Country Reports

Afghanistan

Afghanistan is not a regional financial or banking center. However, its formal financial system is growing rapidly while its traditional informal financial system remains significant in reach and scale. Afghanistan is a major drug trafficking and drug producing country and the illicit narcotics trade is the primary source of laundered funds. 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. The most fundamental obstacles continue to be legal, cultural and historical factors that conflict with more Western-style proposed reforms to the financial sector.

According to United Nations statistics, in 2005 and 2006, opium production increased and today Afghanistan accounts for over 90 percent of the world's opium production. Opium gum itself is sometimes 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 at least 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.

Much of the recent rise in opium production comes from Taliban strongholds in the southern part of the country. There are reports that the Taliban impose taxes on narcotics dealers, which undoubtedly helps finance their terrorist activities. Additional revenue streams for the Taliban and regional warlords come from "protecting" opium shipments, running heroin labs, and from "toll booths" established on transport and smuggling routes.

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 traditional hawala system that uses trade as the primary medium to balance accounts. In addition, the narcotics themselves are often used as tradable goods and as a means of exchange for automobiles, construction materials, foodstuffs, vegetable oils, electronics, and other goods between Afghanistan and neighboring Pakistan. Many of these goods are smuggled into Afghanistan from neighboring countries, particularly Iran and Pakistan, or enter via the Afghan Transit Trade without payment of customs duties or tariffs. Most of the trade goods imported into Afghanistan originate in Dubai. Invoice fraud, corruption, indigenous smuggling networks, underground finance, and legitimate commerce are all intertwined.

Afghanistan is widely served by the hawala system, which provides a range of financial and nonfinancial business services in local, regional, and international markets. Financial activities include foreign exchange transactions, funds transfers (particularly to and from neighboring countries with weak regulatory regimes for informal remittance systems), 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 risks), it is a traditional form of finance and deeply entrenched and widely used throughout Afghanistan and the neighboring region.

There are over 200 known hawala dealers in Kabul, with 100-300 additional dealers in each province. These dealers are loosely organized into informal provincial unions or guilds whose members maintain a number of agent-principal and partnership relationships with other dealers throughout the

country and internationally. Their record keeping and accounting practices are robust, 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 licensed; however the licensing regime that existed from April 2004 until September of 2006 was overly burdensome and resulted in issuance of few licenses. In September of 2006, Da Afghanistan Bank (DAB)—Afghanistan's Central Bank—issued a new money service provider regulation that streamlined the licensing process and substantially reduced the licensing and ongoing compliance burden for hawaladars. The regulatory focus of the new regulation is on AML and CTF. The regulation requires and provides standard mechanisms for record keeping and reporting of large transactions. DAB has provided training sessions on the new regulation and has developed a streamlined application process. Several licenses have already been issued under the new regulation, with the majority of Kabul area hawaladars expected to obtain licenses in the near-term as a result of DAB outreach, law enforcement actions, pressure from commercial banks where they hold accounts, and customer demand for licensed providers. Options for strengthening the hawaladar unions and promoting self regulation are also being studied.

In early 2004, DAB worked in collaboration with international donors 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 Anti-Money Laundering (AML) and Proceeds of Crime and Combating the Financing of Terrorism (CTF) 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. 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 is functioning as a semi-autonomous unit within DAB. Banks and other financial and nonfinancial institutions 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. Currently, in excess of four thousand electronically formatted cash transaction reports are being received and processed each month. 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. At present the formal banking sector consists of three recently re-licensed state-owned banks, five branches of foreign banks, and six additional domestic banks. AML examinations have been conducted in half of these banks. The result is a growing awareness of AML requirements and deficiencies among the banks and a building of AML capacity. Additionally, the Central Bank has worked with the banking community to develop several ongoing topical working groups focused on AML issues (e.g. "know your customer" provisions and reporting of suspicious transactions).

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 is charged with administering the AML and CTF legislation, conducting examinations, licensing new institutions, overseeing money service providers, and liaising with the commercial banking sector generally. The effectiveness of the Supervision Department in the AML area remains limited due to staffing, organization, and management issues.

The Ministry of Interior and the Attorney General's Office are the primary financial enforcement authorities. However, 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 DAB. There is a need for significant training for judges and administrative staff before the Tribunal will be effective. The Tribunal will review supervisory actions of DAB, but will 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.

Border security continues to be a major issue throughout Afghanistan. At present there are 21 border crossings that have come under central government 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 improved, but smuggling and corruption continue to be major concerns, as well as trade fraud, which includes false and over-and-under invoicing. Thorough cargo inspections are not conducted at any gateway. A pilot program for declaring large, cross-border currency transactions has been developed for the Kabul International Airport, but has not yet been implemented. If successful, this prototype will serve as the foundation for expansion to other crossings.

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 nonprofit 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" nonprofit 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. In July 2006, Afghanistan became a member in the Asia Pacific Group, a Financial Action Task Force Style Regional Body (FSRB), and has obtained observer status in the Eurasian Group, another FSRB. Additionally the FIU has initiated the process for joining the Egmont Group of Financial Intelligence Units.

