. The FIU is not yet fully staffed or operational, and its scrutiny of suspicious transactions is therefore limited. It is still unclear what role entity financial enforcement authorities will play in this interim period, and how they will relate to the FIU once it is fully operational.

The Law on the Prevention of Money Laundering applies to any person who "accepts, exchanges, keeps, disposes of, uses in commercial or other commercial or other activity, otherwise conceals or tries to conceal money or property he knows was acquired through perpetration of a criminal offense, when such a money or property is of larger value or when such an act endangers the common economic space of Bosnia and Herzegovina or has detrimental consequences to the operations or financing of institutions of Bosnia and Herzegovina."

For amounts above Bosnia Convertible Mark (BAM) 50,000 (approximately $30,000), the penalty is a term of imprisonment of between one and ten years. For lesser amounts, the penalty is a term of imprisonment of between six months and five years. The money laundering law applies to all individuals and institutions. However, there is no formal supervision mechanism in place for non-bank financial institutions and intermediaries. SIPA and the Federation and RS police bodies are responsible for the investigation of financial crimes.

BiH has not enacted bank secrecy laws that prevent the disclosure of client and ownership information to bank supervisors and law enforcement authorities. The banking community cooperates with law enforcement efforts to trace funds and freeze bank accounts. There is no State-level banking supervision agency. However, a number of banks, including all those within the Federation, do have compliance officers. Although the respective banking agencies have provided training to compliance officers, bankers note that a State-level working group to assist the banks with various technical, training and compliance issues would be helpful. BiH generally adheres in practice to the Basel Committee's Core Principles for Effective Banking Supervision, including legal requirements to report suspicious transactions and conduct due diligence. Financial institutions must maintain detailed deposit records and report suspicious transactions on a daily basis to regulatory authorities.

The Entity-level banking supervision agencies supervise and examine financial institutions for compliance with anti-money laundering and terrorism finance laws. Banks and other financial institutions are required to know, record, and report the identity of customers engaging in significant transactions, including currency transactions above 30,000 BAM ($18,000). They are also required to maintain records in order to respond to law enforcement requests. Reporting of all suspicious transactions is mandatory. There is no threshold amount for suspicious transactions. Reporting individuals (bankers and others) are protected by law with respect to law enforcement cooperation. There are no statutory requirements limiting or monitoring the international transportation of currency and monetary instruments. The law requires that information on all transportation of cash and securities in excess of 10,000 BAM ($6,000) be reported to the FIU by customs administration authorities. Transactions that violate the law may be prosecuted. The taxation authority, which has responsibility for Customs, suffers like other BiH State agencies from a lack of resources and sufficient trained personnel.

The cash threshold for currency transaction monitoring is 30,000 BAM (about $20,000). In 2004, the Federation Financial Police received reports on 77,422 currency transactions totaling 6.8 billion BAM (about $4.6 billion) from financial institutions and customs authorities. Out of this number, 128

transactions in amount of 11.1 million BAM (about $7.5 million) were identified as suspicious and reported to prosecutors. The accounts of 1,234 fictitious companies were blocked and assets in amount of 1.3 million BAM (about $870,000) were frozen. Criminal charges were pressed against 67 individuals. In 2005, the FIU received 98,891 currency reports from banks. Of these, 83 were identified as suspicious transactions warranting additional measures such as temporary freezing of assets, seizure and analysis of documentation, and carrying out of interviews with individuals linked to the suspicious transaction. The FIU reports that it froze 1,985,225 BAM ($1,203,167) in 2005.

In order to avoid misuse of the banking system by multiplication of accounts, the Central Bank of Bosnia and Herzegovina (CBBH) has established a central registry of bank accounts. The Single Transaction Account Registry, which became operational on July 5, 2004, contains all the transactional accounts of the legal entities in BiH. Only the CBBH Main Units can issue data from the Registry. Any legal entity or citizen can submit a request for information from the Single Transactional Accounts Registry, provided they can justify the request and provide proof of fee payment.

There have been several multiple-defendant indictments for money laundering, most of which have been disposed of by plea bargain. There were three major money laundering cases in BiH in 2005. In the first case, three persons were indicted for money laundering. One individual was sentenced to two years imprisonment. The trial for the other two has not yet been completed. In a second case, a plea agreement was reached and the defendant was sentenced to two years' imprisonment and a 10,000 BAM ($6,000) fine. In the third case, three persons were indicted. One defendant was sentenced to two years and agreed to testify against the other two defendants. Their trial remains ongoing. There were no arrests or prosecutions for terrorist financing in 2005.

The BiH has adequate and comprehensive procedures for forfeiture of criminal proceeds. BiH authorities have the authority to identify, freeze, seize, and forfeit terrorist finance- related and other assets. Forfeiture proceedings are initiated and conducted by the Prosecutor. The banking agencies, in particular, have the capability to freeze assets. However, the prosecutor and courts do not have the administrative mechanisms in place to seize assets, maintain them in storage, dispose of them, or route the proceeds to the appropriate authorities. BiH law does not designate any appropriate authority for this purpose. Property may be seized for criminal offenses for which a term of imprisonment of five years or more is prescribed. A specific relationship to the crime does not have to be proven for the assets to be seized. There is no mechanism for civil confiscation in place and none is anticipated in the near future.

On October 21, 2002, the UN High Representative put in place amendments to Federation and RS Banking Laws, banning the use of money for terrorism. Citizens of BiH can be prosecuted for terrorism financing when a terrorist act is committed abroad; non-citizens can be extradited. BiH will not extradite its own citizens, but will prosecute them in BiH. The amendments provide Federation and RS Banking Agencies with clear legal authority to freeze assets of suspected terrorists. Banking agencies cooperate well with U.S. authorities. The Entity banking agencies are cognizant of the requirements to sanction suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list. However, BiH State authorities do not circulate the consolidated list to them on a regular basis. In 2004, the Government of BiH disrupted the operations of several organizations listed by the UN 1267 Sanctions Committee as having direct links with Al-Qaida. Authorities continue to investigate other organizations and individuals for links to terrorist financing. Non-bank financial transfers are very difficult for BiH law enforcement and customs officials to monitor. BiH authorities have not dealt explicitly with the issue of alternative remittance systems which bypass financial institutions. Any illegal transactions fall under the scope of the money laundering provisions of the BiH criminal procedure code.

A National Action Plan, adopted in October 2003, incorporates the Council of Europe's recommendations against corruption and organized crime. The National Coordination team continued its work in 2004, establishing concrete steps and timelines for accomplishing goals in the areas of institution-building, legislative reform and implementation, and operational cooperation. In implementing the plan, BiH has taken several important steps such as the continued development of the nascent SIPA, the State Intelligence Agency, and the Citizen Identification Protection System.

Mutual Legal Assistance Treaties that had been signed by either the former Yugoslavia or the Kingdom of Serbia have carried over into BiH. There is no formal bilateral agreement between the United States and BiH regarding the exchange of records in connection with narcotics investigations and proceedings. Local authorities have made good faith efforts to exchange information informally with officials from the USG and regional states, particularly Slovenia and Croatia. BiH has signed bilateral agreements for information exchange regarding bank supervision with Croatia, Serbia, and Slovenia.

BiH is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. BiH has signed, but has not yet ratified, the UN Convention against Corruption. BiH is a party to all 12 of the international conventions and protocols relating to terrorism. The Government of BiH adheres to relevant international money laundering standards. However, BiH has historically proven unable or unwilling to pass implementing legislation for the international conventions to which it is a party.

While BiH generally has law and regulations in place that conform to relevant international money laundering standards, it should do a better job of implementing those existing laws and regulations, as well as international conventions to which it is a party. BiH should also fully operationalize and staff its centralized regulatory and law enforcement authorities, including the financial intelligence unit (FIU) within the State Investigative and Protection Agency (SIPA) as soon as possible. At present, both the SIPA and the FIU remain under-funded and under-resourced. Although progress in implementation and enforcement has been made, BiH should continue to strengthen its institutions, particularly those State-level institutions responsible for the prevention of money laundering and terrorist financing. Significant additional training should be implemented so that law enforcement, prosecutors, and judges will have a better understanding of money laundering and terrorist financing and how to pursue it. BiH should consider how best to implement plans to harmonize any remaining legislation and to work toward the establishment of competent state-level institutions.

Botswana

Botswana is a developing regional financial center as well as a nascent offshore financial center. Botswana has a relatively well-developed banking sector and is vulnerable to money laundering. Neither the narcotics trade nor the laundering of its proceeds appears to be a major problem in Botswana. Financial crimes such as bank fraud and counterfeit currency were down marginally from 2004. Reportedly, illicit diamonds are smuggled from Botswana into South Africa and other neighboring countries.

Section 14 of the Proceeds of Serious Crime Act of 1990 criminalizes money laundering related to all serious crimes. The Bank of Botswana requires financial institutions to report any transaction in which BWP (Botswana Pula) 10,000 (approximately $2,500) or more is transferred. The Bank of Botswana has the discretion to provide information on large currency transactions to law enforcement agencies. In 2001, Botswana amended the Proceeds of Serious Crimes Act to require identification of financial bodies and owners of corporations and accounts. Additionally, Section 44 of the Banking Act of 1995 requires banks to exercise due diligence, and any bank which acts in breach of the requirements of this section is guilty of an offense and liable for a fine. The Bank of Botswana may revoke the license of a bank that has been convicted by a court of competent jurisdiction of an offense related to the use or

laundering of illegal proceeds. License revocation also applies if the bank is the affiliate, subsidiary, or parent company of a bank that has been convicted.

In 2003, the Government of Botswana enacted the Banking (Anti-Money Laundering) Regulations, which are minimum guidelines to banks on the application of international best practices on anti-money laundering. The regulations require banks to record and verify the identification of all personal and corporate customers. Banks must maintain all records on transactions, both domestic and international, for at least five years. Banks also must comply expeditiously with information requests from the Directorate on Corruption and Economic Crime (DCEC), which bears some of the responsibilities of a financial intelligence unit, and other law enforcement authorities. Implementation assessments by the Government in 2005 found compliance with these regulations to be satisfactory. These regulations do not apply to non-bank financial institutions.

The 2003 Banking Regulations also require banks to report suspicious transactions. For reporting purposes, banks must designate an employee at management level as a money laundering reporting officer, who serves as a contact between the bank, the Central Bank, and the DCEC. In practice, banks regularly submit reports of suspicious transactions to the Bank of Botswana, which supervises compliance with anti-money laundering regulations, and to the DCEC. From January to November 2005, the DCEC received 93 reports of suspicious activity, of which 85 were investigated. In 2004, the government established regulations governing bureaux de change, including measures to prevent the use of these institutions to launder money. Customs regulations require travelers carrying the equivalent of P10,000 (approximately $2,000) or more to declare that currency upon entering Botswana.

Botswana is in the early stages of developing an offshore financial center and, consequently, licenses offshore banks and businesses. Background checks are performed on applicants for offshore banking and business licenses, as well as on their directors and senior management. The supervisory standards applied to domestic banks are also applicable to offshore banks. The Bank of Botswana has licensed two offshore banks, but only one has commenced operations.

Bank and business directors are subject to the "fit and proper test" required by Section 29 of the Banking Act of 1995. Anonymous directors and trustees are not allowed. Currently, no offshore trusts operate in Botswana. Shell companies are prohibited in Botswana.

There were no prosecutions for money laundering or terrorist financing from January to November 2005. Terrorist financing is not criminalized as a specific offense in Botswana. However, acts of terrorism and related offenses, such as aiding and abetting, can be prosecuted under the Penal Code and under the Arms and Ammunitions Act. The Bank of Botswana has circulated to financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and the European Union's list. Under the Proceeds of Serious Crime Act, courts have the authority to confiscate proceeds of terrorist finance-related assets.

Botswana is a party to both the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Botswana is also a party to the UN Convention against Transnational Organized Crime. Botswana officially became a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) in February 2003.

The Government of Botswana is preparing a draft strategy to combat money laundering and the financing of terrorism, including interagency procedures and coordination. Although Botswana does not yet have a full-fledged financial intelligence unit, the DCEC has responsibility for investigating suspected instances of money laundering, and it can demand access to bank records if needed during the course of an investigation. Currently the law provides for asset forfeiture only after a conviction. During an investigation, the government may appeal to the High Court for a restraining order

effectively freezing the financial assets of a suspect, but only for a non-renewable, seven-day period. Government agencies are actively considering the need for broader asset forfeiture to allow a financial intelligence unit to effectively combat money laundering and the financing of terrorism. Legislation authorizing a financial intelligence unit and granting it sufficient powers to investigate would increase the government's capacity to combat financial crimes.

Brazil

Due to its size and large economy, Brazil is considered a regional financial center but not an offshore financial center. Brazil is a major drug-transit country. Brazil maintains adequate banking regulations, retains some controls on capital flows, and requires disclosure of the ownership of corporations. Brazilian authorities report that money laundering in Brazil is primarily related domestic crime, especially drugs-trafficking, corruption, organized crime, and trade in contraband, all of which generate funds that may be laundered through the banking system, real estate investment, or financial asset markets. According to Brazilian authorities, organized crime groups use the proceeds of domestic drug trafficking to purchase weapons from Colombian guerilla groups. The authorities believe that Brazilian institutions do not engage in illegal currency transactions that include significant amounts of U.S. currency derived from illegal drug sales in the United States or that otherwise significantly affect the United States. An Inter-American Development Bank study of money laundering in the region found that Brazil's relatively strong institutions helped reduce the incidence of money laundering to below average for the region.

In 2005, the Government of Brazil (GOB) continued investigating corrupt public figures, including customs inspectors, federal tax authorities, and high-ranking politicians, and the use of offshore companies to launder money. The year 2005 saw a range of corrupt activities of spectacular scope come to light, as Brazilian congressional and law enforcement authorities began multiple investigations into illicit financing by several political parties of their 2002 presidential campaigns. The campaign financing investigations uncovered a multi-layered corruption scandal involving alleged vote-buying in Congress by elements within the president's Worker's Party (PT) and executive branch, financed by kickbacks on contracts. While the investigations are ongoing, it appears that two medium-sized regional banks served as conduits for illicit payments, making use of a publicity firm's bank accounts. It appears that some payments were made into bank accounts overseas.

The Triborder Area shared by Argentina, Brazil, and Paraguay is well known for its multi-billion dollar contraband re-export trade, and arms and drug trafficking. A wide variety of counterfeit goods, including cigarettes, CDs, DVDs, and computer software, are imported into Paraguay from Asia and transported primarily across the border into Brazil, with a significantly smaller amount remaining in Paraguay for sale in the local economy. The area is also suspected by the U.S. and others to be a source of terrorist financing. The GOB, however, has stated that its concern over the Triborder Area is due to the significant loss of tax revenue as a result of the contraband trade (estimated at $1.2 billion per year), rather than the financing of terrorism, of which the Government says it has not seen any evidence. In 2005, Brazilian customs authorities launched a campaign to reduce contraband smuggling from the Triborder Area into Brazil, with inspections targeting buses used by contraband couriers.

The GOB has a comprehensive anti-money laundering regulatory regime in place. Law 9.613 of 1998 criminalizes money laundering related to drug trafficking, terrorism, arms trafficking, extortion, and organized crime, and penalizes offenders with a maximum of 16 years in prison. The law expands the GOB's asset seizure and forfeiture provisions and exempts "good faith" compliance from criminal or civil prosecution. Regulations issued in 1998 require that individuals transporting more than 10,000 reais (then approximately $10,000, now approximately $4,300) in cash, checks, or traveler's checks across the Brazilian border must fill out a customs declaration that is sent to the Central Bank. Law 10.467 of 2002, which modified Law 9.613, put into effect Decree 3,678 of 2000, thereby penalizing

active corruption in international commercial transactions by foreign public officials. Law 10.467 also added penalties for this offense under Chapter II of Law 9.613. Law 10.701 of 2003, which also modifies Law 9.613, criminalizes terrorist financing as a predicate offense for money laundering. The law also establishes crimes against foreign governments as predicate offenses, requires the Central Bank to create and maintain a registry of information on all bank account holders, and enables the Brazilian financial intelligence unit (FIU) to request from all government entities financial information on any subject suspected of involvement in criminal activity.

Law 9.613 also created a financial intelligence unit, the Conselho de Controle de Actividades Financieras (COAF), which is housed within the Ministry of Finance. The COAF includes representatives from regulatory and law enforcement agencies, including the Central Bank and Federal Police. The COAF regulates those financial sectors not already under the jurisdiction of another supervising entity. Currently, the COAF has a staff of approximately 31, comprised of 13 analysts, two international organizations specialists, a counterterrorism specialist, two lawyers and support staff.

Between 1999 and 2001, the COAF issued a series of regulations that require customer identification, record keeping, and reporting of suspicious transactions to the COAF by obligated entities. Entities that fall under the regulation of the Central Bank, the Securities Commission (CVM), the Private Insurance Superintendence (SUSEP), and the Office of Supplemental Pension Plans (PC), file suspicious activity reports (SARs) with their respective regulator, either in electronic or paper format. The regulatory body then electronically submits the SARs to COAF. Entities that do not fall under the regulations of the above-mentioned bodies, such as real estate brokers, money remittance businesses, factoring companies, gaming and lotteries, dealers in jewelry and precious metals, bingo, credit card companies, commodities trading, and dealers in art and antiques, are regulated by the COAF and send SARs directly to COAF either via the Internet or using paper forms. Banks are also required to report cash transactions exceeding 100,000 reais (approximately $43,000) to the Central Bank, and the lottery sector must notify COAF of the names and data of any winners of three or more prizes equal to or higher than 10,000 reais within a 12-month period. In 2005, COAF issued Resolution 13 of September 30, 2005, which subjects entities engaged in factoring—a growing business of extending credit based on accounts receivable, especially to small and medium-sized enterprises with more limited access to the banking system—to existing "know-your-client" provisions, record keeping requirements, and suspicious transaction reporting.