The Government of Afghanistan has made progress over the past year in developing its overall AML/CTF regime. Improvement has been seen in development of the FIU, the reporting of financial intelligence, participation in international AML bodies, improvement in bank AML compliance awareness, systems, and reporting, and in efforts to bring money service providers into a legal and regulatory framework that will result in meaningful AML compliance. However, much work remains to be done. Afghanistan should develop secure, reliable, and capable relationships among departments and agencies involved in law enforcement. Afghanistan should develop the investigative capabilities of law enforcement authorities in the areas of financial crimes, particularly money laundering and terrorist finance. Judicial authorities should also be trained in money laundering prosecutions. Afghan customs authorities should implement cross-border currency reporting and be trained to recognize forms of trade-based money laundering. Border enforcement should be a priority, both to enhance

scarce revenue and to disrupt narcotics trafficking and illicit value transfer. Afghan authorities should work to address widespread corruption in commerce and government. Afghanistan should ratify the UN Convention against Corruption.

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, often 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 remains primarily cash-based. Electronic and ATM transactions are relatively few in number, but are growing rapidly as more banks introduce this technology. The number of ATMs rapidly expanded following the decision of the Government of Albania (GOA) to deliver salaries through electronic transfers. By the end of 2005, all central government institutions had converted to electronic pay systems. Credit card usage has also increased in Albania. However, thus far a small number of people possess them and usage is primarily limited to a few large vendors.

There are 17 banks in Albania, but only five of them are considered to have a significant national presence. 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. Albania is not considered an offshore financial center, nor do its current laws facilitate such types of activity. Although current law permits the operation of free trade zones, the GOA has not pursued the implementation of them and none are currently in operation.

The Albanian economy is particularly vulnerable to money laundering activity because it is a cash-based economy. The GOA estimates that proceeds from the informal sector account for approximately 30-60 percent of Albania's 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, encompassing 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 Albania 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 (FIUs).

Albania criminalized money laundering in Article 287 of the Albanian Criminal Code of 1995, consolidated version as of December 1, 2004. However, the law was largely ineffectual as it required proof of a predicate offense.

Albania's original money laundering law was On the Prevention of Money Laundering, or Law No. 8610 of 17 May 2000. 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 international conventions. Under the revised Criminal Code many powers

were expanded and improved upon. The new law also revised the definition of money laundering, outlawed the establishment of anonymous accounts, and permitted the confiscation of accounts. Albania's money laundering law places reporting requirements on both financial institutions and individuals. Financial institutions are required to report to an anti-money laundering agency all transactions that exceed approximately $200,000 as well as those that involve suspicious activity. Private individuals (both Albanian and foreign) are required to report to customs authorities all cross-border transactions that exceed approximately $10,000. Declaration forms are available at border crossing points. The law also mandates the identification of beneficial owners. Banks and other institutions are required to maintain records of suspicious transaction reports (STRs) for ten years. All other reports are subject to a five-year record retention period. There have been cases of individuals sentenced for illegal transfer of money based on information from foreign FIUs, and the Albanian FIU occasionally shares cash smuggling reports with its counterparts in Turkey, Bulgaria, and Macedonia.

Financial institutions are required to report transactions within 48 hours if the origin of the money cannot be determined. In addition, there are requirements to report all financial transactions that exceed certain thresholds. However, financial institutions have no legal obligation to identify customers prior to opening an account. While most banks have internal rules mandating customer identification, Albania's money laundering law only requires customer identification prior to conducting transactions that exceed approximately $20,000 or when there is a suspicion of money laundering.

Albania's 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 applies a difficult burden of proof in that it requires a prior or simultaneous conviction for the predicate crime before an indictment for money laundering can be issued. According to the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) mutual evaluation report (MER), whose team conducted the evaluation in September 2005, and which accepted the MER in July 2006, Albanian authorities estimated that Albania had two cases of money laundering and five convictions, with another five cases at the prosecutor's office. There is no information available regarding cases, prosecutions or convictions of money laundering offenses for 2006.Albanian law also has no specific laws pertaining to corporate criminal liability, however it may be possible (though unlikely) for legal entities to be prosecuted for money laundering under Article 45 of the Criminal Code.

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 nonbank financial institutions, enforcement has been poor in practice. There is an increasing number of STRs coming from banks as the banking sector becomes more mature, although the majority continues to come from tax and customs authorities 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.

Albania's money laundering law also mandates the establishment of an agency to coordinate the GOA's efforts to detect and prevent money laundering. Albania's FIU, the General Directorate for the Prevention of Money Laundering (DPPP), 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 2006, there were a total of 15 suspicious activity reports that the FIU acted upon, out of a total of 46,630 reports received.

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 coordination on the both the policy and the technical level. On the policy level, an inter-ministerial group was established. The group is headed by Albania's Prime Minister and includes the participation of the Central Bank Governor and the General Prosecutor. On the technical level, a group of experts was established. The Albanian government is reportedly in the process of preparing a new draft law on money laundering.

In addition to the FIU, 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.

Albanian law also allows freezing or blocking of financial transactions believed to involve money laundering. In 2004, 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, 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.

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, criminalizing the financing of terrorism and mandating strong penalties for any actions or organizations linked with terrorism. The law permits the GOA to administratively sequester or freeze 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 the one freeze action conducted in 2004, the GOA has frozen the assets of seven additional individuals or entities in 2005, and supports USG and UN designation efforts.

The Ministry of Finance is the main entity responsible for issuing freeze orders. The order is executed by the Minister of Finance and then delivered by the FIU to other government agencies that take action to freeze any assets found belonging to the named individual or entity. In the case of individuals or entities whose names appear on the UNSCR 1267 consolidated list, the sequestration 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, their assets may 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 ordered confiscated and any proceeds are 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. The purpose of the agency is to safeguard sequestered assets and to dispose of assets ordered confiscated. After a difficult start, the GOA first staffed the AASCA in early December 2005. However, the agency receives little support from the Ministry of Finance and has also experienced a large turnover in staffing.

Between 2001 and 2005, the GOA 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). In 2005, the previous freezing orders were converted under the new law against terrorism financiers. As of 2005, 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. As of 2006, charitable organizations are required 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.

Albania is a member of MONEYVAL and participates in the Southeastern Europe Cooperative Initiative (SECI). The Albanian FIU is a member of the Egmont Group, 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 29 countries. Most recently, in February 2006, the Albanian FIU signed an MOU with its Kosovo counterpart that will allow the two FIUs to share information relating to money laundering. The FIU also participates in regional anti-money laundering seminars and conferences.

Albania 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. In May 2006, Albania ratified the UN Convention against Corruption.

The Government of Albania has enhanced its anti-money laundering/counterterrorist financing regime; however, additional improvements are greatly needed. Albania should amend Article 287 of the Criminal Code to allow authorities to prosecute money laundering without first obtaining a conviction for a predicate offense. The FIU should create or obtain a database to allow analysis of the large volume of currency transaction reports (CTRs) and suspicious transaction reports received so that these reports currently received in hard copy can be analyzed. Training for the FIU should also be a high priority, as its staff is largely new and inexperienced. Training and modernization for the other facets of financial crime investigation should also be in order. The Albanian police force still has no central database and its investigators lack training in modern financial investigation techniques. The Prosecutor's Office also lacks well-trained prosecutors to effectively manage and try cases. Albania should also 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.

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, nonbank financial professions such as lawyers, accountants, stockbrokers, insurance agents, pension managers, and dealers of precious metals and antiquities. Provided information is shared with 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 noncompliance range from 50,000 to 5 million Algerian dinars (approximately U.S. $700 to U.S. $70,000). In addition to its provisions pertaining to money laundered from illicit activities, the law allows the investigation of terrorist-associated funds derived from "clean" sources.

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 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 deadline of September 1, 2006 after which all payments in excess of $70,000 must be made by check, wire transfer, payment card, bill of exchange, promissory note, or other official bank payment. While nonresidents are exempt from this requirement, they must (like all travelers to and from the country) report foreign currency in their possession to the Algerian Customs Authority. The government suspended the deadline in September 2006, however, in response to the slow implementation of a nation-wide electronic check-clearing system that failed to gain the confidence of the Algerian business community.

The Ministry of Interior is charged with registering foreign and domestic nongovernmental organizations in Algeria. 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.

There are reports that Algerian customs and law enforcement authorities are increasingly concerned with cases of customs fraud and trade-based money laundering. Algerian authorities are taking steps to coordinate information sharing between concerned agencies.

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. The Ministry of Justice is expected to create a pool of judges trained in financial matters.

Over the last three years, Algeria has taken significant steps to enhance its statutory regime against anti-money laundering and terrorist financing. It needs to move forward now to implement those laws and eliminate bureaucratic barriers among various government agencies by empowering CTRF, which in 2006 investigated only 15 suspicious transactions, to be the focal point for the AML/CTF investigations. In addition, given the scope of Algeria's informal economy, it should renew its initiative to limit the size of cash transactions. Algerian law enforcement and customs authorities should be trained in recognizing and investigating trade-based money laundering, value transfer, and bulk cash smuggling used for financing terrorism and other illicit financial activities.

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. The Government of the Republic of Angola (GRA) 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 method of "mixing parcels" of licit and illicit diamonds, the Kimberly certification process can be compromised. Corruption and 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. Additional laws remain in draft form only. 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 counter narcotics laws criminalize money laundering related to narcotics trafficking. One of three draft laws designed to reform the banking sector specifically targets money laundering. The money laundering bill, which is currently under consideration in the Angolan Congress, was drafted with the assistance of the World Bank.

The high cash flow in Angola makes its financial system an 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 currency per month, largely in dollars, without a corresponding cash outflow. Local bank representatives have reported that clients have walked into banks with up to $2 million in a briefcase to make a deposit. There are no currency transaction reports that cover these large cash transactions. 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 or search for patterns.

Corruption is a pervasive problem in Angolan society and is found in commerce and at the highest levels of government. Angola is rated 142 out of 163 countries in Transparency International's 2006 International Corruption Perception Index.

Angola is party to the 1988 UN Drug Convention and the UN Convention against Corruption. 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 legislation that adheres to world standards, the GRA should establish a system of financial transparency reporting requirements and a corresponding Financial Intelligence Unit. The GRA should then move quickly to implement the legislation and bolster the capacity of law enforcement to investigate financial crimes. Angola's judiciary should prioritize the prosecution of financial crimes, including corruption. The GRA 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 GRA should increase efforts to combat official corruption, including an effective system to identify, trace, seize, and forfeit assets.

Antigua and Barbuda

As with other countries in the region, illicit proceeds from the transshipment of narcotics are laundered in Antigua and Barbuda. However, its offshore financial sector as well as its internet gaming industry remain primary vulnerabilities in Antigua and Barbuda. In 2006, Antigua and Barbuda reported 16 offshore banks, two offshore trusts, two offshore insurance companies, 6,303 international business corporations (IBCs), and 30 internet gaming companies. Antigua and Barbuda has five domestic casinos that also are vulnerable to money laundering.