The COAF has direct access to the Central Bank database, so that it has immediate access to the SARs reported to the Central Bank. In 2006, it will gain access to the Central Bank's new database of all current accounts in the country. COAF also has access to a wide variety of government databases, and is authorized to request additional information directly from the entities it supervises and the supervisory bodies of other obligated entities. Complete bank transaction information may be provided to government authorities, including the COAF, without a court order. Domestic authorities that register with COAF may directly access the COAF databases via a password-protected system. The COAF receives roughly 10,000 cash transaction reports and 2500 SARs per month; about 2.5 percent of the latter are referred to law enforcement authorities for investigation.

The Central Bank has established the Departamento de Combate a Ilícitos Cambiais e Financeiros (Department to Combat Exchange and Financial Crimes, or DECIF) to implement anti-money laundering policy, examine entities under the supervision of the Central Bank to ensure compliance with suspicious transaction reporting, and forward information on the suspect and the nature of the transaction to the COAF. In 2005, DECIF brought on-line a national computerized registry of all current accounts (e.g., checking accounts) in the country. A 2005 change in regulations governing foreign exchange transactions requires that banks must report identifying data on both parties for all foreign exchange transactions and money remittances, regardless of the amount of the transaction.

The GOB has begun to institutionalize is national strategy for combating money laundering, holding its third annual high-level planning and evaluation session in December 2005. The strategy aims to advance six strategic goals: improve coordination of disparate federal and state level anti-money laundering efforts, utilize computerized databases and public registries to facilitate the fight against money laundering, evaluate and improve existing mechanisms to combat money laundering, increase international cooperation to fight money laundering and recover assets, promote an anti-money laundering culture, and prevent money laundering before it occurs. The main goal for 2006 is the introduction of requirements for banks to more closely monitor accounts belonging to politically exposed persons (PEPs) for patterns of suspicious transactions. The national anti-money laundering strategy has put in place more regular coordination and clarified the division of labor among various federal agencies involved in combating money laundering.

The GOB reported substantial growth in the number of money laundering investigations, trials and convictions over the last three years. The annual number of investigations grew from 198 in 2003 to 310 in 2004 and 359 in 2005. These investigations led to 26 trials in 2003, 74 in 2004 and 48 in 2005, while convictions ranged from 172 in 2003 to 87 in 2004 and 90 in 2005. These numbers represent a substantial increase from the 2000 to 2002 period, in which there was an average of 40 new investigations per year and only nine convictions (all in 2002). To deal with the increasing number of money laundering cases, special money laundering courts were created in 2003. Fifteen of these courts have been established in 14 states, including two in Sao Paulo, with each court headed by a judge who receives specialized training in national money laundering legislation. A 2006 national anti-money laundering strategy goal aims to build on the success of the specialized courts by creating complementary specialized federal police financial crimes units in the same jurisdictions. Brazil has a limited ability to employ advanced law enforcement techniques such as undercover operations, controlled delivery, and the use of electronic evidence and task force investigations that are critical to the successful investigation of complex crimes, such as money laundering. Generally, such techniques can be used only for information purposes, and are not admissible in court.

The GOB credits the increasing number of money laundering investigations, trials, and convictions to the success of the specialized courts, as well as to the large number of money laundering cases from the Banestado bank scandal, which began to move to trial during this period.

Investigations into the scandal involving Banestado, the state bank of Parana, continued in 2005 with many cases moving to prosecution. In 1995, five banks in the Triborder region of Brazil, Paraguay, and Argentina, including Banestado, were authorized to open currency exchange accounts, known as CC-5 accounts. CC-5 accounts quickly became used as a means of laundering money. Money changers opened hundreds of fake CC-5 accounts, into which criminals deposited millions of reais. The money was then wired in dollars to the Banestado branch in New York City and from there to other banks, usually in countries considered to be tax havens. The money changers and Banestado officials took cuts from each transaction.

Over 250 phony CC-5 accounts have been identified, and it is suspected that as much as $30 billion passed through CC-5 Banestado accounts in the United States between 1996 and 1999, a large portion of which was likely laundered. The GOB believes some of the Banestado money has returned to Brazil in the form of investment or loans from offshore companies. Many high-level GOB officials were implicated in this case. The Brazilian Congress began an investigation into the matter in June 2003, but the inquiry committee was considered to be polarized along party lines, and information gathered by the inquiry was leaked to the press prior to the October 2004 municipal elections. The committee concluded its inquiry on December 14, 2004, with a politicized final report recommending that law enforcement agencies indict 91 individuals in the case. Out of the 91 implicated, only two were high-level GOB officials. The Brazilian Federal Police and the Public Ministry have continued with their own investigations and have brought several individuals to trial in the case.

In 2005, the GOB drafted a bill to update its anti-money laundering legislation. If passed, this bill—which was called for in the first national anti-money laundering strategy conference in 2003—would facilitate greater law enforcement access to financial and banking records during investigations, criminalize illicit enrichment, allow administrative freezing of assets, and facilitate prosecutions of money laundering cases by amending the legal definition of money laundering and making it an autonomous offense. The draft law also allows the COAF to receive suspicious transaction reports directly from obligated entities, without their first having to pass through the supervisory bodies. The COAF would also be able to request additional information directly from the reporting entities. The draft law has not yet been presented to Congress.

Brazil has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets. The COAF and the Ministry of Justice manage these systems jointly. Police authorities and the customs and revenue services are responsible for tracing and seizing assets, and have adequate police powers and resources to perform such activities. The GOB plans to introduce in 2006 a computerized registry of all seized assets to improve tracking and disbursal. The judicial system has the authority to forfeit seized assets, and Brazilian law permits the sharing of forfeited assets with other countries.

The main weakness in Brazil's anti-money laundering regime lies in the lack of legislation criminalizing the financing of terrorism. Some GOB officials have declared that the 1983 National Security Act, which was passed under the military dictatorship and contains provisions criminalizing terrorism, could be used to prosecute terrorists or terrorist financiers, should the need arise. However, because of public resistance and the history of the law, it is generally not used in criminal matters. Although terrorist financing is considered to be a predicate offense for money laundering under Law 10.701 of 2003, terrorist financing is not an autonomous crime. There have been no money laundering prosecutions to date in which terrorist financing was a predicate offense, and so it remains to be seen if the financing of terrorism could be contested as an enforceable predicate offense due to the lack of legislation specifically criminalizing it. In 2005, the Ministry of Justice announced plans to require all non-profit organizations, which the Financial Action Task Force (FATF) has designated as an area of concern with regard to the financing of terrorism, to submit annual reports for the purposes of detecting the abuse of their non-profit status, including money laundering. These regulations would apply to non-governmental organizations, churches and charitable organizations.

The GOB has responded to U.S. efforts to identify and block terrorist-related funds. Since September 11, 2001, the COAF has run inquiries on hundreds of individuals and entities, and has searched its financial records for entities and individuals on the UNSCR Sanctions Committee's consolidated list. None of the individuals and entities on the consolidated list has been found to be operating or executing financial transactions in Brazil, and the GOB insists there is no evidence of terrorist financing in the area. In November 2003, the GOB extradited an alleged financier, Assad Ahmad Barrakat, to Paraguay on charges of tax evasion; he was convicted in May 2004 and sentenced to six and one-half years in prison.

In 2005, the GOB ratified the UN International Convention for the Suppression of the Financing of Terrorism and the OAS Inter-American Convention on Terrorism. Brazil is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. In June 2005, the GOB ratified the UN Convention against Corruption, which entered into force on December 14, 2005. Brazil is a full member of the Financial Action Task Force (FATF), and is a founding member of GAFISUD (the Financial Action Task Force Against Money Laundering in South America), and has sought to comply with the FATF Special Recommendations on Terrorist Financing. Brazil will hold the GAFISUD presidency in 2006. Brazil is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The COAF has been a member of the Egmont Group of financial intelligence units since 1999. In February 2001, the Mutual Legal Assistance Treaty between Brazil and the United States

entered into force, and a bilateral Customs Mutual Assistance Agreement, which was signed in 2002, entered into force in 2005. Using the Customs Agreement framework, the GOB and the U.S. Bureau of Immigration and Customs Enforcement began work in 2005 to implement a trade transparency unit (TTU) to detect money laundering via trade transactions. The GOB also participates in the "3 Plus 1" Counter-Terrorism Dialogue between the United States and the Triborder Area countries.

The Government of Brazil should criminalize terrorist financing as an autonomous offense. In order to continue to successfully combat money laundering and other financial crimes, Brazil should also develop legislation to regulate the sectors in which money laundering is an emerging issue. Brazil should enact and implement legislation to provide for the effective use of advanced law enforcement techniques, in order to provide its investigators and prosecutors with more advanced tools to tackle sophisticated organizations that engage in money laundering, financial crimes, and terrorist financing. It should continue the implementation of its TTU. Brazil should also enforce currency controls and cross-border reporting requirements, particularly in the Triborder region. Additionally, Brazil and its financial intelligence unit, the Conselho de Controle de Actividades Financieras (COAF), must continue to fight against corruption and ensure the enforcement of existing anti-money laundering laws.

British Virgin Islands

The British Virgin Islands (BVI) is a Caribbean overseas territory of the United Kingdom (UK). During 2005, the United States has not developed any new information on money laundering vulnerabilities and countermeasures in the BVI. Yet the BVI remains vulnerable to money laundering, primarily due to its financial services industry. Tourism and financial services account for approximately 50 percent of the economy. The offshore sector offers incorporation and management of offshore companies, and provision of offshore financial and corporate services. The BVI has 11 banks, 2,023 mutual funds with 448 licensed mutual fund managers/administrators, 312 local and captive insurance companies, 1,000 registered vessels, 90 licensed general trust companies, and 61,000 international business companies (IBCs). According to the International Business Companies Act of 1984, BVI-registered IBCs cannot engage in business with BVI residents, provide registered offices or agent facilities for BVI-incorporated companies, or own an interest in real property located in the BVI except for office leases. BVI has approximately 90 registered agents that are licensed by the Financial Services Commission (FSC). The process for registering banks, trust companies, and insurers is governed by legislation that requires detailed documentation, such as a business plan and vetting by the appropriate supervisor within the FSC. Registered agents must verify the identities of their clients.

The Proceeds of Criminal Conduct Act of 1997 expands predicate offenses for money laundering to all criminal conduct, and allows the BVI Court to grant confiscation orders against those convicted of an offense or who have benefited from criminal conduct. The law also creates a Financial Intelligence Unit (FIU), referred to as the Reporting Authority-Financial Services Inspectorate, which is responsible for the collection of suspicious activity reports. Under the Financial Investigation Agency Act 2003, implemented in 2004, the FIU was reorganized and renamed the Financial Investigation Agency.

The Joint Anti-Money Laundering Coordinating Committee (JAMLCC) coordinates all anti-money laundering initiatives in BVI. The JAMLCC is a broad-based, multi-disciplinary body comprised of private and public sector representatives. The Committee has drafted Guidance Notes based on those of the UK and Guernsey.

On December 29, 2000, the Anti-Money Laundering Code of Practice of 1999 (AMLCP) entered into force. The AMLCP establishes procedures to identify and report suspicious transactions. The AMLCP also requires covered entities to create a clearly defined reporting chain for employees to follow when

reporting suspicious transactions, and to appoint a reporting officer to receive these reports. The reporting officer must conduct an initial inquiry into the suspicious transaction and report it to the authorities, if sufficient suspicion remains. Failure to report could result in criminal liability.

The BVI proposed the Code of Conduct (Service Providers) Act (CCSPA), which would encourage professionalism, enhance measures to deter criminal activity, promote ethical conduct, and encourage greater self-regulation in the financial sector. The CCSPA also would establish the Council of Service Providers, a body that would regulate the conduct of individuals within the financial services industry. Additionally, the CCSPA would formulate policy, procedures, and other measures to regulate the industry, advise the government on legislation and policy matters, and monitor compliance within the industry.

In 2000, the Information Assistance (Financial Services) Act (IAFSA) was enacted to increase the scope of cooperation between BVI's regulators and regulators from other countries.

The BVI has criminalized terrorism and terrorist financing through the Terrorism (United Nations Measures) (Overseas Territories) Order 2001 and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002. BVI is a member of the Caribbean Financial Action Task Force and received a second mutual evaluation of its financial sector and regulations during November 17-21, 2003. BVI is subject to the 1988 UN Drug Convention and as a British Overseas Territory has implemented measures in accordance with this convention and the UN Convention against Transnational Organized Crime. Application of the U.S./UK Mutual Legal Assistance Treaty concerning the Cayman Islands was extended to the BVI in 1990. The Financial Investigation Agency is a member of the Egmont Group.

The Government of the British Virgin Islands should continue to strengthen its anti-money laundering regime by fully implementing its programs and legislation.

Brunei

In 2000, The Government of Brunei Darussalam adopted anti-money laundering legislation referred to as the Money Laundering Order and created a presiding organization called the National Anti-Money Laundering Committee (NAMLC), comprised of the: Financial Institutions divisions, Ministry of Finance (Domestic), Brunei International Financial Center (BIFC), Attorneys General's Chambers (AGC), Royal Brunei Police Force (RBPF), Royal Customs and Excise Department, Anti-Corruption Bureau, Narcotics Control Bureau, Immigration Department and Brunei Currency and Monetary Board. Brunei also implemented an asset seizure and forfeiture law, and the Criminal Conduct (Recovery of Proceeds) Order. This legislation applies both domestically and offshore.

In 2001, Brunei set into motion its plans to become an offshore financial center by bringing into effect a series of laws that established the Brunei International Financial Center (BIFC). The relevant laws are: the International Business Companies Order 2003 (amended in 2005); the International Banking Order 2000; the Registered Agents and Trustees Licensing Order 2000; the International Trusts Order 2000; the International Limited Partnerships Order 2000; the Mutual Fund Order 2001; the Securities Order 2003 (originally established in 2001) and the International Insurance and Takaful Order 2002.

The BIFC offers general banking, Islamic banking, insurance, international business companies (IBCs), trusts (including asset protection trusts), mutual funds, and securities services. Bearer shares are not permitted, but nominee shareholders are allowed for IBCs. Brunei residents are allowed to become shareholders of IBCs. In December 2005, 4,064 IBCs were registered in the BIFC database. Reportedly, many may be inactive. The eight Registered Agents and Licensed Trustees are responsible for filing all IBC compliance documents and for the International Trusts and asset protection trusts

There are six offshore banks licensed in Brunei. In July 2005,the Overseas Chinese Banking Corporation Ltd (OCBC) was awarded a full international Islamic banking license and opened its inaugural international Islamic banking branch in Brunei.

The BIFC also launched a virtual Stock Exchange in 2002 that offers securities and mutual funds. The Government also recently established the Brunei Economic Development Board to attract more foreign direct investment. There are no exchange controls.

The BIFC also offers International Insurance and Takaful. Comprehensive and imaginative legislation, coupled with a flexible regulatory regime to suit sophisticated business and personal international insurance and insurance related activities are governed by the International Insurance and Takaful Order, 2002 (IITO). There are several types of licenses available, which include the conduct of general insurance, life insurance, life and general insurance and captive insurance businesses. Licenses for the players include the International Insurance Manager, the International Underwriting Manager and the International Insurance Broker. Applicants may be companies including an established foreign or domestic insurance company or licensed registered agent and trust company in Brunei acting as representative for the purpose of license application. Special provision has been provided to the needs of unit-linked life products, reinsurance and captive insurance.

Brunei has no Central Bank. Acting through the Financial Institutions Division and the Head of Supervision, a segregated unit of the Ministry of Finance oversees the BIFC. This unit combines both regulatory and marketing responsibilities. The multi-disciplinary group is comprised of persons responsible for the supervision of banking, insurance, corporations, and trusts.

In 2002, Brunei enacted the Drug Trafficking Recovery of Proceeds Act and the Anti-Terrorism Financial and other Measures Orders. The latter explicitly criminalize the financing and support of terrorism.

Brunei is a party to the 1998 UN Drug Convention and to the UN International Convention for the Suppression of the Financing of Terrorism. Brunei became a member of the Asia/Pacific Group on Money Laundering (APG) in 2003. The APG's Terms of Reference include a commitment to adopt the international standards contained in the revised FATF Forty Recommendations on Money Laundering and the Special Nine Recommendations on Terrorist Financing.

In early 2005, Brunei Darussalam underwent a mutual evaluation by the Asia/Pacific Group on Money Laundering of its Anti-Money Laundering regime. The Government of Brunei has evaluated the report and is adopting recommendations from the evaluation. The Ministry of Finance has been discussing the establishment of a Financial Intelligence Unit (FIU) and the Australian FIU, AUSTRAC, has provided consultation to the Government of Brunei regarding the development of the unit. The Government is drafting a new Banking Order, which will incorporate such provisions as, amongst others, confidentiality of customers and permitted disclosures, confidentiality of inspection and investigation reports.

Under the jurisdiction of the Attorney General's Office, The Mutual Assistance in Criminal Matters Order, 2005 was published in March 2005 and will came into force on January 1, 2006. Brunei has signed the Treaty on Mutual Legal Assistance in Criminal Matters in Kuala Lumpur, Malaysia and will ratify the treaty in early 2006. To date, the treaty has been signed by eight Asian countries.

The Government of Brunei should continue to enhance its anti-money laundering regime by separating the regulatory and marketing functions of the Authority to avoid potential conflict of interest. Additionally, Brunei should adequately regulate its offshore sector to reduce its vulnerability to misuse by money launderers and financiers of terrorism. For all IBCs, Brunei should provide for identification of all beneficial owners, or immobilized the bearer shares. Brunei should also establish a Financial Intelligence Unit capable of receiving, analyzing and disseminating financial information to law enforcement agencies and to foreign analogs. As a member of the APG, Brunei has committed to

comport with international anti-money laundering/counterterrorist financing standards. The Government of Brunei Darussalam should remedy all deficiencies noted in the APG mutual evaluation report.

Bulgaria

Bulgaria is not considered an important regional financial center. Its significance in terms of money laundering stems from its geopolitical position, a well-developed financial sector relative to other Balkan countries, and lax regulatory control. Although Bulgaria is a major transit point for drugs into Western Europe, it is unknown whether drug trafficking constitutes the primary generator of criminal proceeds and subsequent money laundering in Bulgaria. Financial crimes, including fraud schemes of all types, smuggling of persons and commodities, and other organized crime offenses also generate significant proceeds susceptible to money laundering. Bank and credit card fraud remains a serious problem. Tax fraud and credit card fraud are also prevalent. The sources for money laundered in Bulgaria likely derive from both domestic and international criminal activity. Organized crime groups operate very openly in Bulgaria. There have been significant physical assaults on Bulgarian public officials as well as journalists who challenge organized crime operations. Smuggling remains a problem in Bulgaria and is undoubtedly sustained by ties with the financial system. While counterfeiting of currency, negotiable instruments, and identity documents has historically been a serious problem in Bulgaria, joint activities of the Bulgarian government and the U.S. Secret Service have contributed to a decline in counterfeiting in recent years. There has been no indication that Bulgarian financial institutions engage in narcotics-related currency transactions involving significant amounts of U.S. currency or otherwise affecting the United States.

Since 2003, the operation of duty free shops has been targeted by the Ministry of Finance (MOF) as part of its efforts to address the gray economy and the smuggling of excise goods. Duty free shops play a major role in cigarette smuggling in Bulgaria, as well as smuggling of alcohol, and to a lesser extent perfume and other luxury goods. Attempts by the MOF to close down shops operating in Bulgaria have been unsuccessful, in part due to political opposition within the ruling coalition. The focus of the Government of Bulgaria (GOB) has been on the use of the duty free shops to violate customs and tax regimes. It is wholly possible that the shops are used to facilitate other crimes, including financial crimes. Credible allegations have linked many duty free shops in Bulgaria to organized crime interests involved in forced prostitution, the illicit drug trade, and human trafficking. There is no indication, however, of links between duty free shops or free trade areas and terrorist financing. The MOF's Customs Agency and General Tax Directorate have supervisory authority over the duty free shops. According to these authorities, reported revenues and expenses by the shops have clearly included unlawful activities in addition to duty free trade. Good identification procedures are lacking. For example, MOF inspections have revealed that it is practically impossible to monitor whether customers at the numerous duty free shops have actually crossed an international border.

In February 2004, Parliament adopted a revised national strategy for fighting serious crime. The crime strategy covers a two-year period and focuses on the importance of cooperation between various government agencies such as the General Tax Directorate and Customs Agency, the Interior Ministry, and Bulgaria's financial intelligence unit (FIU), the Financial Intelligence Agency (FIA). However, despite the GOB's efforts to address serious crime, lax enforcement remains an issue.

Article 253 of the Bulgarian Penal Code criminalizes money laundering. The article was adopted in 1997 and amended in 1998 and 2004. The most recent amendments broaden the list of activities that constitute money laundering offenses, increase penalties (including in cases of conspiracy and abuse of office), and clarify that predicate crimes committed outside Bulgaria can support a money laundering charge brought in Bulgaria. Article 253 is an "all offense" money laundering provision. As such, drug-trafficking is but one of many recognized predicate offenses.

All financial sectors are susceptible to money laundering. There are 29 categories of reporting entities under the Bulgarian Law on Measures Against Money Laundering (LMML). Under the LMML, lawyers, real estate agents, auctioneers, tax consultants, and security exchange operators are subject to reporting requirements, which include both suspicious and currency transaction reporting requirements. To date, only the banking sector has substantially complied with the law's requirement to file Suspicious Transaction Reports (STRs) in cases of suspected money laundering. Lower rates of reporting compliance by exchange bureaus, casinos, and other non-bank financial institutions can be attributed to a number of factors, including a lack of understanding of or respect for legal requirements, lack of inspection resources, and the general absence of effective regulatory control over the non-bank financial sector.

Banks and the 28 other reporting entities under the LMML are required to apply "know your customer" (KYC) standards. The LMML was amended in 2003 to include provisions to require listed reporting entities to demand an explanation of the source of funds for operations or transactions in an amount greater than 30,000 Bulgarian Leva (BGL) (approximately$18,072) or foreign exchange transactions in an amount of 10,000 BGL (approximately $6,024). Reporting entities are also required to notify the Bulgarian FIA of each payment made in cash, in an amount greater than 30,000 BGL (approximately $18,000).

The LMML requires reporting entities (including banks and other financial institutions) to maintain records on clients and their transactions for five years. Those institutions may also be subject to internally established record keeping requirements. The degree to which such information can be provided expediently to law enforcement is impacted by bank secrecy provisions that limit dissemination absent a court order based on evidence of a committed crime. The legislation also introduces a currency transaction reporting requirement of 30,000 leva (15,000 euros), thus bringing Bulgaria into compliance with Council Directive 2001/97/EC on prevention of the use of the financial system for money laundering (2nd EU Money Laundering Directive). However, the procedures for identifying the origin of funds used to acquire banks and businesses in the privatization process are still inadequate.

The LMML obligates financial institutions to a five-year record keeping requirement and provides a "safe harbor" to reporting entities. Penal Code Article 253B was enacted in 2004 to establish criminal liability for noncompliance with LMML requirements. Although case law remains weak, when it was assessed in September 2003 for purposes of EU accession, Bulgaria's anti-money laundering legislation was determined to be in full compliance with all EU standards. The LMML amendments also changed the name of Bulgaria's FIU from the Bureau of Financial Intelligence to the Financial Intelligence Agency (FIA), commensurate with its status as a full agency within the Ministry of Finance. The amendments also further institutionalize and guarantee functional independence of the FIU's director and provide for a supervisor within the Ministry of Finance who can oversee the activities of the FIA but is prohibited by law from issuing operational commands. The FIA is also authorized to perform on-site compliance inspections. Since high-value goods dealers have been required to report since 2001, and there is no supervisory authority, the FIA also acts as the compliance authority for this sector. The FIA is authorized to obtain all information without a court order, to share all information with law enforcement, and to receive reports of suspected terrorism financing. Notwithstanding the increase in activity, the FIA remains handicapped technologically, but it is working on improving its databases and its data management to make them more efficient for analytical use. In 2005, a high-level interagency working group began meeting that will review the LMML and proposed additional amendments in 2006 in order to make the law fully compliant with international standards. Members of the working group (the Legislative Working Group on Amendments to the Law on Measures against Money Laundering and the Law on Measures against Financing of Terrorism) include the following agencies: FIA, Ministry of Justice, Ministry of Interior,

Bulgarian National Bank, Gaming Commission, Financial Supervision Commission, Customs Agency, and the General Tax Directorate.

The FIA is an administrative unit and does not participate in active criminal investigations. The FIA forwards reports of potential criminal activity to the Prosecutor's Office. The Prosecutor then has the discretion to open an investigation by referring the case to either law enforcement officers from the Ministry of Interior (MOI) or to investigating magistrates from the National Investigative Service (NIS). The MOI and the NIS are the two agencies responsible for investigating money laundering and any underlying predicate criminal activity. If the Prosecutor's Office determines that an STR referred by the FIA does not merit prosecution, the FIA has the authority to appeal the Prosecutor's decision. In the time period between January and November 2005, the FIA received 662 STRs and 130,631 currency transaction reports (CTRs). The STRs had a total combined value of approximately $280 million. On the basis of the forwarded reports, 646 cases were opened. During the same period, the FIA referred 74 cases to the Supreme Prosecutor's Office of Cassation and 265 cases to the Ministry of Interior. The FIA also forwarded 33 reports to supervisory authorities for administrative action. Although money laundering has been pursued in court cases, there has never been a conviction for the crime. In fact, there are very few successful prosecutions for other financial crimes and predicate criminal activity that give rise to money laundering. This is mainly due to the fact that prosecutors, investigators, and law enforcement officials, especially at the district level, lack significant training in money laundering. GOB officials, however, hope that this trend is changing. In 2005, the Prosecution Service has reported indictments of organized crime figures for money laundering. Prosecution figures are also expected to increase in 2006 following a recent Directive issued by the Prosecutor General instructing Bulgarian prosecutors to use multiple count indictments, including indictments that charge money laundering in addition to predicate offenses. This Directive purports to change the current practice of charging only the predicate offenses.

Bulgaria has strict and wide-ranging banking, tax, and commercial secrecy laws that limit the dissemination of financial information absent the issuance of a court order based on evidence of a committed crime. While the FIA enjoys an exemption from these secrecy provisions, they apply to all other government institutions and often are cited as an impediment to the performance of legitimate law enforcement functions. In a small effort to remedy the situation in 2004, amendments made to the Bulgarian Penal Code permit the repeal of overly broad tax secrecy provisions, improving dissemination of some information previously covered by tax secrecy laws.

There are few, if any, indications of terrorist financing connected with Bulgaria. The GOB amended its Penal Code at Article 108a to criminalize terrorism and terrorist financing. Under Article 253 of the Criminal Code, terrorist acts and financing qualify as predicate crimes under Bulgaria's "all crimes" approach to money laundering. The GOB also enacted the Law on Measures Against Terrorist Financing (LMATF) in February 2003, which links counterterrorism measures with financial intelligence and compels all covered entities to report a suspicion of terrorism financing or pay a penalty of 25,000 Bulgarian Leva (approximately $15,000). The law was passed to be consistent with the FATF Special Recommendations on Terrorist Financing. The law also authorizes the FIA to use its resources and financial intelligence to combat terrorism financing, as well as in fighting money laundering.

Under the provisions of the LMATF, the GOB may freeze the assets of a suspected terrorist for up to 45 days. The FIA, in cooperation with the Bulgarian National Bank, circulates to the banking sector the 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, along with those designated by the EU under its relevant authorities. To date, no suspected terrorist assets have been identified, frozen, or seized by Bulgarian authorities. In 2005, a joint task force comprised of representatives from between the FIA and the National Security Service was established to identify possible terrorist financing activities and terrorist supporters.

There are no reported initiatives underway to address alternative remittance systems. Although they may operate there, Bulgarian officials have not officially acknowledged their existence. In general, regulatory controls over non-bank financial institutions are still lacking, with some of those institutions engaging in banking activities absent any regulatory oversight. Similarly, exchange bureaus are subject to minimal regulatory oversight, and some anecdotal evidence suggests that charitable and non-profit legal status is occasionally used to conceal money laundering. In 2005, as part of its ongoing effort to strengthen its anti-money laundering and counterterrorist financing regime, the GOB made non-bank financial institution oversight deficiencies a top priority. Results of these efforts to date, however, have been mixed.

In cases where a conviction has been obtained, the Bulgarian Penal Code provides legal mechanisms for forfeiting assets (including substitute assets in money laundering cases) and instrumentalities. Bulgaria's money laundering and terrorist financing laws both include provisions for identifying, tracing, and freezing assets related to money laundering or the financing of terrorism. A new criminal asset forfeiture law, targeted at confiscation of illegally acquired property, came into effect in March 2005. The law permits forfeiture proceedings to be initiated against property valued in excess of 60,000 Bulgarian Leva (approximately $36,000) if the owner of the property is the subject of criminal prosecution for enumerated crimes (terrorism, drug trafficking, human trafficking, money laundering, bribery, major tax fraud, and organizing, leading, or participating in a criminal group) and a reasonable assumption can be made that the property was acquired through criminal activity. The law requires the establishment of a criminal assets identification commission that has the authority to institute criminal asset identification procedures, as well as request from the court both preliminary injunctions and ultimately the forfeiture of assets. Although the Commission has been appointed, it is not yet functional. Key players in the process of asset freezing and seizing, as prescribed in existing law, include the MOI, MOF (including the FIA), Council of Ministers, Supreme Administrative Court, Sofia City Court, and the Prosecutor General.

The United States does not have a mutual legal assistance treaty with Bulgaria. Information is exchanged formally through the letter rogatory process. Currently, the FIA has bilateral memoranda of understanding (MOU) regarding information exchange relating to money laundering with 27 countries. Negotiations with five more states are currently in progress. The FIA is authorized by law to exchange financial intelligence on the basis of reciprocity without the need of an MOU. Between January and December 2005, the FIA sent 332 requests for information to foreign FIUs and received 83 requests for assistance from foreign FIUs. Bulgaria has also entered into an intergovernmental agreement with Russia that promotes anti-money laundering cooperation.

Bulgaria participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The FIA is a member of the Egmont Group and participates actively in information sharing with foreign counterparts. Bulgaria is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Bulgaria is also a party to the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. In December 2003, the GOB signed the UN Convention against Corruption.

On September 21, 2005, the Bulgarian Parliament passed amendments to the 1969 law on Administrative Violations and Penalties, which establishes the liability of legal persons (companies) for crimes committed by their employees. This measure is in accordance with international standards and allows the GOB to implement its obligations under a number of international agreements, including: the OECD Anti-bribery Convention, the European Council Convention on Corruption, the UN International Convention for the Suppression of Terrorist Financing, and the UN Convention against Transnational Organized Crime. Under the amendments, Bulgaria also aligns itself with the provisions of the EU Convention on the Protection of the Communities' Financial Interests and its Protocols, a requirement for EU accession.

Although Bulgaria has done well to enact legislative changes consistent with international anti-money laundering standards, the lack of enforcement remains an issue. There appears to be no political will to amend unduly broad bank secrecy provisions that are said to hamper law enforcement efforts, and the banking community has a very strong lobby within Parliament. The GOB must take steps to improve and tighten its regulatory regime (especially with regard to non-bank financial institutions) and the consistency of its Customs reporting enforcement. Bulgaria should also establish procedures to identify the origin of funds used to acquire banks and businesses during privatization. Bulgaria should provide sufficient resources to the Financial Intelligence Agency (FIA) and incorporate technological improvements. The FIA should also continue to work cooperatively with all institutions having a role to play in combating money laundering to ensure full implementation of Bulgaria's anti-money laundering regime and to improve prosecutorial effectiveness in money laundering cases.

Burma

Burma, a major drug producing and trafficking country, has a mixed economy with substantial state-controlled companies, mainly in energy and heavy industry, and with private business primarily in agriculture and light industry. Burma's economy continues to be vulnerable to drug money laundering due to its under-regulated financial system, inadequate implementation of its anti-money laundering regime, and policies that facilitate the funneling of drug money into commercial enterprises and infrastructure investment. The government has addressed key areas of concern identified by the international community by implementing some anti-money laundering measures, but Burma remains on the Financial Action Task Force (FATF) list of Non-Cooperative Countries and Territories (NCCT), and the United States maintains countermeasures against Burma as of December 2005.

Burma enacted a "Control of Money Laundering Law" in 2002. It also established the Central Control Board of Money Laundering in 2002 and a financial intelligence unit (FIU) in 2003. It set a threshold amount for reporting cash transactions by banks and real estate firms, albeit at a high level of 100 million kyat (approximately $100,000). Since adopting a "Mutual Assistance in Criminal Matters Law" in 2004, Burma has taken additional steps to address money laundering and to combat terrorist financing, including adding fraud to the list of predicate offenses and defining penalties for "tipping off" suspicious transaction reports. As a result, FATF lifted its countermeasures in October 2004. The GOB's 2004 anti-money laundering measures amended regulations, originally instituted in 2003, which had set out 11 predicate offenses, including narcotics activities, human and arms trafficking, cyber crime, and "offenses committed by acts of terrorism," among others. The 2003 regulations also called for suspicious transaction reports (STRs) by banks, the real estate sector, and customs officials, and imposed severe penalties for non-compliance.

The GOB established a Department Against Transnational Crime in 2004 with a mandate that included anti-money laundering activities. It is staffed by police officers and support personnel from banks, customs, budget, and other relevant government departments. In response to a February 2005 FATF request, the Government of Burma submitted an anti-money laundering implementation plan and progress reports. In 2005, the government also increased the size of the FIU from 10 to 40 staff. In August 2005, the Central Bank of Myanmar issued guidelines for on-site bank inspections and required reports reviewing banks' compliance with AML legislation. Since then, the Central Bank has disbursed teams to instruct on the new guidelines and to inspect banking operations for compliance.

Despite the lifting of countermeasures, Burma remains on the FATF's list of non-cooperative countries and territories because it has not yet implemented all the required reforms in its anti-money laundering regime. As of December 2005, the United States maintains the countermeasures it adopted against Burma in 2004. At that time, the United States issued final rules finding the jurisdiction of Burma and two private Burmese banks, Myanmar Mayflower Bank and Asia Wealth Bank, to be "of primary money laundering concern," and requiring U.S. banks to take certain special measures with

respect to all Burmese banks, with particular attention to Myanmar Mayflower and Asia Wealth Bank. These rules were issued by the Financial Crimes Enforcement Network within the Treasury Department pursuant to Section 311 of the 2001 USA PATRIOT Act.

The rules prohibit most U.S. financial institutions from establishing or maintaining correspondent or payable-through accounts in the United States for, or on behalf of, Myanmar Mayflower and Asia Wealth Bank and, with narrow exceptions, for all other Burmese banks. Myanmar Mayflower and Asia Wealth Bank have been directly linked to narcotics trafficking organizations in Southeast Asia. In March 2005, following a GOB investigation, the Central Bank of Myanmar revoked Myanmar Mayflower Bank's and Asia Wealth Bank's licenses to operate, citing infractions of the Financial Institutions of Myanmar Law. As of December 2005, Government of Burma investigations into these two cases continue. In August 2005, the Government of Burma seized the assets of another private institution, the Myanmar Universal Bank (MUB), and arrested the bank's chairman under the Narcotics and Psychotropic Substances Law, charging him with drug-related money laundering crimes. As of December 2005, the case was still in court.