The International Business Corporations Act 1982 (IBCA), as amended, is the governing legal framework for offshore businesses in Antigua and Barbuda. The IBCA requires offshore banks to maintain full details of all transactions in relation to deposits and withdrawals, and to retain the information obtained for a period of six years. No offshore bank may serve as the originator or recipient in the transfer of funds on behalf of an entity who is not an account holder. Bearer shares are permitted through a registered agent. However, the registered agent must maintain a register that includes such information as the names of the beneficial owners and the number of shares issued. Failure to do so could result in a fine of $50,000. Any entity licensed under the IBCA must maintain a physical presence with at least one full-time employee, and maintain all files and records for the company. Internet gaming companies must incorporate as an IBC, while land-based casinos must incorporate as a domestic company. As such, internet gaming companies must also meet the physical presence requirement, and are considered to have physical presence when the primary server is located in Antigua and Barbuda. Deemed a financial institution under the IBCA, internet gaming companies are also required to enforce know-your-customer verification procedures and maintain records relating to all gaming and financial transactions of each customer for six years. In addition, internet gaming companies must submit quarterly financial statements in addition to annual statements.

The Eastern Caribbean Central Bank (ECCB) supervises Antigua and Barbuda's domestic banking sector. In 2002, the IBCA was amended to create the Financial Services Regulatory Commission (FSRC) as the regulatory and supervisory authority that oversees offshore financial sectors, including internet gaming companies. The FSRC is an autonomous body supervised by a four-member Board comprised of public officials, and is presently chaired by the Solicitor General. The FSRC is also responsible for issuing IBC licenses and maintaining the register for all corporations. The FSRC is funded through the revenue generated by registration and licensing fees. Amendments to the IBCA in 2005 provide the FSRC with the ability to decline or revoke a license if it has reason to suspect that the corporation may be used for criminal purposes. To ensure compliance with legislation and regulations, the FSRC conducts annual on-site examinations and off-site examinations of offshore financial institutions as well as certain domestic nonbanking financial institutions, such as insurance companies, trusts, and money remitters.

The Government of Antigua and Barbuda (GOAB) reportedly receives approximately $2.8 million per year from license fees and other charges related to the internet gaming industry. A nominal free trade zone in the country also seeks to attract investment in priority areas of the GOAB. Casinos and sports book-wagering operations in Antigua and Barbuda's Free Trade Zone are supervised by the Office of National Drug Control Policy (ONDCP) and the Directorate of Offshore Gaming (DOG), a department within the FSRC. In 2001, the DOG issued Interactive Gaming and Interactive Wagering Regulations in order to establish regulations for the licensing of the industry and address possible money laundering through client accounts of internet gambling operations.

The Money Laundering Prevention Act (MLPA) 1996, as amended, is the cornerstone of Antigua and Barbuda's anti-money laundering legislation. The MLPA makes it an offense for any person to obtain, conceal, retain, manage, or invest illicit proceeds or bring such proceeds into Antigua and Barbuda if that person knows or has reason to suspect that they are derived directly or indirectly from unlawful activity. The MLPA covers institutions defined under the Banking Act, IBCA, and the Financial Institutions (Non-Banking) Act, which include offshore banks, IBCs, money service businesses, credit unions, building societies, trust businesses, casinos, internet gaming companies, and sports betting companies. Intermediaries such as lawyers and accountants are not included in the MLPA. The MLPA requires reporting entities to report suspicious activity suspected to be related to money laundering, whether a transaction was completed or not. There is no reporting threshold imposed on banks and financial institutions except for internet gaming companies, which are required to report to all payouts over $25,000. The MLPA also requires banks to monitor transactions involving individuals, businesses, and other financial institutions from countries that have not adopted a comprehensive anti-money laundering regime.

The Office of National Drug Control and Money Laundering Policy (ONDCP) Act 2003 establishes the ONDCP as the financial intelligence unit (FIU) of Antigua and Barbuda. An independent organization, the ONDCP is under the Ministry of National Security and is primarily responsible for the enforcement of the MLPA and for directing the GOAB's anti-money laundering efforts in coordination with the FSRC. The ONDCP assumes the role and fulfills the responsibilities of the Supervisory Authority as described in the MLPA, which includes the supervision of all financial institutions in respect to filing suspicious activity reports (SARs). As of October 2006, the ONDCP received 52 SARs of which 20 were investigated. In addition to receiving SARs, auditors of financial institutions review their compliance program and submit reports to the ONDCP for analysis and recommendations. The director of the ONDCP has the ability to appoint law enforcement officers to investigate narcotics trafficking, fraud, money laundering, and terrorist financing offenses. In 2005, two arrests were made on money laundering charges, but no arrests, prosecutions or convictions were reported in 2006.

In 2002, the ONDCP published guidelines which detail reporting entities' responsibilities including internal controls, customer identification, record keeping, reporting SARs, and anti-money laundering training for staff. The ONDCP has developed an anti-money laundering awareness training program and has trained a number of financial institutions, GOAB officials, and law enforcement officials with respect to their duties and responsibilities under the law.

The ONDCP has the ability to direct a financial institution to freeze property up to seven days, while it makes an application for a freeze order. A freeze order is made based upon a defendant being charged or about to be charged with a money laundering offense, or if the defendant is suspected of engaging in money laundering activity. Under the MLPA, a freeze order will lapse after 30 days unless charges are brought against the defendant, or an application for a civil forfeiture order has been filed. The Misuse of Drugs Act empowers the court to forfeit assets related to drug offenses. Forfeited assets are placed into the Forfeiture Fund and can be used by the ONDCP. The GOAB is currently working on asset forfeiture agreements with other jurisdictions. An MOU was recently signed with Canada.

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. On its own initiative, the GOAB froze over $90 million 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 million.