Burma remains under a separate U.S. Treasury Department advisory stating that U.S. financial institutions should give enhanced scrutiny to all financial transactions relating to Burma. The Section 311 rules complement the 2003 Burmese Freedom and Democracy Act (renewed in July 2005) and an accompanying Executive Order. These laws imposed additional economic sanctions on Burma following the regime's May 2003 attack on pro-democracy leader Aung San Suu Kyi and her convoy. The sanctions prohibit the import of Burmese-produced goods into the United States, ban the provision of financial services to Burma by U.S. persons, freeze the assets of identified Burmese institutions, including those of the ruling junta, and expand visa restrictions to include managers of state-owned enterprises, in addition to senior government officials and family members associated with the regime. In August 2005, the U.S. Treasury amended and reissued the Burmese Sanctions Regulations in their entirety to implement the 2003 Executive Order, which placed sanctions on Burma.

Burma holds observer status in the Asia/Pacific Group on Money Laundering and applied for full membership in 2005. Burma is a party to the 1988 UN Drug Convention. Over the past several years, the Government of Burma (GOB) has extended its counternarcotics cooperation with other states. The GOB has bilateral drug control agreements with India, Bangladesh, Vietnam, Russia, Laos, the Philippines, China, and Thailand that address cooperation on drug-related money laundering issues. In July 2005, the Myanmar Central Control Board signed an MOU with Thailand's Anti-Money Laundering Office governing the exchange of information and financial intelligence.

Burma is a party to the UN Convention against Transnational Organized Crime and has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. Burma plans to sign the ASEAN Multilateral Assistance in Criminal Matters Agreement in early 2006.

The GOB now has in place a framework to allow mutual legal assistance and cooperation with overseas jurisdictions in the investigation and prosecution of serious crimes. Burma must improve enforcement of the regulations and oversight of its banking system, and end all policies that facilitate the investment of drug money into the legitimate economy. It also must discourage the widespread use of informal remittance or "hundi" networks. Burma should continue to work toward full implementation of a viable anti-money laundering/counterterrorist financing regime, and should provide the necessary resources to administrative and judicial authorities that supervise the financial sector, so they can successfully implement and enforce the government's latest regulations to fight money laundering. Burma should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism and criminalize the funding of terrorism.

Cambodia

Cambodia is not an important regional financial center. Nevertheless, Cambodia remains vulnerable to money laundering. It has a very weak anti-money laundering regime, a cash-based economy with an active informal banking system, porous borders with attendant smuggling, and widespread official corruption. The National Bank of Cambodia (NBC) has made some strides in recent years by beginning to regulate the small official banking sector, but other non-bank financial institutions, such as casinos, remain outside its jurisdiction. The Ministry of Interior has legal responsibility for oversight of the casinos and providing security, it exerts little supervision over them. The Cambodian government continues to work on draft legislation that would criminalize money laundering and the financing of terrorism, but the law is not expected to pass until 2006.

Cambodia's banking sector is small but expanding, with fifteen general commercial banks, and four specialized commercial banks and numerous microfinance institutions. However, overall lending and banking activity remains limited. Recently, one of Australia's largest banks, ANZ Banking Group Ltd, decided to enter the Cambodian market through a joint venture with one of the largest local business conglomerates, the Royal Group of Companies. Otherwise, the banking sector is largely dominated by a handful of Cambodian-owned banks such as Canadia, Mekong, and ACLEDA, the government-owned Foreign Trade Bank.

The NBC has oversight responsibility for the banking sector and, with relatively small numbers of transactions and deposits in the system, believes it exercises comprehensive oversight. There are no reports to indicate that banking institutions themselves are knowingly engaged in money laundering. The NBC regularly audits individual banks to ensure compliance with laws and regulations. There is a standing requirement for banks to declare transactions over $10,000. The NBC says its audits reveal that this requirement is generally followed. A more likely route for larger scale money laundering in Cambodia is through informal banking activities or business activities. Neither the NBC nor any other Cambodian entity is responsible for identifying or regulating these informal financial networks or activities.

With increased political stability and the gradual return of normalcy in Cambodia after decades of war and instability, bank deposits have continued to rise and the financial sector shows some signs of deepening as domestic business activity continues to increase in the handful of urban areas. Nevertheless, foreign direct investment in the general economy remains limited, and is on a downward trend, largely due to the high risks of doing business in Cambodia, including an incomplete legal framework, inadequate legal enforcement, and official corruption.

There is no apparent increase in the extent of financial crime over the past year. There is a significant black market in Cambodia for smuggled goods, including drugs, but no evidence that smuggling is funded primarily by drug proceeds. Heroin is smuggled through Cambodia to other countries. Most of the smuggling that takes place is intended to circumvent official duties and taxes and involves items such as fuel, alcohol and cigarettes. Some government officials and their private sector associates have a significant amount of control over the smuggling trade and thus its proceeds. Cambodia has a cash-based and dollar-based economy, and the smuggling trade is usually conducted in dollars, which facilitates money laundering. Such proceeds are rarely transferred through the banking system or other financial institutions. Instead, they are readily converted into land, housing, luxury goods or other forms of property. It is also relatively easy to hand-carry cash into and out of Cambodia. In addition, neither money laundering (except in connection with drug trafficking) nor terrorism financing is a specific criminal offense in Cambodia at this time.

The NBC does not yet have the authority to apply anti-money laundering controls to non-bank financial institutions such as casinos or other intermediaries, such as lawyers or accountants. However, this authority is included in draft anti-money laundering legislation.

The major non-bank financial institutions in Cambodia are the casinos, where foreigners are allowed to gamble but most Cambodians are not. The regulation of casinos falls under the jurisdiction of the Ministry of Interior, although the Ministry of Economy and Finance issues casino licenses. The Interior Ministry stations a few officials at each casino on a 24-hour basis. It does not appear that Interior Ministry staff at the casinos exercise any actual supervision over casino operations, beyond making sure that the Ministry receives its share of casino payouts that ensures security for the casinos.

There are currently 19 licensed casinos in Cambodia, with a few more either under construction or applying for a license. Most are located along Cambodia's borders with Thailand or Vietnam. There is one large casino and other smaller gambling establishments located in Phnom Penh that have avoided the regulation that all casinos be at least 200 kilometers from the capital city.

Reportedly, most casino patrons simply hand-carry their money across borders. For patrons placing large bets, the casinos have accounts with major banks, usually in Thailand. In practice, the patron wires a large amount of money to one of these accounts in Thailand. After a quick phone call to verify the transfer, the casino in Cambodia issues the appropriate amount in chips. Regardless of whether funds are hand-carried into Cambodia or wired into a Thai bank, the casinos do not practice due diligence.

In 1996, Cambodia criminalized money laundering related to narcotics trafficking through the Law on Drug Control. In 1999, the government also passed the Law on Banking and Financial Institutions. These two laws provide the legal basis for the NBC to regulate the financial sector. The NBC also uses the authority of these laws to issue and enforce new regulations. The most recent regulation, dated October 21, 2002, is specifically aimed at money laundering. The decree established standardized procedures for the identification of money laundering at banking and financial institutions. In October 2003, the NBC issued a circular to assist banks in identifying suspicious transactions. In addition to the NBC, the Ministries of Economy and Finance, Interior, Foreign Affairs, and Justice also are involved in anti-money laundering matters.

The 1996 and 1999 laws include provisions for customer identification, suspicious transaction reporting, and the creation of an Anti-Money Laundering Commission (AMLC) under the Prime Minister's Office. The composition and functions of the AMLC have not yet been fully promulgated by additional decrees. A Sub-Decree on the composition and duties of AMLC has been drafted but is unlikely to be passed until passage of the new anti-money laundering legislation. The NBC currently performs many of the AMLC's intended functions. The 1999 Law on Banking and Financial Institutions imposed new capital requirements on financial institutions, increasing them from $5 million to $13.5 million. Commercial banks must also maintain 20 percent of their capital on deposit with the NBC as reserves.

Cambodia ratified the 1988 UN Drug Convention in 2005. It has signed the UN International Convention for the Suppression of the Financing of Terrorism. While Cambodia is drafting legislation that would specifically address terrorism financing, it currently does not have any laws that do so. It does circulate to financial institutions the list of individuals and entities included on the UNSCR 1267 Sanction Committee's consolidated list. NBC reviews the banks for compliance in maintaining this list and reporting any related activity. To date, there have been no reports of designated terrorist financiers using the Cambodian banking sector. Should sanctioned individuals or entities be discovered using a financial institution in Cambodia, the NBC has the legal authority to freeze the assets but not to seize them.

In June 2004, Cambodia joined the Asia/Pacific Group on Money Laundering (APG), a Financial Action Task Force (FATF) regional body. The APG has 30 members, including the U.S. Among its activities, the APG conducts mutual evaluations of members' anti-money laundering and terrorism financing efforts. The APG planned to conduct an evaluation of Cambodia in 2005 but the Cambodian government requested that the APG delay its evaluation until after the passage of the draft Law on

Anti-Money Laundering. The government also plans to work with the APG members to establish a Financial Intelligence Unit (FIU). According to the draft law, the FIU will be placed under the control of the NBC with a permanent secretariat working under the authority of a board composed of the senior representatives from Ministries of Economy and Finance, Justice, and Interior. In order to decide where to locate the FIU, an "unofficial" Anti-Money Laundering Committee was formed recently, consisting of the NBC and the Ministries of Commerce, Foreign Affairs, Finance and Justice. The Committee held its first session in December 2004.

A Working Group, including the NBC and the Ministries of Economy and Finance, Interior, and Justice, the National Anti-Drug Committee was formed on November 26, 2003 to draft anti-money laundering legislation that meets international standards. Among other priority actions, the Working Group's draft legislation and action plan to fight money laundering and the financing of terrorism envisions the following: criminalizing money laundering and the financing of terrorism; ratification of all relevant UN conventions; regulating and controlling NGOs; reducing the use of cash and encouraging the use of the formal banking system for financial transactions; enhancing the effectiveness of bank supervision; ensuring the use of national ID cards as official documents for customer identification; and regulating casinos and the gambling industry. The draft legislation also addresses preventive obligations related to customer due diligence, record keeping, internal controls reporting of suspicious transactions, and setting up an FIU to receive, analyze and disseminate information and to supervise compliance with all relevant laws and regulations. The IMF is assisting the NBC in issuing regulations to strengthen the existing anti-money laundering framework while the draft legislation is considered. Absent passage of the draft legislation in 2005, the NBC plans to issue a series of regulations that have the force of law (Praksas) and that will criminalize money laundering and terrorism financing, as well as update existing financial rules and regulations.

Pending legislation on industrial zones would create several free trade zones along Cambodia's borders. Some observers have raised concerns about the potential for money laundering in the free trade zones, and it is unclear if the pending legislation will address this issue. In May 2005, Prime Minister Hun Sen cited money laundering as a major concern during his remarks at the Ministerial Meeting of Signatory Countries on 1993 MOU on Drug Control Cooperation.

Continuing work on the draft anti-money laundering legislation and becoming a party to the 1988 UN Drug Convention are positive steps. Cambodia should pass the draft anti-money laundering and counterterrorist financing legislation as soon as possible. Cambodia should also ratify the UN Convention Against Transnational Organized Crime. However, the larger questions remain regarding the government's ability to implement and enforce the measures once they are in place. Cambodia should also engage fully with the Asia/Pacific Group on Money Laundering and take full advantage of its upcoming mutual evaluation and training programs offered by international donors.

Canada

Canada has implemented several measures in recent years to reduce its vulnerability to money laundering and terrorist financing. Canadian financial institutions, however, remain susceptible to currency transactions involving international narcotics proceeds, including significant amounts of funds in U.S. currency derived from illegal drug sales in the United States. The United States and Canada share a border that sees over $1 billion in trade a day. Both the U.S. and Canadian governments are particularly concerned about the criminal abuse of cross-border movements of currency. The growth in Chinese and Colombian criminal organizations inside Canada is being reflected in increased narcotics-related crime and higher seizures. Canada has no offshore financial centers.

In 2000, the Government of Canada (GOC) passed the Proceeds of Crime (Money Laundering) Act to assist in the detection and deterrence of money laundering, facilitate the investigation and prosecution

of money laundering, and create a financial intelligence unit (FIU). The Proceeds of Crime (Money Laundering) Act was amended in December 2001 to become the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The list of predicate money laundering offenses was expanded and now covers all indictable offenses, including terrorism and the trafficking of persons.

The PCMLTFA creates a mandatory reporting system for suspected terrorist property, suspicious financial transactions, large cash transactions, large international electronic funds transfers, and cross-border movements of currency and monetary instruments totaling Canadian $10,000 (approximately $8,500) or greater. Failure to report cross-border movements of currency and monetary instruments could result in seizure of funds or penalties ranging from Canadian $250 to $5,000 (approximately $200 to $4,000).

A second set of regulations, published in May 2002, relates to internal compliance regimes, the reporting of large cash transactions and large international electronic funds transfers, the reporting of transactions where there are reasonable grounds to suspect terrorist financing, the reporting of possession or control of terrorist property, and record keeping and client identification requirements. Certain requirements were phased in during 2003. A further set of regulations concerning the reporting of cross-border movements of currency and monetary instruments became effective in January 2003.

Money service businesses, casinos, accountants, and real estate agents handling third-party transactions are required to report suspicious financial transactions. Failure to file a suspicious transaction report (STR) could lead to up to five years' imprisonment, a fine of Canadian $2,000,000 (approximately $1,730,000), or both. During 2005, the reporting requirements for the legal profession were being clarified.

The FIU, the Financial Transactions and Reports Analysis Center of Canada (FINTRAC), was established in July 2001. FINTRAC operates as an independent agency that receives and analyzes reports from financial institutions and other financial intermediaries and makes disclosures to law enforcement and intelligence agencies. FINTRAC is also mandated to ensure the compliance of these reporting entities with the legislation and regulations. The PCMLTFA expanded FINTRAC's mandate to include counterterrorist financing and to allow disclosure to the Canadian Security Intelligence Service of information related to financial transactions relevant to threats to the security of Canada.

FINTRAC now receives mandatory reports on all international funds transfers and cash transaction and cross-border movements of Canadian $10,000 (approximately $8,500) or more. During 2004-2005 FINTRAC received more than 10.8 million reports. The majority of the reports were filed electronically. FINTRAC produced a total of 142 case disclosures in 2004-2005, totaling approximately Canadian $2 billion (approximately $1.7 billion), almost triple the value of the previous year. The law protects those filing reports on suspicious transactions from civil and criminal prosecution, and there has been no apparent decline in deposits made with Canadian financial institutions as a result of Canada's revised laws and regulations. FINTRAC's case disclosures have not yet resulted in prosecutions.

In a November 2004 report to Parliament, Canada's Auditor General stated that "privacy concerns restrict FINTRAC's ability to disclose intelligence to the Police, and as a result, law enforcement and security agencies usually find that the information they receive is too limited to justify launching investigations." Additionally, U.S. law enforcement officials have echoed concerns that Canadian privacy laws and the high standard of proof required by Canadian courts inhibit the full sharing of timely and meaningful intelligence on suspicious financial transactions. Such intelligence may be critical to investigating and prosecuting international terrorist financing or major money laundering investigations. Recently, concern has focused on the inability of U.S. and Canadian law enforcement officers to exchange promptly information concerning suspected sums of money found in the possession of individuals attempting to cross the U.S.-Canadian border. A 2005 Memorandum of

Understanding on exchange of cross-border currency declarations expanded the extremely narrow disclosure policy. However, the scope of the exchange remains restrictive.

In order to address these concerns, the GOC has recently proposed a series of legislative changes that would expand information available in FINTRAC disclosures in order to enhance the critical identifiers and investigative links that law enforcement and intelligence agencies can use to further money laundering and terrorist financing investigations while respecting the privacy and Charter rights of Canadians.

The PCMLTFA enables Canadian authorities to deter, disable, identify, prosecute, convict, and punish terrorist groups. As of June 2002, STRs are required on financial transactions suspected to involve the commission of a terrorist financing offense. The GOC has also listed and searched financial records for suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list.

FINTRAC has the authority to negotiate information exchange agreements with foreign counterparts. It has signed 29 memoranda of understanding to establish the terms and conditions to share intelligence with FIUs, and is negotiating several other memoranda. Canada has longstanding agreements with the United States on law enforcement cooperation, including treaties on extradition and mutual legal assistance. Canada has provisions for sharing seized assets, and exercises them regularly.

Canada is a member of the Financial Action Task Force (FATF) and the OAS Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). Canada also participates with the Caribbean Financial Action Task Force (CFATF) as a Cooperating and Supporting Nation, and as an observer jurisdiction to the Asia/Pacific Group on Money Laundering (APG). In June 2002, FINTRAC became a member of the Egmont Group. Canada is a party to the OAS Inter-American Convention on Mutual Assistance in Criminal Matters. Canada is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Crime and the 1988 UN Drug Convention. The GOC has signed, but not yet ratified, the UN Convention against Corruption.

The Government of Canada continues to take significant steps to reduce its vulnerability to money laundering and terrorist financing in line with international standards. Canada is currently conducting a comprehensive review and significant updating of its AML/CTF framework in the context of the upcoming parliamentary review of the PCMLTFA. Proposed measures by the GOC include enhanced client identification, increased compliance and enforcement, and strengthening FINTRAC's intelligence function.

Canada should continue its efforts to work toward ensuring the timely sharing of financial information that may be critical to international terrorist financing or major money laundering investigations. Canada also should continue its active participation in international fora dedicated to the fight against money laundering and terrorist financing.

Cayman Islands

The Cayman Islands, a United Kingdom (UK) Caribbean overseas territory, continues to make strides in strengthening its anti-money laundering program, including its first successful prosecution of a money laundering case in February 2005. Nevertheless, the islands remain vulnerable to money laundering due to their significant offshore sector. As the world's fifth largest financial center, the Cayman Islands is home to a well-developed offshore financial center that provides a wide range of services such as private banking, brokerage services, mutual funds, and various types of trusts, as well as company formation and company management. There are over 500 banks and trust companies, 7,100 mutual and hedge funds, and 727 captive insurance companies licensed in the Cayman Islands.

Since the placement of the Cayman Islands on the FATF list of Non-Cooperative Countries and Territories in 2000 and subsequent removal in 2001, the Cayman Islands has rapidly passed, amended, and revised several anti-money laundering (AML)-related laws and regulations. Recent revisions include: the Money Services Law (2003), the Monetary Authority Law (2004), Building Societies Law (2001), Cooperative Societies Law (2001), Insurance Law (2004), Mutual Funds Law (2003), the Proceeds of Criminal Conduct (2004), and the Anti-Money Laundering Regulations (2003, 2004). A draft bill is currently being reviewed that will increase the ability to confiscate property in money laundering cases including civil forfeitures.

The Cayman Islands Monetary Authority (CIMA) is responsible for the licensing, regulation, and supervision of the Cayman Islands' financial industry, which includes banks, trust companies, mutual funds, insurance companies, money service businesses, and corporate service providers. CIMA received independence to issue and revoke licenses and enforce regulations through the Monetary Authority Law (2003 Revision). Supervision of licensees is carried out through on-site and off-site examinations. A provision of the Banks and Trust Companies Law (2001 Revision) grants CIMA access to audited account information from licensees who are incorporated under the Companies Management Law (2001 Second Revision). The Companies Law (2001 Second Revision) institutes a custodial system in order to immobilize bearer shares. There are no shell banks on the Cayman Islands. CIMA is able to share information with like foreign regulatory authorities through the execution of memoranda of understanding. In June 2005, the CIMA signed a memorandum of understanding (MOU) with the U.S. Securities and Exchange Commission (SEC).

Money laundering regulations entered into force in late 2000 that specify employee training, record keeping, and "know your customer" (KYC) identification requirements for financial institutions and certain financial services providers; the regulations specifically cover individuals who establish a new business relationship, engage in one-time transactions over Cayman Islands (CI) $15,000 (approximately $18,000), or who may be engaging in money laundering. Amendments to the Proceeds of Criminal Conduct Law (PCCL) make failure to report a suspicious transaction a criminal offense that could result in fines or imprisonment.

Established under the Proceeds of Criminal Conduct (Amendment) Law 2003 (PCCL), the Financial Reporting Authority (FRA) replaces the former financial intelligence unit of the Cayman Islands. The FRA opened on January 12, 2004. Staff consists of the director, a legal advisor, an accountant, a senior analyst, a junior analyst, and an administrative officer. The FRA is a separate civilian authority governed by the Anti-Money Laundering Steering Group (AMLSG), which is chaired by the Attorney General. Other members of the AMLSG include the Financial Secretary, the Managing Director of the Cayman Islands Monetary Authority, the Commissioner of Police, the Solicitor General and the Collector of Customs. The FRA is responsible for, among other things, receiving, analyzing, and disseminating disclosures of financial information regarding proceeds or suspected proceeds, including those relating to the financing of terrorism. From June 2004 to June 2005, the FRA received 244 SARs. The FRA completed work on 195 out of 244 SARS. Of the 195, 107 required no further action, 88 were forwarded to foreign FIUs or law enforcement, and 29 were still in progress.

The Cayman Islands is subject to the U.S./UK Treaty concerning the Cayman Islands, relating to Mutual Legal Assistance in Criminal Matters. It is estimated that in approximately 230 cases the United States and the Cayman Islands have cooperated since the MLAT entered into force in 1990, and with respect to those cases, it is estimated that approximately $10 million has been shared with the Cayman Government. The Cayman Islands, through the United Kingdom, is subject to the 1988 UN Drug Convention. The Cayman Islands is a member of the Caribbean Financial Action Task Force (CFATF), and its FIU is a member of the Egmont Group.

The Cayman Islands is subject to The Terrorism (United Nations Measure) (Overseas Territories) Order 2001 (TUNMOTO). The Cayman Islands criminalized terrorist financing through the passage of

the Terrorism Bill 2003, which extends criminal liability to the use of money or property for the purposes of terrorism. It also contains a specific terrorist financing money laundering provision. In March 2005, the IMF published its assessment of the Cayman Islands (originally conducted in October 2003). The IMF found that the Cayman's regime for combating money laundering and the financing of terrorism is compliant with international standards.

The Cayman Islands should continue its efforts to implement its anti-money laundering regime.

Chile

Chile's large well-developed banking and financial sector stands out as one of the strongest in the region. With rapidly increasing trade and currency flows, the government is actively seeking to turn Chile into a global financial center. However, the Chilean Government continues to believe money laundering is not a significant threat. Stringent bank secrecy laws emphasizing privacy rights have been broadly interpreted and hamper Chilean efforts to identify and combat money laundering and terrorist financing. There is strong evidence that Chile's favorable reputation and incomplete regulatory oversight are attracting an increasing number of money launderers, particularly in the northern free trade zone and in the money exchange house sector. Money laundering in Chile appears to be primarily narcotics-related.

Money laundering in Chile is criminalized under Law 19.366 of January 1995 and Law 19.913 of December 2003. Prior to the approval of Law 19.913, Chile's anti-money laundering program was based solely on Law 19.366, which criminalized only narcotics-related money laundering activities. The law required only voluntary reporting of suspicious or unusual financial transactions by banks and offered no "safe harbor" provisions protecting banks from civil liability; as a result, the reporting of such transactions was extremely low. Law 19.366 gave only the Council for the Defense of the State (Consejo de Defensa del Estado, or CDE) authority to conduct narcotics-related money laundering investigations. The Department for the Control of Illicit Drugs (Departmento de Control de Trafico Ilícito de Estupefacientes) within the CDE functioned as Chile's financial intelligence unit (FIU) until a new FIU with broader powers (the Unidad de Análisis Financiero, or UAF) was created under Law 19.913.

Law 19.913 went into effect on December 18, 2003. Under Law 19.913, predicate offenses for money laundering are expanded to include (in addition to narcotics trafficking) terrorism in any form (including the financing of terrorist acts or groups), illegal arms trafficking, fraud, corruption, child prostitution and pornography, and adult prostitution.

Law 19.913 requires mandatory reporting of suspicious transactions by banks and financial institutions, financial leasing companies, general funds-managing companies and investment funds-managing companies, the Foreign Investment Committee, money exchange firms and other entities authorized to receive foreign currencies, firms that carry out factoring operations, credit cards issuers and operators, securities companies, money transfer and transportation companies, stock exchanges, stock exchange brokers, securities agents, insurance companies, mutual funds managing companies, forwards and options markets operators, tax free zones' legal representatives, casinos, gambling houses and horse tracks, customs general agents, auction houses, realtors and companies engaged in the land development business, and notaries and registrars. However, the law does not specify the parameters for determining suspicious activity. Each entity independently decides what constitutes irregularities in financial transactions. The law also does not grant any government or supervisory entity the authority to impose penalties for partial or non-compliance; in effect, there is still only voluntary—not compulsory—reporting of suspicious or unusual financial transactions.

In addition to reporting suspicious transactions, Law 19.913 also requires that obligated entities maintain registries of cash transactions that exceed 450 unidades de fomento (approximately $12,000),

and imposes record keeping requirements of five years. All cash transaction reports (CTRs) contained in the internal registries must be sent to the UAF at least once a year, or more frequently at the request of the UAF. In October 2005, the UAF issued a regulation requiring all banks to file these reports electronically and on a monthly basis. The Chilean tax service (Servicio de Impuestos Internos) has also issued a regulation, Resolution 120, requiring all banks, exchange houses and money remitters to report all transactions exceeding $10,000 sent to or received from foreign countries. The physical transportation of funds exceeding 450 unidades de fomento into or out of Chile must be reported to the customs agency, which then files a report with the UAF. These reports are sent to the UAF on a daily basis. However, Customs and other law enforcement agencies are not permitted to seize or otherwise stop the movement of funds, and the entry or exit of these funds is not subject to taxation.

Shortly after the passage of Law 19.913 in September 2003, portions of the new law—specifically those that dealt with the UAF's ability to gather information, impose sanctions, and lift bank secrecy provisions—were deemed unconstitutional by Chile's constitutional tribunal. The tribunal held that some of the powers granted to the UAF in the law violated privacy rights guaranteed by the constitution. The tribunal's decisions eliminate the ability of the UAF to request background information from government databases or from the reporting entities (including information on the reports they submit) and prevent UAF from imposing sanctions on entities for failure to file or maintain reports, or for failure to lift bank secrecy protections. The law went into effect in December 2003 without the above-mentioned powers. A new bill has been drafted to restore some of these powers to the UAF, but it has been stalled in Congress for over eighteen months. The bill was approved by the lower house in August 2005, but it is unlikely that further progress will be made until late 2006 due to the change in presidency that will take place in March.

The UAF began operating in April 2004, and began receiving suspicious transaction reports (STRs) from reporting entities in May 2004. The UAF receives approximately ten STRs from financial institutions per month. Suspicious transaction reports from financial institutions are received electronically, via a system known as SINACOFI (Sistema Nacional de Comunicaciones Financieras) that is used by banks to distribute information in an encrypted format among themselves and the Superintendence of Banks. Banks in Chile are supervised formally by the Superintendence of Banks and informally by the Association of Banks and Financial Institutions. Banks are obligated to abide by "know-your-customer" standards and other money laundering controls for checking accounts. However, savings accounts are not subject to the same compliance standards. Only a limited number of banks rigorously apply money laundering controls to non-current accounts.

The UAF has not yet developed a suspicious transaction disclosure form for entities other than banks and financial institutions, and therefore does not regularly receive STRs from non-financial institutions. Cash transaction reports are only reported upon request of the UAF. A major gap in Chile's efforts to combat money laundering is that non-bank financial institutions, such as money exchange houses, currently do not fall under the supervision of any regulatory body. The Superintendent of Casinos is the supervisory body for the seven casinos located throughout the country, but has no law enforcement or regulatory authority.

After receiving a suspicious transaction report, the UAF may request account information on the subject of the STR from the institution that filed the report. If the draft law is passed, the UAF will be able to request information from any entity that is required to file STRs, even if that entity did not file the STR that is being investigated. The draft law will also permit the UAF to request information from any entity that is not required to report suspicious transactions, if that information is necessary to complete the analysis of an STR, and will allow the UAF access to any government databases necessary for carrying out its duties. In order to perform these functions detailed in the draft law, the UAF will need the authorization of the Santiago Appeals Court. However, in the case of access to government databases, the UAF only needs court authorization for protected information, such as information related to taxes.

The Consejo de Defensa del Estado (CDE) continues to analyze and investigate any cases opened prior to the establishment of the UAF. Until June 2005, all cases that were deemed by the UAF to require further investigation were sent to the CDE. Beginning in June 2005, the Public Ministry (the public prosecutor's office) is responsible for receiving and investigating all cases from the UAF. To date, the Public Ministry has received only two cases from the UAF. Under the new law, the Public Ministry has the ability to request that a judge issue an order to freeze assets under investigation, and can also, with the authorization of a judge, lift bank secrecy provisions to gain account information if the account is directly related to an ongoing case. The Public Ministry has up to two years to complete an investigation and prosecution.

Primarily due to the above legislative restrictions and narrow interpretation of Law 19.913, no money laundering cases have been prosecuted to date. At the same time, the Chilean investigative police (PICH) and public prosecutor's office continue to cooperate with U.S. and regional law enforcement in money laundering investigations.

Chile's gaming industry consists of the Superintendent of Casinos, which is a supervisory body without law enforcement or regulatory authority, and seven casinos located throughout the country. However, Chile is engaged in sorting through international and domestic bids for 17 additional casinos legislated by the Chilean congress. There is currently no legal framework for regulating the money moving through the gaming industry.

One free trade zone exists in the northern region of Chile at Arica. The borders within the free trade zone are porous and largely unregulated. Reportedly, there are strong indications that money laundering schemes are rampant in the free trade zone, and Chilean resources to combat this issue are extremely limited.

Terrorist financing in Chile is criminalized under Law 18.314 and Law. 19.906. Law 19.906 went into effect in November 2003 and modifies Law 18.314 in order to sanction more efficiently terrorist financing in conformity with the UN International Convention for the Suppression of the Financing of Terrorism. Under Law 19.906, the financing of a terrorist act and the provision (directly or indirectly) of funds to a terrorist organization are punishable. The Superintendence of Banks circulates the UNSCR 1267 Sanctions Committee's consolidated list to banks and financial institutions.

No terrorist assets belonging to individuals or groups named on the list have been identified to date in Chile. If assets were found, the legal process that would be followed to freeze and seize them is still unclear; Law 19.913 contains provisions that allow for prosecutors to request that assets be frozen, based on a suspected connection to criminal activity. Government officials have stated that Chilean law is currently sufficient to effectively freeze and seize terrorist assets; however, the new provisions for freezing assets are based on provisions in the drug law, which at times have been interpreted narrowly by the courts. While assets have been frozen during two drug investigations, it is unclear how the new system would operate for a terrorist financing case. The Ministry of National Property currently oversees forfeited assets, and proceeds from the sale of forfeited assets are passed directly to the national regional development fund to pay for drug abuse prevention and rehabilitation programs. Under the present law, forfeiture is possible for real property and financial assets. Civil forfeiture is not permitted under current law.

Chile 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 Inter-American Convention on Terrorism. Chile has also signed but not ratified the UN Convention against Corruption. Chile is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the South American Financial Action Task Force on Money Laundering (GAFISUD). The CDE became a member of the Egmont Group of financial intelligence units in 1997, and the UAF was vetted by the Egmont Group in October 2004 to replace the CDE. The UAF has signed memoranda of understanding for the

exchange of financial information with Argentina, Australia, Bolivia, Brazil, Colombia, France, Guatemala, Korea, Mexico, Panama, Paraguay, Peru, Poland, Romania, Slovenia, Spain and the United States.

In the establishment of the UAF, the Government of Chile has created an FIU that meets the Egmont Group's definition of a financial intelligence unit. However, several weaknesses remain that hamper the operations of the UAF, such as its inability to sanction reporting entities or individuals for failure to file reports, its lack of access to information from other government agencies, and, reportedly, a very narrow interpretation of how the FIU should coordinate with law enforcement and other government agencies. Non-bank financial institutions represent a threat and should be subject to regulatory guidance and supervision. The continuation of these limitations will be a step backward, reversing the steps that have been taken in Chile over the past years to create a regime capable of investigating, punishing, and deterring financial crimes. With signs of growing money laundering, Chile lacks the legal ability to obtain necessary information and coordinate efforts to address these issues. Chile should take all necessary steps to ensure that the UAF and other key agencies are capable of effectively combating money laundering and terrorist financing.

China, People's Republic of

Money laundering remains a major concern as the People's Republic of China (PRC) restructures its economy. A more sophisticated and globally connected financial system in one of the world's fastest growing economies will offer significantly more opportunities for money laundering activity. Most money laundering cases now under investigation involve funds obtained from corruption and bribery. Narcotics trafficking, smuggling, alien smuggling, counterfeiting, fraud and other financial crimes remain major sources of laundered funds. Proceeds of tax evasion, recycled through offshore companies, often return to the PRC disguised as foreign investment, and as such, receive tax benefits. Continuing speculation following the July adjustment of the renminbi exchange rate system also fueled illicit capital flows into China throughout 2005. Hong Kong-registered companies figure prominently in schemes to transfer corruption proceeds and in tax evasion recycling schemes. The International Monetary Fund recently estimated that money laundering in China may total as much as $24 billion annually.

In 2005, China drafted a new Anti-Money Laundering Law, under the direction of a ministerial-level coordinating committee created in 2004. This new law is expected to broaden the scope of existing anti-money laundering regulations and to establish more firmly the Central Bank's authority over national anti-money laundering efforts. The new law was submitted to the National People's Congress Standing Committee at the end of 2005, but as of the end of December 2005, the NPC had not reviewed the draft legislation. The authorities expect the law to be passed in 2006.

China has taken steps to enhance its anti-money laundering regime. After conducting studies on how to strengthen the system, the People's Bank of China (PBC) and the State Administration of Foreign Exchange (SAFE) promulgated a series of anti-money laundering regulatory measures for financial institutions. These include: Regulations on Real Name System for Individual Savings Accounts, Rules on Bank Account Management, Rules on Management of Foreign Exchange Accounts, Circular on Management of Large Cash Payments, and Rules on Registration and Recording of Large Cash Payments.

Measures came into effect in 2004 that further strengthened China's anti-money laundering efforts, including a March 2004 PBC regulation entitled "Regulations on Anti-Money Laundering for Financial Institutions," which strengthens the regulatory framework under which Chinese banks and financial institutions must treat potentially illicit financial activity. The regulation effectively requires Chinese financial institutions to take responsibility for suspicious transactions, instructing them to create their own anti-money laundering mechanisms. Banks are required to report suspicious or large

foreign exchange transactions of more than $10,000 per person in a single transaction or cumulatively per day in cash, or non-cash foreign exchange transactions of $100,000 per individual or $500,000 per entity either in a single transaction or cumulatively per day.

Banks are also required to report large renminbi transactions, including single credit transfers of over 1 million RMB (approximately $120,500), cash transactions above 200,000 RMB (approximately $24,000), and domestic fund transfers of over 200,000 RMB, and are expected to report suspicious RMB transactions and refuse services to suspicious clients. Under the regulation, banks are further required to submit monthly reports to the PBC outlining suspicious activity and to retain transaction records for five years. Banks which fail to report on time can be fined up to the equivalent of approximately $3,600.

These measures complement the PRC's 1997 Criminal Code, which criminalized money laundering under Article 191 for three categories of predicate offenses, including narcotics trafficking, organized crime, and smuggling. In 2001, Article 191 was amended to add terrorism as a fourth predicate offense. Additionally, Article 312 criminalizes complicity in concealing the proceeds of criminal activity, and Article 174 criminalizes the establishment of an unauthorized financial institution. However, the class of existing predicate offenses needs to be expanded.