The ONDCP, with Cabinet approval, may enter into written agreements with other government agencies and foreign counterparts. Currently, the ONDCP has memoranda of understanding (MOUs) with the Royal Antigua and Barbuda Police Force, Customs, Immigration, and the Antigua and Barbuda Defense Force. The ONDCP also has an MOU with the FSRC, and expects to sign an MOU with the ECCB in 2007.

All travelers are required to fill out a Customs declaration form indicating if they are carrying in excess of $10,000 in cash or currency. The GOAB Customs Department maintains statistics on cross-border cash reports and seizures for failure to report. This information is shared with the ONDCP and the Police.

The GOAB enacted the Prevention of Terrorism Act 2001, amended in 2005, to implement the Counter Terrorism Conventions of the United Nations. The Act 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 Act also provides the authority for the seizure of property used in the commission of a terrorist act; seizure and restraint of property that has been, is being or may be used to commit a terrorism offence; forfeiture of property on conviction of a terrorism offence; and forfeiture of property owned or controlled by terrorists. The Act requires financial institutions to report every three months whether they are in possession of any property owned or controlled by or on behalf of a terrorist group. In addition, financial institutions must report every transaction that is suspected to be related to the financing of terrorism to the ONDCP.

The Attorney General may revoke or deny the registration of a charity or nonprofit 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 has not undertaken any specific initiatives focused on the misuse of charities and nonprofit entities

The GOAB continues its bilateral and multilateral cooperation in various criminal and civil investigations and prosecutions. The amended Banking Act of 2004 enables the ECCB to share information directly with foreign regulators through an MOU. In 1999, a Mutual Legal Assistance Treaty (MLAT) 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. Because of such assistance, the GOAB has benefited through an asset sharing agreement and has received asset sharing revenues from the United States.

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). The ONDCP joined the Egmont Group in June 2003. 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. On June 21, 2006 Antigua and Barbuda acceded to the UN Convention against Corruption.

The GOAB should implement and vigorously enforce all provisions of its anti-money laundering legislation including the strict and effective supervision of its offshore sector and gaming industry.

Despite the comprehensive nature of the law, Antigua and Barbuda has yet to prosecute a money laundering case. Moreover, there is an over-reliance on SARs to initiate investigations. Law enforcement and customs authorities should be trained to recognize money laundering typologies that fall outside the formal financial sector. The GOAB should vigorously enforce its anti-money laundering laws by actively prosecuting money laundering and other financial crimes.

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 gradual 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 nonbank 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 the majority of 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 combat money laundering in 2006, including enacting amendments to its money laundering legislation with the passage of Law 26.087 in March, granting greater authority to Argentina's financial intelligence unit (the Unidad de Información Financiera, or UIF), creating a new National Coordination Unit in the Ministry of Justice and Human Rights to oversee and manage overall GOA anti-money laundering efforts, and creating a Special Prosecutors Unit within the Attorney General's Office for money laundering and terrorism finance cases. In addition, the Central Bank of Argentina (BCRA) completed plans for a specialized bank examination unit, announced in 2005, devoted specifically to money laundering and terrorism finance. On December 20, 2006, President Kirchner approved Argentina's long-awaited draft antiterrorism and counterterrorism financing law, which he sent to Congress for approval on the same day

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 the UIF under the Ministry of Justice and Human Rights. The law requires 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 for Insurance (Superintendencia de Seguros de la Nación, or SSN). The law forbids institutions to notify their clients when filing suspicious transaction reports (STRs), 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 Attorney General's Office. As of October 31, 2006, the UIF had received 2174 reports of suspicious or unusual activities since its inception in 2002, forwarded 136 suspected cases of money laundering to prosecutors for review, and assisted prosecutors with 107 cases. 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.

On March 29, 2006, the Argentine Congress passed Law 26.087, amending and modifying Law 25.246, in order to address Financial Action Task Force (FATF) concerns regarding the inadequacies in Argentine money laundering and terrorism financing legislation and enforcement. The FATF conducted a mutual evaluation of Argentina in October 2003, which 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 weaknesses in Argentina's anti-money laundering legislation, as well as the lack of terrorist financing legislation or a national anti-money laundering and counterterrorist financing coordination strategy.

Law 26.087 responds to many of the deficiencies noted by the FATF. It makes substantive improvements to existing law, including lifting bank, stock exchange and professional secrecy restrictions on filing suspicious activity reports; partially lifting tax secrecy provisions; clarifying which courts can hear requests to lift tax secrecy requests, and requiring decisions within 30 days. Law 26.087 also lowers the standard of proof required before the UIF can pass cases to prosecutors, and eliminates the so-called "friends and family" exemption contained in Article 277 of the Argentine Criminal Code for cases of money laundering, while narrowing the exemption in cases of concealment. Overall, the law clarifies the relationship, jurisdiction, and responsibilities of the UIF and the Attorney General's Office, and improves information sharing and coordination. The law also reduces restrictions that have prevented the UIF from obtaining information needed for money laundering investigations by granting greater access to STRs filed by banks. However, the law does not lift financial secrecy provisions on records of large cash transactions, which are maintained by banks when customers conduct a cash transaction exceeding 10,000 pesos (approximately $3,225). Also in response to FATF concerns, as noted in the mutual evaluation report, the Argentine government established a new National Coordination Unit in the Ministry of Justice and Human Rights. The National Coordination Unit represents Argentina at the FATF and GAFISUD, has the lead in developing money laundering and terrorism financing legislation, and manages the government's overall anti-money laundering and counterterrorist financing efforts.