While official scrutiny of cross-border transactions is improving, the Chinese Government is also moving to loosen capital-account restrictions. For example, as of January 1, 2005, travelers can take up to 20,000 RMB (approximately $2,400) in or out of the country on each trip, up from 3,000 RMB (approximately $360) previously. New provisions allowing the use of RMB in Hong Kong have also created new loopholes for money laundering activity. Authorities are also allowing greater use of domestic, renminbi-denominated, credit cards overseas. Such cards can now be used in Hong Kong, Macau, Singapore, Thailand, and South Korea. To address online fraud, the PBOC tightened regulations governing electronic payments. In 2005, the Central Bank announced new rules that consumers could not make online purchases of more than RMB 1,000 (approximately $124) in any single transaction or more than 5,000 RMB (approximately $620) in a single day. Enterprises are limited to electronic payments of no more than 50,000 RMB (approximately $6,200) in a single day.

In 2003, the Chinese Government established a new banking regulator, the China Banking Regulatory Commission (CBRC), which assumed substantial authority over the regulation of the banking system. The CBRC has been authorized to supervise and regulate banks, asset management companies, trust and investment companies, and other deposit-taking institutions, with the aim of ensuring the soundness of the banking industry. One of its regulatory objectives is to combat financial crimes. However, primary authority for anti-money laundering efforts remains with the PBC, the country's Central Bank, along with the Ministry of Public Security in terms of enforcement.

In 2004, the PBC established a central national Financial Intelligence Unit (FIU) -the China Anti-Money Laundering Monitoring and Analysis Center, whose function is to collect, analyze and disseminate suspicious transaction reports and currency transaction reports. This move was an important accomplishment of the Anti-Money Laundering Strategy Team tasked with developing the legal and regulatory framework for countering money laundering in the banking sector. The team is chaired by a Vice-Governor of the PBC and is composed of representatives of the PBC's 15 functional departments

In September 2002, SAFE adopted a new system to supervise foreign exchange accounts more efficiently. The new system allowed for immediate electronic supervision of transactions, collection of statistical data, and reporting and analysis of transactions. A separate Anti-Money Laundering Bureau was established at the PBOC in late 2003 to coordinate all anti-money laundering efforts in the PBC and among other agencies, and to supervise the creation of the new FIU.

In spite of China's efforts, institutional obstacles and rivalries between financial and law-enforcement authorities continue to hamper Chinese anti-money laundering work and other financial law enforcement. Continuing efforts by some Chinese officials to strengthen the relatively weak legal framework under which money laundering offenses are currently prosecuted in the Chinese criminal code have yet to bear fruit. Furthermore, the current Anti-Money Laundering Law does not allow certain investigative practices commonly used with success in the United States. Also, anti-money laundering efforts are hampered by the prevalence of counterfeit identity documents and cash transactions conducted by underground banks, which in some regions reportedly account for over one-third of lending activities. China has increased efforts in recent years to crack down on such underground lending institutions. According to Chinese media reports, authorities shut down 155 underground banks dealing in $1.5 billion worth of illegal foreign exchange transactions between April and December 2004. Overall in 2004, 50 money laundering cases were jointly investigated by the police, the PBC and SAFE, according to the Chinese press.

A continued structural impediment is the absence of a nationwide automated network to monitor banking transactions through the PBOC. Many inter-banking transactions from one region to another are conducted manually, which delays the PBC's ability to prevent money laundering. As a result, weaknesses in the Chinese banking and criminal regulatory structure continue to be exploited by both domestic and foreign criminal enterprises.

To remedy these deficiencies, the PBOC launched a national credit-information system in early 2005. The system officially began operation in January 2006. Although still very limited, this system will allow banks to have access to information on individuals as well as on corporate entities. PBOC rules obligate financial institutions to perform customer identification and due diligence, and record keeping. However, there is currently no legislative instrument, only administrative rules, requiring customer due diligence and record keeping. SAFE implemented a new regulation on March 1, 2004 requiring non-residents, including those from Hong Kong, Macau, Taiwan, and Chinese passport holders residing outside mainland China, to verify their real names when opening bank accounts with more than $5,000.

The PRC supports international efforts to counter the financing of terrorism. Terrorist financing is now a criminal offense in the PRC, and the government has the authority to identify, freeze, and seize terrorist financial assets. Subsequent to the September 11, 2001, terrorist attacks in the United States, the PRC authorities began to actively participate in U.S. and international efforts to identify, track, and intercept terrorist finances, specifically through implementation of United Nations Security Council counterterrorist financing resolutions.

China's concerns with terrorist financing are generally regional, focused mainly on the western province of Xinjiang. Chinese law enforcement authorities have noted that China's cash-based economy, combined with its robust cross-border trade, has led to many difficult-to-track large cash transactions. There is concern that groups may be exploiting such cash transactions in an attempt to bypass China's financial enforcement agencies. While China is proficient in tracing formal foreign currency transactions, the large size of the informal economy—estimated by the Chinese Government at about 10 percent of the formal economy, but quite possibly larger—makes monitoring of China's cash-based economy very difficult.

The PRC signed the UN International Convention for the Suppression of the Financing of Terrorism on November 13, 2001, but has not ratified it. The PRC has signed mutual legal assistance treaties with 24 countries.

The United States and the PRC signed a mutual legal assistance agreement (MLAA) in June 2000, the first major bilateral law enforcement agreement between the countries. The MLAA entered into force in March 2001 and provides a basis for exchanging records in connection with narcotics and other criminal investigations and proceedings. The PRC is a party to the 1988 UN Drug Convention, and in

2003 ratified the UN Convention against Transnational Organized Crime. In January 2006, it ratified the UN Convention against Corruption.

The United States and the PRC cooperate and discuss money laundering and other enforcement issues under the auspices of the U.S.-PRC Joint Liaison Group's (JLG) subgroup on law enforcement cooperation. The JLG meetings are held periodically in either Washington, D.C., or Beijing. In addition, the United States and the PRC have established a Working Group on Counter-Terrorism that meets on a regular basis. The PRC has established similar working groups with other countries as well.

In late 2004, China joined the newly-created Eurasian Group (EAG), a Financial Action Task Force (FATF)-style regional group which includes Russia and a number of Central Asian countries. In January 2005, China became an observer to the FATF and desires to become a full member of the FATF.

In 2005, China's CBRC signed a memorandum of understanding with the Philippine Central Bank, Bangko Sentral ng Pilipinas, to share information on suspected money laundering activity. China's financial intelligence unit, the China Anti-Money Laundering Monitoring and Analysis Center, also signed its first MOU with a foreign counterpart at the end of 2005, with South Korea's FIU, allowing the two to exchange information related to money laundering, terrorism financing and other criminal financial activity.

The Government of the People's Republic of China should continue to build upon the substantive actions taken in recent years to develop a viable anti-money laundering/terrorist financing regime consistent with international standards. Important steps include expanding its list of predicate crimes to include all serious crimes, and continuing to develop a regulatory and law enforcement environment designed to prevent and deter money laundering. China should ensure that the FIU is an independent, centralized body with adequate collection, analysis and disseminating authority, including the ability to share with foreign analogs and law enforcement, and that a system of STR reporting is adequately implemented. It will be important for China's FIU to join the Egmont Group of Financial Intelligence Units as soon as possible to ensure it has access to vital financial information on possible illicit transactions occurring in other jurisdictions. China should provide for criminal penalties for non-compliance with requirements that financial institutions perform customer identification, due diligence, and record keeping, as well as incorporating the suspicious transaction-reporting requirement into law. China should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Colombia

The Government of Colombia (GOC) is a regional leader in the fight against money laundering. Comprehensive anti-money laundering legislation regulations have allowed the government to refine and improve its ability to combat financial crimes and money laundering. Nevertheless, the laundering of drug money from Colombia's lucrative cocaine and heroin trade continues to penetrate its economy and affect its financial institutions. Additionally, a complex legal system and limited resources for anti-money laundering programs constrain the effectiveness of the GOC's efforts. Laundering illicit funds is related to a number of criminal activities (narcotics trafficking, commercial smuggling for tax and import duty evasion, kidnapping for profit, and arms trafficking and terrorism connected to violent paramilitary groups and guerrilla organizations), and is carried out, to a large extent, by officially recognized foreign terrorist organizations. The GOC and U.S. law enforcement agencies are closely monitoring transactions that could disguise terrorist finance activities for local foreign terrorist organizations. The U.S. and Colombia exchange information and cooperation based on Colombia's 1994 ratification of the United Nations Convention against Illicit Trafficking in Narcotics and Psychotropic Substances. This convention extends into most money laundering activities that are the result of Colombia's drug trade.

Colombia's economy is robust and diverse and is fueled by a significant export sector that ships goods such as palm oil, textiles and apparel, flowers, and coffee to the U.S. and beyond. While Colombia is not a regional financial center, the banking sector is mature and well-regulated. An increase in financial crimes, such as bank fraud, not related to money laundering or terrorist financing, has not been widely seen in Colombia, although criminal elements have used the banking sector to launder money, under the guise of licit transactions. Money laundering has occurred in the non-bank financial system, especially related to transactions that support the informal or underground economy. Colombian money is also laundered through offshore centers, generally relating to transactions involving drug-related proceeds.

Financial institutions are required by law to maintain records of account holders and financial transactions for five years. This enables them to respond quickly to information requests from appropriate government authorities. Secrecy laws have not been an impediment to bank cooperation with law enforcement officials. They are required to issue suspicious activity reports (SARs) on any transaction that raises concern. Money laundering investigations are often initiated through the details provided by SAR reporting. Colombia's banks have strict compliance procedures, and work closely with the GOC, other foreign governments, and private consultants to ensure system integrity. Financial institutions are not exempted from compliance with law enforcement obligations, but compliance officers are not held liable under Colombian law for the content of their SARs. General negligence laws and criminal fraud provisions ensure the financial sector complies with its responsibilities while protecting consumer rights. Citizens are afforded rights to privacy, and investigations are carried out in accordance with legal requirements to protect those rights.

Colombian law is unclear over the government's authority to block assets of individuals and entities on the UN 1267 Sanctions Committee consolidated list. The government circulates the list widely among financial sector participants and banks are able to close accounts, but not seize assets. Banks also monitor other lists, such as OFAC publications, to ensure that services are denied to criminal elements, through the closing of accounts and denial of services. Charities and NGOs are regulated to ensure compliance with Colombian law and to guard against their involvement in terrorist activity. This regulation consists of several layers of scrutiny, including the regulation of incorporation and the tracing of suspicious financial flows through the collection of intelligence or SAR reporting. Reportedly, the GOC acknowledges that monitoring NGOs and charities is an issue that needs continued work and vigilance. Colombia is improving its ability to regulate alternative remittance systems. These systems include networks of informal cash remittances through family member connections or the use of smuggling rings that form the backbone of the black market peso exchange.

Money launderers in Colombia employ a wide variety of techniques. Trade-based money laundering, such as the Black Market Peso Exchange (BMPE), through which money launderers furnish narcotics-generated dollars in the United States to commercial smugglers, currency dealers, travel agents, investors and others in exchange for Colombian pesos in Colombia, remains a prominent method for laundering narcotics proceeds. Working with the Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Colombia established a prototype Trade Transparency Unit (TTU) that examined anomalies in trade data that could be indicative of customs fraud and trade-based money laundering. Analysis of suspect data showed a direct financial relationship between the narcotic cartels and the terrorist organization, the Revolutionary Armed Forces of Colombia (FARC).

Colombia also appears to be a significant destination and transit location for bulk shipment of narcotics-related U.S. currency. Local currency exchangers convert narcotics dollars to Colombian pesos and then ship the U.S. currency to Central America and elsewhere for deposit as legitimate exchange house funds that are then reconverted to pesos and repatriated by wire to Colombia. Other methods include the use of debit cards to draw on financial institutions outside of Colombia and the transfer of funds out of and then back into Colombia by wire through different exchange houses to create the appearance of a legal business or personal transaction. Colombian authorities have also

noted increased body smuggling of U.S. and other foreign currencies and an increase in the number of shell companies operating in Colombia. Smart cards, internet banking, and the dollarization of the economy of neighboring Ecuador represent some of the growing challenges to money laundering enforcement in Colombia.

From a money laundering standpoint, casinos in Colombia lack regulation and transparency, making them a target ripe for abuse. Free trade zones in some areas of the country likewise present opportunities for smugglers to take advantage of lax customs regulations, or the corruption of low-level officials to move products into the informal economy. Although corruption of government officials remains a problem, it has not been reported as widespread. The GOC has taken dramatic steps to ensure the integrity of its most sensitive institutions and senior government officials.

Colombia has broadly criminalized money laundering. In 1995, Colombia established the "legalization and concealment" of criminal assets as a separate criminal offense. Also, in 1997, Colombia more generally criminalized the laundering of the proceeds of extortion, illicit enrichment, rebellion, and narcotics trafficking. Effective in 2001, Colombia's criminal code extended the predicate offenses of money laundering to include arms-trafficking, crimes against the financial system or public administration and criminal conspiracy. Penalties under the criminal code range from two to six years with possibilities for aggravating enhancements of up to three-quarters of the sentence. Persons who acquire proceeds from drug trafficking are subject to a potential sentence of six to fifteen years, while illicit enrichment convictions carry a sentence of six to ten years. Failure to report money laundering offenses to authorities, among other offenses, is itself an offense punishable under the criminal code, with penalties increased in 2002 to imprisonment of two to five years.

Colombian law provides for both conviction-based and non-conviction-based in rem forfeiture, giving it some of the most expansive forfeiture legislation in Latin America. A general criminal forfeiture provision for intentional crimes has existed in Colombian Penal Law since the 1930s. Since then, Colombia has adopted more specific criminal forfeiture provisions in other statutes, most notably those containing Colombia's principal counternarcotics statute, Law 30 of 1986. In 1996, Colombia added non-conviction-based forfeiture with the enactment of Law 333 of 1996, which established a process that allows for the extinguishing of ownership rights for assets tainted by criminal activity. This process is only a first step in Colombian law that requires a second judicial procedure to transfer the title from the original owner to the GOC. This second procedure can take years if the original owner decides to fight the transfer. Despite an expansive legislative regime, procedural and other difficulties led to only limited forfeiture successes in the past, with substantial assets tied up in proceedings for years. However, in 2002 the counternarcotics and maritime unit of the prosecutor general's office used Law 333 to successfully forfeit $35 million of U.S. currency seized in 2001 with the assistance of DEA.

In 2002, the GOC took additional forceful measures to remove practical obstacles to the effective use of forfeiture to combat crime. In September, the GOC issued a decree to suspend application of Law 333 and implement more streamlined procedures in forfeiture cases. These reforms were refined and formally adopted through the enactment of Law 793 of 2002. Among other things, Law 793 repeals Law 333 and establishes new procedures that eliminate interlocutory appeals that prolonged and impeded forfeiture proceedings in the past, imposes strict time limits on proceedings, and places obligations on claimants to demonstrate their legitimate interest in property. In addition, Law 793 requires expedited consideration of forfeiture actions by judicial authorities, and establishes a fund for the administration of seized and forfeited assets. The amount of time for challenges was shortened and the focus was moved from the accused to the seized item (cash, jewelry, boat, etc.), placing more burdens on the accused to prove the item was acquired with legitimately obtained resources.

In December 2002, the GOC strengthened its ability to administer seized and forfeited assets by enacting Law 785 of 2002. This statute provides clear authority for the National Drug Directorate

(DNE) to conduct interlocutory sales of seized assets and contract with entities for the management of assets. Notably, Law 785 also permits provisional use of seized assets prior to a final forfeiture order, including assets seized prior to the enactment of the new law. In 2004, the department of administration of property within the prosecutor general's office seized nearly 17,000 properties. The DNE, with assistance from the United States Marshals Service, has developed a modern asset management and electronic inventory system for seized assets.

The Colombian government has been aggressively pursuing the seizure of assets obtained by drug traffickers through their illicit activities. As a prime example, for the last two years the CNP/SIU, in conjunction with DEA, OFAC, and the Colombian Fiscalia (prosecutor's office) have been investigating the Cali cartel business empire under the Rodriguez Orejuela brothers. A series of investigations designed to identify and seize assets either purchased by money gained through illegal drug activity or assets used to launder drug proceeds took place under the name Operation Dinastia.

On October 21, 1995, pursuant to Executive Order 12978, the Treasury Department's Office of Foreign Assets Control (OFAC) added the Colombian drugstore chain Drogas la Rebaja (which later changed its name to evade U.S. sanctions) to its specially designated narcotics traffickers (SDNT) list because it was owned or controlled by Cali cartel leaders Miguel and Gilberto Rodriguez Orejuela (currently in custody in the U.S. awaiting trial). After a lengthy investigation by Colombian Law enforcement, on September 16, 2004, the CNP/SIU mobilized 3,200 police officers and 465 fiscales (Colombian prosecutors) nationwide in order to seize approximately 480 retail stores of the Drogas la Rebaja drug store chain. As part of the operation, the largest pharmaceutical laboratory in Colombia was seized as well. This is the largest asset forfeiture in Colombian history to date. The operation took place in 28 of the 32 Colombian departments over a three day period. The Colombian Direccion Nacional de Estupefacientes (DNE) took control of the stores and has replaced the top 24 company executives with DNE administrators. All 4,200 company employees continue to work, but all company profits will be utilized by the Colombian government in furtherance of counternarcotics programs.

The public and political response to asset forfeiture has been positive. Press reports have been matter-of-fact concerning asset seizure operations, and the court-sanctioned nature of the seizure orders mitigates political pressure. In general, Colombians recognize the relationship between criminals and their illicitly gotten gains. The banking sector has been cooperative with law enforcement activity based on judicial order. Banks and other financial sector entities are also mindful of USA PATRIOT Act provisions that require action against criminals that fall under the jurisdiction of that act. Criminals in Colombia often act violently against vigorous law enforcement activities. As a result, GOC officials at all levels of involvement must guard against retaliatory action taken by criminal elements.

Colombia formally adopted legislation in 1999 to establish a unified, central financial intelligence unit (FIU), the "Unidad de Informacion y Anlisis Financiero" (UIAF), that is located within the Ministry of Finance and Public Credit. The UIAF, which currently has 45 personnel, has broad authority to access and analyze financial information from public and private entities in Colombia. Obligated entities (including financial institutions, institutions regulated by the Superintendence of Securities and the Superintendence of Notaries, export and import intermediaries, credit unions, wire remitters, exchange houses and public agencies) are required to file suspicious transaction reports with the UIAF, and are barred from informing their clients of their reports. Most obligated entities are also required to establish "know-your-customer" provisions. Exchange houses must file currency reports for transactions involving $700 or more. In 2005, 8,227 SARs were filed; however, financial institutions are believed to underreport transactions.

The UIAF is widely viewed as a hemispheric leader in efforts to combat money laundering and supplies considerable expertise in organizational design and operations to other financial intelligence units in Central and South America. The UIAF is a member of the Egmont Group of financial

intelligence units, and the UIAF director currently serves in the capacity as vice-chair of the Egmont Committee. Although FIUs are not required to sign agreements amongst themselves in order to exchange information under the auspices of the Egmont Group, the Colombian FIU has signed memoranda of understanding with 27 FIUs around the world.

The UIAF is currently working on a project called SCCI (Sistema Centralizado de Consultas de Informacion) that connects 17 governmental entities as well as one private sector association (Asobancaria). SCCI will allow these entities to exchange information online and share their databases in a secure manner. The pilot phase of the project was made possible due to USG financial contributions. It is expected that SCCI will be operational in April 2006.

Currency transactions and cross-border movements of currency in excess of $10,000 must also be reported to the UIAF, and certified money couriers must be used for the cross-border movements of currency. Colombia has criminalized cross-border cash smuggling and defines it as money laundering. However, customs officials are inadequately equipped to detect cross-border currency smuggling. Workers rotate frequently producing inadequately trained staff. In addition, the individual customs officials are held liable for any inspected article that they damage, causing hesitation in conducting thorough inspections. Reportedly, corruption is also a problem. It has also been noted that customs officials lack the proper technical equipment necessary to do their job. The GOC has been slow to make needed changes.

Bilateral cooperation between the GOC and the USG remains strong and active. In 1998, DEA established a sensitive investigative unit (SIU) within the Colombian administrative security (DAS) to investigate drug trafficking and money laundering organizations. In late 2003, the SIU arrested 21 money laundering facilitators in support of a U.S. operation based in south Florida. This operation exposed numerous flower export companies operating in Colombia as fronts for money laundering activities, and resulted in the seizure of over $17 million.

A financial investigative unit, formed within the Colombian National Police intelligence and investigations unit (DIJIN) in 2002, has worked several cases, some of which have been closed by investigation and arrests. This unit works closely with the Immigration and Customs Enforcement agency (ICE) of the U.S. Department of Homeland Security. The cases are financial in nature and include money laundering and terrorist financing, and many are the subject of extradition proceedings, including several that involve high profile defendants.

Although terrorism is already an autonomous crime under Colombian law, there is no legislation criminalizing the financing of terrorism. A draft law has been introduced to amend the penal code to define and criminalize direct and indirect financing of terrorism, of both national and international terrorist groups. Per GAFISUD and Egmont Group recommendations, the UIAF will receive SARs regarding terrorist financing. The new law will allow the UIAF to freeze terrorists' assets immediately after their designation. In addition, banks will now be held responsible for their client base. Banks will be required to immediately inform the UIAF of any accounts held by newly designated terrorists. Banks will also have to screen new clients against the current list of designated terrorists before the banks are allowed to provide prospective clients with services. Previously, banks were not legally required to comply either of these regulations, but many had complied regardless. The bill has been presented to Congress and currently awaits approval. The proposal may be delayed due to congressional elections in March 2006, with the new congress taking office in July 2006. President Uribe reportedly supports the new legislation.

Colombia plays a strong role in multilateral efforts to combat money laundering. In addition to its membership in Egmont, Colombia is a member of the Financial Action Task Force of South America Against Money Laundering (GAFISUD). In 2004 Colombia was a participant on the GAFISUD Executive Director Selection Committee and on the Budget Committee. Colombia also underwent a mutual evaluation by GAFISUD in 2004, and Colombia continued to provide experts for the mutual

evaluations of other GAFISUD countries. Colombia is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group, which it chaired in 2005. In October 2004, Colombia became a party to the UN International Convention for the Suppression of the Financing of Terrorism. The GOC is a party to the UN Convention Against Transnational Organized Crime and has signed, but not ratified, the UN Convention Against Corruption.

Although Colombia has a strong financial intelligence unit and comprehensive anti-money laundering laws and regulations, there are still several weaknesses that should be corrected. Enforcement continues to be a challenge for Colombia. Limited resources for prosecutors and investigators have made financial investigations problematic. Continued difficulties in establishing the base predicate offense further contributes to Colombia's limited success in achieving money laundering convictions and successful forfeitures of criminal property. Congestion in the court system, procedural impediments and corruption remain continuing problems. Colombia has not yet criminalized the financing of terrorism, although terrorist financing crimes can be prosecuted under other sections of law. The GOC should move promptly on the legislation, specifically criminalize the financing of terrorism, further eliminate procedural impediments, and take other necessary steps to further strengthen its anti-money laundering and counterterrorist financing programs.

Comoros

The Union of Comoros (Comoros) is not a principal financial center for the region. An anti-money laundering (AML) law, which addresses many of the primary AML issues of concern, was passed by Presidential Decree in 2004. However, Comorian authorities lack the capacity to effectively implement and enforce the legislation. Comoros consists of three islands: Grande Comore, Anjouan and Moheli. An ongoing struggle for influence continues between the Union and island presidents. Political instability remains a concern. Since independence from France in 1975, there have been 19 coups or coup attempts. Union President Azali Assoumane took power in a coup in 1999 and subsequently was elected in 2002 Union presidential elections described by international observers as free and fair. Elections for a new Union President are scheduled to occur in 2006, drawing on candidates from Anjouan, as required by the Union constitution in an effort to facilitate power-sharing among the islands. While broad principles have been agreed upon, some details of the new federal legal system remain to be decided upon, and both Moheli and Anjouan continue to retain much of their autonomy, particularly with respect to their security services, economies, and banking sectors.

The 2004 federal-level AML law is based on the French model. The main features of the law are that it: 1) requires financial and related records to be maintained for five years; 2) permits assets generated or related to money laundering activities to be frozen, seized and forfeited; 3) requires residents to declare all currency or financial instruments upon arrival and departure, and non-residents to declare all financial instruments upon arrival and all financial instruments above Comorian Francs 500,000 ($1,250) on departure; 4) permits provision and receipt of mutual legal assistance with another jurisdiction where a reciprocity agreement is in existence and confidentiality of financial records is respected; 5) requires non-bank financial institutions to meet the same customer identification standards and reporting requirements as banks; 6) requires banks, casinos and money exchangers to report unusual and suspicious transactions (by amount or origin) to the Central Bank and prohibits cash transactions over Comorian Frances 5 million ($12,500); and, 7) criminalizes the provision of material support to terrorists and terrorist organizations. There is no financial intelligence unit or comparable agency in existence in the country.

Federal authorities have a limited ability to implement AML laws in Anjouan and Moheli. Similarly, the island governments of Anjouan and Moheli may have limited control over AML matters. Although Moheli has its own AML law in effect (the Anti-Money Laundering Act of 2002), the law itself has

some serious shortcomings and authorities lack the resources and expertise to enforce its provisions. For example, there is no absolute requirement to report large cash transactions. Comprehensive information on Anjouan's laws and regulations is difficult to obtain, but it does not appear that Anjouan has an AML law, or any legal requirement for offshore banks to maintain records or take any action when confronted with money laundering activities, be they suspected or confirmed. As is the case with Moheli, Anjouan also lacks resources and expertise to address money laundering and related financial crimes. In 2005, Anjouan's island president, Bacar Mohamed, recognized Anjouan's inability to regulate its offshore sector and requested USG assistance to combat misrepresentation of his government in connection with the offshore sector. He denied his government was in any way involved with a website portraying itself as the Government of Anjouan's offshore licensing authority and sought to have the site shut down.

Union President Azali has made efforts to bring AML enforcement under Union government jurisdiction. In May 2005, he issued a note to the Ministry of Finance, the islands' presidents, and the Public Prosecution Department urging these institutions to take action with regard to any illegal offshore banking practices. The note indicated that all banking and financial institutions operating within the jurisdiction of the Union of Comoros, whether offshore or onshore, must abide by the provisions of legislation No. 80-7 of May 3, 1980. According to article 7 of this legislation, a bank or any other financial institution cannot operate in the Union of Comoros without prior authorization from the Union of Comoros Finance Minister upon recommendation from the Comoros Central Bank. Thus, offshore banks operating in the autonomous islands of the Union of Comoros without prior authorization from the Union of Comoros Finance Minister contravene the May 3, 1980 legislation. Consequently, Azali's note directed the ministries and other government institutions responsible for banking and financial matters to take (or to see to it that the necessary measures are taken) to put an end to this "blatant illegality which is prejudicial to the Union of Comoros." Also in May 2005, President Azali told the USG that the Comorian government is prepared to bring to justice the beneficiaries of illegal offshore licenses and sought the assistance and support of the USG in this endeavor.

While the Comoros is not a principal financial center for the region, Moheli and Anjouan may have attempted or may be attempting to develop an offshore financial services sector as a means to finance government expenditures. The Anjouan island government's claim that unrelated companies are presenting themselves as licensed by the government of Anjouan makes authoritative information on Anjouan's offshore sector difficult to establish. Both Moheli, pursuant to the International Bank Act of 2001, and Anjouan, pursuant to the Regulation of Banks and Comparable Establishments of 1999, license off-shore banks. Together, the islands have licensed more than 100 banks. Applicants for banking licenses in either jurisdiction are not required to appear in person to obtain their licenses. In Anjouan, only two documents (a copy of the applicant's passport and a certificate from a local police department certifying the lack of a criminal record) are required to obtain an offshore license and fax copies of these documents are acceptable. Even if additional information was to be required, it is doubtful that either jurisdiction has the ability or resources to authenticate and verify the information. Neither jurisdiction is capable, in terms of expertise or resources, of effectively regulating an offshore banking center. Anjouan, and probably Moheli as well, has delegated much of its authority to operate and regulate the offshore business to private, non-Comorian domiciled parties. In November 2004, Anjouan island government officials denied island government involvement in the offshore sector. They said the Union of Comoros Central Bank was the only authority for the offshore banking sector in the country and insisted the Anjouan island government had not established its own central bank. They admitted that several years earlier the government of Anjouan considered starting an offshore banking sector, but they had not pursued it.

In addition to offshore banks, both Moheli, pursuant to the International Companies Act of 2001, and Anjouan, pursuant to Ordinance Number 1 of 1 March 1999, license insurance companies, internet

casinos, and international business companies (IBC's)—Moheli alone claims to have licensed over 1200 IBC's. Bearer shares of IBC's are permitted under Moheli law. Anjouan also forms trusts, and registers aircraft and ships as well (without requiring an inspection of the aircraft or ship in Anjouan).

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

The Government of the Union of the Comoros (GOC) should harmonize anti-money legislation for the three islands that comprise the federal entity. A unified financial intelligence unit should be established and the unregulated offshore financial sectors in Moheli and Anjouan should either be regulated by federal authorities or be shut down. In either case, bearer shares should be immobilized. The deficiencies in the anti-money laundering/terrorist financing regimes in the Comoros, and the GOC's inability to implement existing legislation make it vulnerable to traditional money laundering and to the financing of terrorism. Comoros should make every effort to comport to international standards. Comoros should specifically criminalize the financing of terrorism.

Cook Islands

The Cook Islands is a self-governing parliamentary democracy in free association with New Zealand and a member of the British Commonwealth. Cook Islanders are citizens of New Zealand.

After the Government of the Cook Islands remedied deficiencies in its anti-money laundering regime, the Financial Action Task Force (FATF) removed the Cook Islands from its Non-Cooperative Countries and Territories list in February 2005. The Cooks had been on the list since 2000. The FATF is conducting a year-long program, due to conclude in February 2006, to closely monitor the islands. The Cook Islands is scheduled for a mutual evaluation in 2008.

By enacting The Financial Transactions Reporting Act (FTRA) 2003, and eight other legislative acts on May 7, 2003, and additional legislation in 2004, Cook Islands authorities strengthened its anti-money laundering/counterterrorism financing (AML/CTF) legal and institutional framework. Reviews are underway to consider how the AML/CTF legislation affects other domestic laws. The Financial Supervisory Commission (FSC), regulator of the licensed financial sector, expects new insurance legislation to be drafted beginning in 2006.

The Financial Transactions Reporting Act (FTRA) 2003, and the updated 2004 amendment, require financial and other institutions to conduct due diligence, ongoing monitoring of customers and transactions, suspicious activity reporting, development and maintenance of internal procedures for compliance, and audit and record keeping. The Act provides for administrative and penal sanctions on institutions for noncompliance.

The FTRA imposes certain reporting obligations on institutions in 26 categories, including banks, offshore banking businesses, offshore insurance businesses, casinos, gambling services, insurers, financial advisors, solicitors/attorneys, accountants, financial regulators, lotteries, and money remitters. The Minister of Finance can extend the reporting obligation to other businesses.

Financial institutions are required to retain all records related to the opening of accounts and financial transactions for a minimum of six years. The records must include sufficient documentary evidence to prove the customer's identity. In addition, financial institutions are required to develop and apply internal policies, procedures, and controls to combat money laundering and to develop audit functions to evaluate such policies, procedures, and controls. Financial institutions must comply with any guidelines and training requirements issued under the amended FTRA 2004.

Financial institutions are required to make currency transaction reports and suspicious transaction reports to the Financial Intelligence Unit (FIU). Those requirements apply to all currency transactions

of NZ$10,000 (approximately $6870) and above; electronic funds transfers of NZ$10,000 and above; transfers of currency, into and out of the Cook Islands, in excess of NZ$10,000; and, any suspicious transactions. Failure to declare such transactions could incur penalties. Institutions obligated to file Suspicious Transaction Reports to the FIU are banks, insurers, financial advisors, bureaux de change, solicitors/attorneys, accountants, financial regulators, casinos, lotteries, money remitters, and pawn shops. In 2005, the FIU received 10 Suspicious Transaction Reports, 566 Cash Transaction Reports, 1,763 Electronic Funds Transaction Reports , and 12 Border Currency Reports. To date, 30 of the 47 Suspicious Transaction Reports have related to non-residents.

The FTRA establishes the supervision and authority of the FIU, including cooperation with supervisors. The FIU is the central unit responsible for processing disclosures of financial information in accordance with anti-money laundering and antiterrorist financing regulations. It became fully operational with the assistance of a Government of New Zealand technical advisor. The FIU has the authority to require reporting institutions to supplement reports. It has broad powers to obtain information required to combat money laundering and the financing of terrorism, including information from any law enforcement agency and supervisory body. The FIU is required to destroy a suspicious transaction report if there has been no activity or information related to the report or to a person named in the report for six years. The FIU does not have an investigative mandate. If it determines that a money laundering offense has been, or is being, committed, it must refer the matter to law enforcement for investigation. The Minister of Finance, who is responsible for administrative oversight, appoints the head of the FIU.

The Cook Islands FIU (CIFIU) is participating in an FIU database project provided by AUSTRAC, the Australian FIU. The CIFIU recently received the database and is now capturing data stored while the database was being developed and tested. The Pacific FIU Database Project includes other jurisdictions that will receive versions of the same database framework.

The Banking Act 2003 and the Financial Supervisory Commission Act 2003 (FSCA 2003) established a new framework for licensing and prudential supervision of domestic and offshore financial institutions in the Cook Islands. The legislation in effect requires offshore banks to have a physical presence in the Cook Islands (the “mind and management” principle), transparent financial statements, and adequate records prepared in accordance with consistent accounting systems. The physical presence requirement was intended to ensure that the Cook Islands would have no shell banks by June 2004. All banks are subject to a vigorous and comprehensive regulatory process, including on-site examinations and supervision of activities.

The legislation established the Financial Supervisory Commission (FSC) as the licensed financial sector’s sole regulator. The FSC is empowered to license, regulate, and supervise the business of banking. It serves as the administrator of the legislation that regulates the offshore financial sector. The FSC can license international banks and offshore insurance companies and register international companies. It also supervises trust and company service providers. The FSC regulates three domestic banks, four international banks, six trustee companies, and eight offshore and three domestic insurance companies. Its policy is to respond to requests from overseas counterparts to the utmost extent possible. The FSC has taken a broad interpretation of the concept of “counterpart” and does not need to establish general equivalence of function before being able to cooperate.

The FTRA requires the FSC to assess the compliance by licensed financial institutions with anti-money laundering regulations. Resulting reports and documentation are provided to the FIU. The FIU is responsible for assessing compliance by non-licensed institutions.

Licensing requirements, as set out in the legislation, are comprehensive. The Banking Act 2003 and a Prudential Statement on Licensing issued in February 2004 contain detailed licensing criteria for both locally incorporated and foreign banks, including “fit and proper” criteria for shareholders and officers, satisfactory risk management, accounting and management control systems, and minimum

capital requirements. The Banking Act 2003 defines banking business, prohibits the unauthorized use of the word "bank" in a company name, and requires prior approval for changes in significant shareholding.

The Cook Islands has an offshore financial sector that licenses international banks and offshore insurance companies and registers international business companies. It also offers company services and trusts, particularly asset protection trusts that contain a "flee clause." Flee clauses state that if a foreign law enforcement agency makes an inquiry regarding the trust, the trust will be transferred automatically to another jurisdiction.

The domestic banking system is comprised of branches of two major Australian banks and the local Bank of the Cook Islands (BCI). The latter is the result of a 2001 merger of the Government-owned Cook Islands Development Bank and the Post Office Savings Bank. Domestic banks are primarily involved in traditional deposit taking and lending. The BCI operates as a stand-alone institution competing against the two Australian banks and is no longer engaged in development lending. Legislation allows for development lending to be undertaken in the future by a separate company not subject to supervision by the FSC. In addition, non-performing loans made by the Cook Islands Development Bank have been transferred to another affiliated company.