The UIF, which began operating in June 2002, has issued resolutions widening the range of institutions and businesses required to report on suspicious or unusual transactions to the UIF beyond those identified in Law 25.246. Obligated entities include the tax authority (Administración Federal de Ingresos Publicos, or AFIP), Customs, banks, currency exchange houses, casinos, securities dealers, insurance companies, postal money transmitters, accountants, notaries public, and dealers in art, antiques and precious metals. The resolutions issued by the UIF also provide guidelines for identifying suspicious or unusual transactions. All suspicious or unusual transactions, regardless of the amount, must be reported directly to the UIF. Prior to the passage of Resolution 4/2005 in 2005, only suspicious or unusual transactions that exceeded 50,000 pesos (approximately $16,130) had to be reported; prior to 2004, suspicious transactions that were below a 500,000 peso threshold were first reported to the appropriate supervisory body for pre-analysis. Obligated entities are required to maintain a database of 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.

In September 2006, Congress passed Law 26.119, which amends Law 25.246 to modify the composition of the UIF. The new law reorganizes the UIF's executive structure, changing it from a five-member directorship with rotating presidency to a structure that has a permanent, politically-appointed president and vice-president. Law 26.119 also establishes a UIF Board of Advisors, comprised of representatives of key government entities, including the Central Bank, AFIP, the Securities Exchange Commission, the national counternarcotics secretariat (SEDRONAR), and the Justice, Economy, and Interior Ministries. The Board of Advisors' opinions on UIF decisions and actions are nonbinding.

The Central Bank requires by resolution that all banks maintain a database of all transactions exceeding 10,000 pesos, and periodically submit the data to the Central Bank. 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. The UIF further receives copies of the declarations to be made by all individuals (foreigners or Argentine citizens) entering or departing Argentina with over US$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. In 2003, the Argentine Congress passed Law 22.415/25.821, which 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. However, the President vetoed the law because it allegedly conflicted 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.

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.

Terrorism and terrorist acts are not yet criminalized under Argentine law. Because these acts are not autonomous offenses, terrorist financing is not a predicate offense for money laundering. During 2005 and 2006, several bills were introduced in the Congress to implement the provisions of international treaties on terrorist financing under Argentine law. Various ministries in the government, as well as the "Comisión Mixta" (Mixed Commission—comprised of the Central Bank, Congress, Ministry of Economy, SEDRONAR, and Judicial branch), also developed draft counterterrorism finance laws. Argentina's new National Coordinator reviewed and harmonized the draft laws, and completed a final draft for the President to submit to Congress. The President approved the draft and sent it to Congress on December 20, 2006. Congress will consider it in March 2007, or in February if the President calls an extraordinary session. The draft law criminalizes both acts of terrorism and the financing of terrorism, and if approved, would provide the legal foundation for the UIF, Central Bank, and other law enforcement bodies to investigate and prosecute such crimes. FATF members will review either the draft or the newly enacted law during the February 2007 FATF Plenary to determine whether it meets international standards.

In the absence of terrorist financing legislation, the Central Bank issued Circular A 4273 in 2005 (titled "Norms on 'Prevention of Terrorist Financing'"), requiring banks to report any detected instances of the financing of terrorism. The Central Bank has regularly updated and modified the original Circular, with the most recent modification being Circular A 4599 of November 17, 2006. Bankers complain 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 draft counterterrorism law currently before Congress would provide the necessary legal backing for the Central Bank's administrative measures. The Central Bank of Argentina also 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.

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

Working with the U.S. Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Argentina has established a Trade Transparency Unit (TTU). The TTU examines anomalies in trade data that could be indicative of customs fraud and international trade-based money laundering. The TTU will generate, initiate, and support investigations and prosecutions related to trade-based money laundering and the movement of criminal proceeds across international borders. One key focus of the TTU, as well as of other TTUs in the region, will be financial crimes occurring in the Triborder Area, which is bound by Puerto Iguazu, Argentina, Foz do Iguacu, Brazil, and Ciudad del Este, Paraguay. The creation of the TTU was 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, 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 against Terrorism, and the UN Convention against Transnational Organized Crime. Argentina ratified the UN Convention against Corruption on August 28, 2006. Argentina participates in the "3 Plus 1" Security Group (formerly the Counter-Terrorism Dialogue) between the United States and the Triborder Area countries. The UIF has been a member of the Egmont Group since July 2003, and has signed memoranda of understanding regarding the exchange of information with a number of other financial intelligence units. 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 Laws 26.119, 26.087 and 25.246, the ratification of the UN International Convention for the Suppression of the Financing of Terrorism, a reorganized UIF, and enhanced enforcement capability via the Special Prosecutors Unit and Central Bank's specialized bank examination unit, Argentina has the legal and regulatory capability to prevent and combat money laundering more effectively. Additional legislative and regulatory changes would significantly improve the anti-money laundering and counterterrorist financing regime in Argentina, particularly the passage of the domestic legislation criminalizing the financing of terrorism that is currently before Congress. The GOA should enact legislation to expand the UIF's role to enable it to investigate money laundering arising from all crimes, rather than just six enumerated crimes; establish money laundering as an independent offense; and eliminate the currently monetary threshold of 50,000 pesos required to establish a money laundering offense. To comply with the latest FATF recommendation on the regulation of bulk money transactions, Argentina will also need to review the legislation vetoed in 2003 to find a way to regulate such transactions consistent with its MERCOSUR obligations. Continuing priorities are the effective 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. There is also a need for increased public awareness of the problem of money laundering and its connection to

narcotics, corruption and terrorism. Finally, the new National Coordinator's Office should alleviate the past problems of inadequate coordination and cooperation between government agencies.