Progress since June 2004 includes the Cook Islands' response to the issues surrounding implementation of the AML/CFT regime. The head of the FIU chairs the Coordinating Committee of Agencies and Ministries, which promotes, formalizes and maintains coordination among relevant government agencies, assists the Government in the formulation of policies related to AML/CFT issues, and enables government agencies to share information and training resources gathered from their regional and international networks, including meetings or training seminars attended by their officials. The AML/CFT consultative group of stakeholders facilitates consultation between government and the private sector and ensures all financial sector "players" are involved in the decision making and problem solving process regarding AML/CFT regulations and reporting. The FIU is also a member of the Anti-Corruption Committee, along with the Office of the Prime Minister, Police, Crown Law, Audit Office, and the Financial Secretary.

The GOCI is an active member of the Asia/Pacific Group on Money Laundering (APG) with representation on the Steering Group, chairmanship of the Implementation Issues Working Group, and membership in the Typologies Working Group. The FIU became a member of the Egmont Group in June 2004, has bilateral agreements allowing the exchange of financial intelligence with Australia, and is negotiating a memorandum of understanding (MOU) with Thailand. All other exchanges have not required MOUs and have involved New Zealand, the United States, Hong Kong, Singapore, India, the United Kingdom, and several others. The Cook Islands is considering membership in the Offshore Group of Banking Supervisors (OGBS). The Cook Islands has received eight requests for mutual legal assistance since the Mutual Assistance in Criminal Matters Act came into force in 2003. Four have been answered, and four are pending, two of which were received in late 2005. The Cook Islands has not received any extradition requests, but successfully extradited one person from New Zealand. This court case is due to commence in February 2006

The GOCI is a party to the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. It is a party to the UN Convention against Transnational Organized Crime and to the UN International Convention for the Suppression of the Financing of Terrorism. The Terrorism Suppression Act 2004—based on the model law drafted by an expert group established under the auspices of the Pacific Islands Forum Secretariat. The Act criminalizes the commission and financing of terrorism. The United Nations (Security Council Resolutions) Act 2003 allows the Cook Islands, by way of regulations, to give effect to the Security Council resolutions concerning international peace and security.

The Cook Islands should continue to implement legislation designed to strengthen its nascent institutions, should maintain vigilant regulation of its offshore financial sector, and should abolish "flee clauses" in new asset protection trusts to ensure that it comports with international standards.

Costa Rica

Costa Rica is not a major financial center, but it remains vulnerable to money laundering and other financial crimes. This is due in part to narcotics trafficking in the region, particularly of South American cocaine, and the presence in Costa Rica of Internet gaming companies. Reforms to the Costa Rican counternarcotics law in 2002, which expand the scope of anti-money laundering regulations, also create a loophole by eliminating the government's licensing and supervision of casinos, jewelers, realtors, attorneys, and other non-bank financial institutions. No actions were taken to close this loophole in 2005. Gambling is legal in Costa Rica, and there is no requirement that the currency used in Internet gaming operations be transferred to Costa Rica. Currently, over 250 sports-book companies have registered to operate in Costa Rica. Many of these registered firms have the same owners and addresses.

In 2002, the Government of Costa Rica (GOCR) expanded the scope of Law 7786 via Law 8204. This expansion criminalizes the laundering of proceeds from all serious crimes. Serious crimes are defined as carrying a sentence of four years or more. Law 8204 also obligates financial institutions and other businesses (such as money exchangers) to identify their clients, report currency transactions over $10,000, report suspicious transactions, keep financial records for at least five years, and identify the beneficial owners of accounts and funds involved in transactions. While Law 8204, in theory, covers the movement of all capital, current regulations, based on Law 8204, Chapter IV, Article 14, apply a restrictive interpretation that covers only those entities that are involved in the transfer of funds as a primary business purpose.

The formal banking industry in Costa Rica is tightly regulated. However, the offshore banking sector that offers banking, corporate, and trust formation services remains open and is an area of concern. Foreign-domiciled "offshore" banks can only conduct transactions under a service contract with a domestic bank, and they do not engage directly in financial operations in Costa Rica. Costa Rican authorities acknowledge that they are unable to adequately assess risk. Costa Rican financial institutions are regulated by the Office of the Superintendent of Financial Institutions (SUGEF).

Currently, six offshore banks maintain correspondent operations in Costa Rica, three from the Bahamas and three from Panama. The GOCR has supervision agreements with its counterparts in Panama and the Bahamas, permitting the review of correspondent banking operations. These counterpart regulatory authorities occasionally interpret the agreements in ways that limit review by Costa Rican officials. In September 2005, the GOCR's Attorney General ("Procurador General") ruled that SUGEF has no authority to regulate offshore operations. The ruling was an attempt to clarify apparent contradictions between the 1995 Organic Law of the Costa Rican Central Bank and Law 8204. Draft legislation to correct the contradiction and reassert SUGEF's regulatory power is under review in the Legislative Assembly. However, it is unclear when the Legislative Assembly will take action on this draft legislation.

All persons carrying cash are required to declare any amount over $10,000 to Costa Rican officials at ports of entry. During 2005, officials seized over $850,000, much of it in undeclared cash. In 2004, the GOCR seized $1.2 million.

Eighteen free trade zones operate within Costa Rica, primarily producing electronics, integrated circuits, textiles, and medicines for re-export. The Zones are under the supervision of "PROCOMER" an export-promotion entity. Costa Rican authorities report no indications of trade-based money

laundering schemes in the zones. PROCOMER strictly enforces control over the zones, but its measures are aimed primarily at preventing tax evasion.

Costa Rica's Financial Intelligence Unit (FIU) became operational in 1998 and was admitted into the Egmont Group in 1999. The unit is analytical, screening cases for referral to prosecutors. The FIU has access to the records and databases of financial institutions and other government entities but must obtain a court order if the information collected is to be used as evidence in court. The unit has no regulatory responsibilities. The unit remains ill equipped and under-funded to handle its current caseload (over 120 cases for 2005) and to provide the information needed by investigators. Nevertheless, in 2004, the unit developed evidence it considered formidable in four high-profile cases of money laundering. Three of those cases were successfully prosecuted in 2005. Three additional money-laundering cases began judicial proceedings in 2005, and the FIU assisted international investigators to develop evidence in four more cases.

Costa Rican authorities have received and circulated to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224.

However, these authorities cannot block, seize, or freeze property without prior judicial approval. Thus, Costa Rica lacks the ability to expeditiously freeze assets connected to terrorism. No assets related to designated individuals or entities were identified in Costa Rica in 2005. An interagency effort is underway to reduce the time required to obtain such judicial approval.

The GOCR has ratified the major UN counterterrorism conventions. In 2002, a government task force drafted a comprehensive counterterrorism law with specific terrorist financing provisions. The draft law would expand existing conspiracy laws to include the financing of terrorism. It would also enhance existing narcotics laws by incorporating the prevention of terrorist financing into the mandate of the Costa Rican Drug Institute. In 2004, the Legislative Assembly considered a separate draft terrorism law. In July of 2005, the Assembly's Narcotics Committee approved a bill combining the two proposals, but no further progress has been made.

Costa Rica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. The GOCR has signed, but not yet ratified, the UN Convention against Corruption. The GOCR has also signed the OAS Inter-American Convention on Mutual Assistance in Criminal Matters, and is a member of the Caribbean Financial Action Task Force (CFATF) and the aforementioned Egmont Group.

The GOCR should pass legislation that clarifies contradictions regarding the supervision of its offshore banking sector, and should extend its anti-money laundering regime to cover the Internet gaming sector, exchange houses, gem dealers, casinos and other non-bank financial institutions. Costa Rica also should pass counterterrorism and terrorist finance legislation.

Côte d'Ivoire

Cote d'Ivoire is an important West African regional financial hub. Money laundering occurs, but the government does not consider Cote d'Ivoire to be a financial center for money-laundering.

Money laundering and any terrorist financing present in Cote d'Ivoire are not primarily related to narcotics proceeds. Criminal proceeds that are laundered are reportedly derived from regional criminal activity, such as the smuggling of consumer goods and agricultural exports, which are organized chiefly by nationals from Nigeria and the Democratic Republic of the Congo. As respect for the rule of law continues to deteriorate in Cote d'Ivoire, due to the ongoing political and economic turmoil,

Ivoirians and some Liberian nationals are becoming more and more involved in the laundering of funds. Hizbollah is present in Cote d'Ivoire, and it conducts some fundraising activities, mostly among the large Lebanese expatriate community. Cote d'Ivoire is not an offshore financial center. It does permit the establishment of offshore financial institutions or offshore shell corporations. There are no free trade zones in Cote d'Ivoire. In August 2004, the Ivoirian government adopted a plan for the creation of a free trade zone for information technology and for biotechnology. This project is dormant. Another free trade zone project, which was planned for the port of San Pedro, also remains dormant.

The outbreak of the rebellion in 2002 increased the amount of smuggling of goods across the northern borders, especially of textiles and cigarette products. There have also been reports of an increase in the processing and smuggling of small quantities of diamonds from mines located in the North. Ivoirian law enforcement authorities have no control over the northern half of the country, and therefore they cannot judge what relationship, if any, the funding for smuggled goods might have to narcotics proceeds or other illicit proceeds. Smuggling of sugar, cotton, cocoa, cars, and pirated DVDs occurs in the government-controlled south and is motivated by a desire to avoid the payment of high export or import taxes. This cross-border trade in smuggled goods generates contraband funds that are introduced into the banking system through informal or unregulated moneychangers, fictitious company accounts, and fictitious business contracts.

Criminal enterprises use both the formal and informal financial sector to wash funds. Cash is moved both via the formal banking sector and by cash couriers. Informal money couriers and money transfer organizations similar to hawalas move funds both domestically and within the sub-region. Because of the division of the country, a lack of security, and the lack of a widespread banking system, transportation companies have also stepped in to provide courier services. The standard fee for these services is approximately ten percent. In addition to transferring funds, criminal enterprises launder illicit funds by investing in real estate and consumer goods such as used cars in an effort to conceal the source of funding. The Economic and Financial police have noticed an increase in financial crimes related to credit card theft and foreign bank account fraud, which includes wire transfers of large sums of money primarily involving British and American account holders who are the victims of Internet based advanced fee scams. The Ministry of Finance remains concerned by the high levels of tax fraud, particularly VAT tax fraud by merchants.

The country has seventeen banks and five non-bank financial institutions. Of that number, there are eight foreign-owned banks and two foreign-owned financial institutions in operation. The law requires a capitalization of the CFA equivalent of $2 million for banks and $600,000 for financial institutions. Banks provide traditional banking services such as lending, savings and checking accounts and money transfers, while financial institutions offer leasing, payroll and billing services, and project financing for small businesses. The Ivoirian banking law, enacted in 1990, prevents disclosure of client and ownership information, but it does allow the banks to provide information to judicial authorities, such as investigative magistrates. The law also permits the use of client and ownership information as evidence in legal proceedings or during criminal investigations. The Tax and Economic police can request information from the banks.

Until recently, the penal code criminalized only money laundering related to drug-trafficking, fraud, and arms trafficking. On November 29, 2005, the Ivoirian National Assembly recently adopted the West African Economic and Monetary Union's (WAEMU) model law on money-laundering, making money laundering per se a criminal offense. Money laundering is defined as the intention to conceal the criminal origins of illicit funds. The new law became effective on December 15, 2005.

The new law focuses on the prevention of money laundering and also expands the definition of money laundering to include the laundering of funds from all serious crimes. The law does not set a minimum threshold. It includes standard "know your customer" requirements for banks and other financial

institutions. It establishes procedures, which require these institutions to assist in the detection of money laundering through suspicious transaction reporting, and it creates an Ivoirian FIU. It also provides a legal basis for international cooperation. The new law includes both penal and civil penalties. The law permits the freezing and seizure of assets, which includes instruments and proceeds of crime, including business assets and bank accounts that are used as conduits for money laundering. Substitute assets cannot be seized if there is no relationship with the offense. Legitimate businesses can be seized if used to launder money or support terrorist or other illegal activities.

Under the new money-laundering law, Cote d'Ivoire is required to create and fund an FIU named the "Cellule Nationale de Traitement des Informations Financieres" (CENTIF). The CENTIF will report to the Finance Ministry. On a reciprocal basis, with the permission of the Ministry of Finance, the CENTIF may share information with the FIUs in member states of WAEMU or with those of non-WAEMU countries, so long as those institutions keep the information confidential.

The FIU will take the lead in tracking money laundering, but it will continue to work with previously established investigative units such as the "Centre de Recherche Financiere" (CRF) at the Department of Customs and the Agence Nationale de Strategie et d'Intelligence" (ANSI) at the presidency. The CRF and the ANSI will still continue their missions, which include fiscal and customs fraud and counterfeiting. The Ivoirian Economic and Financial police, the criminal police unit (Police Judiciaire), the Department of Territorial Surveillance (Ivoirian intelligence service), the CRF and ANSI all are responsible for investigating financial crimes, including money laundering and terrorist financing. However, in addition to a lack of resources for training, there is a perceived lack of political will to permit investigative independence.

The Ministry of Finance, the West African Central Bank (BCEAO), and the West African Banking Commission, headquartered in Cote d'Ivoire, supervise and examine Ivoirian compliance with anti-money laundering/counterterrorist financing laws and regulations. Under the new money laundering legislation, Ivoirian banks and financial institutions will be required to verify and record the identity of their customers before establishing new accounts or processing transactions. All Ivoirian financial institutions are now required to begin to maintain customer identification and transaction records for ten years. For example, all bank deposits over approximately CFA 5,000,000 (about $10,000) made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. Law enforcement authorities can access these records to investigate financial crimes upon the request of a public prosecutor. In 2005, there were no arrests or prosecutions for money laundering or terrorist financing.

The new legislation imposes a ten year retention requirement on financial institutions to retain records of all "significant transactions," which are transactions with a minimum value of CFA 50,000,000 (about $100,000) for known customers. For occasional customers, the floor value for "significant transactions" is CFA 5,000,000 (about $10,000).

The new money laundering controls will apply to non-bank financial institutions such as exchange houses, stock brokerage firms, insurance companies, casinos, cash couriers, national lotteries, non-government organizations, travel agencies, art dealers, gem dealers, accountants, attorneys, and real estate agents. The law also imposes certain customer identification and record maintenance requirements on casinos and exchange houses. The tax office (Ministry of Finance) supervises these entities. All Ivoirian financial institutions, businesses, and professionals and non-bank institutions under the scope of the new money-laundering law are required to report suspicious transactions. The Ivoirian banking code protects reporting individuals. Their identities are not divulged with respect to cooperation with law enforcement authorities.

Cote d'Ivoire monitors and limits the international transport of currency and monetary instruments under WAEMU administrative regulation R/09/98/CM/WAEMU. There is no separate domestic law or regulation. When traveling from Cote d'Ivoire to another WAEMU country, Ivoirians and

expatriate residents must declare the amount of currency being carried out of the country. When traveling from Cote d'Ivoire to a destination other than another WAEMU country, Ivoirians and expatriate residents are prohibited from carrying an amount of currency greater than the equivalent of 500,000 CFA francs (approximately $1,000) for tourists, and two million CFA francs (approximately $4,000) for business operators, without prior approval from the Department of External Finance of the Ministry of Economy and Finance. If additional amounts are approved, they must be in the form of travelers' checks.

Cote d'Ivoire's new money-laundering law encompasses the laundering of funds from all serious crimes, but terrorism and terrorist financing are not considered "serious crimes" for the purposes of this law. Cote d'Ivoire does not have a specific law that criminalizes terrorist financing, as required under UNSC resolution 1373. Until the passage of the new law, the GOCI relied on several WAEMU directives on terrorist financing, which provided a legal basis for administrative action by the Ivoirian government to implement the asset freeze provisions of UNSCR 1373.

The BCEAO and Ivoirian government report that they promptly circulate to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list and those on the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. A U.S. financial institution present in Cote d'Ivoire confirms the receipt of notices issued by government authorities. In 2005, no assets related to terrorist entities or individuals were discovered, frozen or seized.

The Ivoirian government admits the existence of informal remittance and cash transfer systems that bypass regular financial institutions and agrees that these could be a possible conduit of laundered funds. Currently, domestic informal cash transfer systems are not regulated. Informal remittance transfers from outside Cote d'Ivoire violate BCEAO money transfer regulations. The Ivoirian government has taken no legal action to prevent the misuse of charitable and or other non-profit entities that can be used as conduits for the financing of terrorism. The Ministry of Interior Security is addressing this problem.

Cote d'Ivoire participates in the ECOWAS-Intergovernmental Group for Action Against Money Laundering (GIABA) based in Dakar, which sits as an observer to the OECD's Financial Action Task Force (FATF). The Ivoirian government has neither adopted laws nor promulgated regulations that specifically allow for the exchange of records with United States on money laundering and terrorist financing. However, under the new money laundering law, after obtaining the approval of the Finance Ministry, the CENTIF could share information related to money laundering records with U.S. or other countries on a reciprocal basis and under an agreement of confidentiality between the two governments.

Cote d'Ivoire has demonstrated a willingness to cooperate with the USG in investigating financial or other crimes. For example, in one case from 2004, an American citizen was being defrauded by someone posing as a GOCI Customs Official requesting demurrage fees for a shipment of goods. With a short window of opportunity for action, the U.S. Embassy notified the Economic Police, who then instructed the Bank Examiner to monitor the suspect's account. The next morning, the Economic Police arrested a Nigerian who came in to retrieve the funds. Armed with a search warrant, the police searched the suspect's house, gathered evidence of a boiler-room operation, and arrested three other Nigerians. The funds ($15,000) were successfully wired back to the victim.

Cote d'Ivoire is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. Cote d'Ivoire has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Cote d'Ivoire should proceed to do so. It should implement its new anti-money laundering law, including the funding and establishing of an FIU. It should expand on the new law by criminalizing terrorist financing.