Aruba

Aruba is an autonomous and largely self-governing Caribbean island under the sovereignty of the Kingdom of the Netherlands; foreign, defense and some judicial functions are handled at the Kingdom level. 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, eleven credit institutions and eleven casinos. The island also has six registered money transmitters, two exempted U.S. money transmitters (Money Gram and Western Union), eight life insurance companies, fourteen general insurance companies, two captive insurance companies, and eleven company pension funds. As of October 27, 2006, there were 5,343 limited liability companies (NVs), of which 372 were offshore limited liability companies or offshore NVs, which may operate until 2007-2008. In addition, there are approximately 2,763 Aruba Exempt Companies (AECs), which mainly serve as vehicles for tax minimization, corporate revenue routing, and asset protection and management.

The offshore NVs and the AECs are the primary methods used for international tax planning in Aruba. The offshore NVs pay a small percentage tax and are subject to more regulation than the AECs. The AECs pay an annual $280 registration fee and must have a minimum of $6,000 in authorized capital. Both offshore NVs and AECs can issue bearer shares. A local managing director is required for offshore NVs. The 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 fiscal legislation in line with OECD standards. In 2003, the GOA introduced a New Fiscal Regime (NFR) containing a dividend tax and imputation credits. As of July 1, 2003, the incorporation of low tax offshore NVs was halted. The NFR contains a specific exemption for the AEC. Nevertheless, as a result of commitments to the OECD, the regime was brought in line with OECD standards as of January 2006. As a result of the NFR, Aruba's offshore regime will cease operations by the end of 2008.

Aruba currently has three designated free zones: Oranjestad Free Zone, Bushiri Free Zone and the Barcadera Free Zone, which 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, including servicing, repairing and maintenance of goods with a foreign destination, could be licensed to operate within the free zones. However, State Ordinance Free Zones 2000 extended licensing to service-oriented companies (excluding financial services). Before being admitted to operate in the free zone, companies must submit a business plan along with personal data of managing directors, shareholders and ultimate beneficiaries, and must establish a limited liability company founded under Aruban law intended exclusively 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.

Aruba was co-chair for the CFATF Typology on International Trade, which took place in Guatemala City in October 2006. Aruba presented the integrity system developed by Free Zone Aruba NV for the free trade zones, and requested feedback from the participating countries and international organizations. Resulting from Aruba's proposed typology is research on free trade zones in the region

in order to identify vulnerabilities, which should lead to an update of the CFATF Guidelines and provide important information for the Financial Action Task Force (FATF) work that is being done to counter trade-based money laundering.

The Central Bank of Aruba is the supervisory and 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. The State Ordinance on the Supervision of Money-Transfer Companies, effective August 12, 2003, 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 currently being drafted.

The anti-money laundering legislation in Aruba extends to all crimes that have a potential penalty of more than four years' imprisonment, including tax offenses. Aruba's criminal code allows for conviction-based forfeiture of assets. All financial and nonfinancial institutions are obligated to identify clients that conduct transactions over 20,000 Aruban guilders (approximately $11,300), and report suspicious transactions to Aruba's financial intelligence unit, the Meldpunt Ongebruikelijke Transacties (MOT). Obligated entities are protected from liability for reporting suspicious transactions. On July 1, 2001, reporting and identification requirements were extended by law to casinos and insurance companies.

The MOT is authorized to inspect all banks, money remitters, casinos, insurance companies and brokers for compliance with reporting requirements for suspicious transactions and the identification requirements for all financial transactions. The MOT is currently staffed by 12 employees. By September 2006, the MOT received 5,017 suspicious transaction reports, resulting in 86 investigations conducted and 22 cases transferred to the appropriate authorities. In June 2000, Aruba enacted a State Ordinance making it a legal requirement to report the cross-border transportation of currency in excess of 20,000 Aruban guilders to the customs department. The law also applies to express courier mail services. Reports generated are forwarded to the MOT to review, and in 2005, approximately 872 such reports were submitted. No data was provided for 2006.

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), 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 MOUs.

Aruba signed a multilateral directive with Colombia, Panama, the United States and Venezuela to establish an international working group to fight money laundering occurring 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.

In 2004, the Penal Code of Aruba was modified to criminalize terrorism, the financing of terrorism, and related criminal acts. The Kingdom of the Netherlands is party to the UN International Convention for the Suppression of the Financing of Terrorism; however, its ratification extends only to the Kingdom in Europe.

Aruba participates in the FATF and the FATF mutual evaluation program through representation in the Kingdom of the Netherlands. The GOA has a local FATF committee comprised of officials from

different departments of the Aruban Government, under the leadership of the MOT, to oversee the implementation of 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. Currently, Aruba is in compliance with seven of the nine FATF Special Recommendations. Aruba plans to 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.

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 GOA is a member of CFATF. The MOT became a member of the Egmont Group in 1997.

The Government of Aruba has shown a commitment to combating money laundering by establishing an anti-money laundering regime 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. Aruba should introduce the Sanctions Ordinance to become fully compliant with the FATF Special Recommendations on Terrorist Financing.

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 AUD1.2 trillion (approximately $905 billon), making it the eighth largest market in the world, and the third largest in the Asia-Pacific region behind Japan and Hong Kong. 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 last four 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, now underway, which is expected to significantly reshape Australia's current AML/CTF regime in line with current international best practices.

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 from commercial exploitation 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.

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 nonbanking 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 equal to or in excess of AUD10,000 (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 AUD10,000 (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 nonbank 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. AUSTRAC also provides advice and assistance to revenue collection, social justice, national security, and law enforcement agencies, and issues guidelines to cash dealers regarding their obligations under the FTR Act and regulations. As such, AUSTRAC plays a central role in Australia's AML system both domestically and internationally. During the 2005-06 Australian financial year, AUSTRAC's FTR information was used in 1,582 operational matters. Of these, in 431 matters FTR information was identified as being very valuable to outcomes. Results from the Australian Taxation Office shows that the FTR information contributed to more than AUD90.7 million (approximately $68 million) in Australian Taxation Office assessments during the year. In 2005-06, AUSTRAC received 13,880,944 financial transaction reports, with 99.6 percent of the reports submitted electronically through the EDDS Web system. AUSTRAC received 24,801 suspect transaction reports (SUSTRs), an increase of 44.1 percent from the precious year.

In 2006, there was a significant increase in the total number of financial transaction reports received by AUSTRAC. Significant cash transactions reports (SCTRs) account for 17 percent of the total number of FTRs reported to AUSTRAC in the 2005-06 Australian financial year and are reported by cash dealers and solicitors. In 2005-06, AUSTRAC received 2,416,427 SCTRs, an increase of 5.6 percent from the previous year. Cash dealers are required to report all international funds transfer instructions (IFTIs) to AUSTRAC. Cash dealers reported 11,411,961 IFTIs to AUSTRAC-a 11.4 percent increase from 2005. International currency transfer reports (ICTR) are primarily declared to the Australian Customs Service by individuals when they enter or depart from Australia. AUSTRAC received 27,755 ICTRs—a 6.0 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

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 noncompliance. 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 noncompliance.

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), which took effect on December 14, 2006, amends 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 inserts 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 2006.

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. In 2006, AFP introduced mandatory consideration of potential money laundering and crime proceeds into its case management processes, thereby ensuring that case officers explore the possibility of money laundering and crime proceeds actions in all investigations conducted by the AFP.

A draft AML/CTF bill developed by the AGD and a package of draft AML/CTF Rules, developed by AUSTRAC, were released for public comment in December 2005 and received Royal Assent on December 12, 2006. The AML/CTF Act covers the financial sector, gambling, bullion dealing and any other professionals or businesses that provide particular designated services and imposes a number of obligations including customer due diligence, reporting requirements, record keeping, and establishing AML/CTF programs. The Act will implement a risk-based approach to regulation. Implementation will occur over a two-year period and include consultation with reporting entities. Under the Act, AUSTRAC will now have an expanded role as the national AML/CTF regulator with supervisory, monitoring and enforcement functions over a diverse range of business sectors.

The package of draft legislation and rules formed the basis for 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 represented a first tranche of reforms. The final component of the first tranche commences in December 2008.

Once the first tranche of AML/CTF reforms are implemented. the Australian Government will consider a second tranche of reforms (to begin in 2007), extending to real estate agents, jewelers, and specified nonfinancial legal and accounting services. Lawyers and accountants are also included in the first tranche, but only where they compete with the financial sector and not for general services, which will be included in the second tranche. The proposed legislative framework authorizes operational details 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 FATF, 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 (FIUs). AUSTRAC has signed exchange Instruments, mostly in the form of Memoranda of understanding (MOUs) allowing the exchange of financial intelligence with FinCEN and the FIUs of 45 other countries.

Following the bombings in Bali in October 2002, the Australian Government announced an AUD10 million (approximately $7.5 million) initiative managed by the Australian Agency for International Development (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 Jakarta Centre for Law Enforcement Cooperation. As part of Australia's broader regional assistance initiatives, AUSTRAC continued its South East Asia Counter Terrorism Program of providing capacity building assistance to 10 South East Asian nations, to develop capacity in detecting and dealing with terrorist financing and money laundering. AUSTRAC is also providing further assistance in terms of IT system enhancement to the Indonesian FIU, PPATK (Indonesian Financial Transaction Reports and Analysis Center). AUSTRAC has provided training and other technical assistance to other developing FIUs in Southeast Asia. In the Pacific region, AUSTRAC has developed and provided unique software and training for personnel to five nascent Pacific island FIUs to fulfill their domestic obligations and share information with foreign analogs. AUSTRAC is also providing a larger scale information management system solution for the Fiji FIU to enable the collection and analysis of financial transaction reports. The AGD received a grant of AUD 7.7 million (approximately $5.75) to develop a four year program to enhance 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 (PALP). The PALP, 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.

The GOA continues to pursue a comprehensive, anti-money laundering/counterterrorist financing regime that meets the objectives of the revised FATF Forty Recommendations and Nine Special Recommendations on Terrorist Financing. To enhance its AML/CTF regime, as noted in the FATF mutual evaluation, AUSTRAC has been provided with substantially increased powers to ensure compliance. There will be more on-site compliance audits and AUSTRAC can require regular compliance reports from reporting entities; can initiate monitoring orders and statutory demands for information and documents; can seek civil penalty orders, remedial directions and injunctions; and, can require a reporting entity to subject itself to an external audit of its AML/CTF program. The AML/CTF Act also provides for greater coordination amongst the regulatory agencies of its financial, securities and insurance sectors.

The GOA is continuing 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. Having significantly enhanced its increased focus on AML/CTF deterrence, the Government of Australia should increase its efforts to prosecute and convict money launderers.

Austria

Austria is not an important financial center, offshore tax haven, or banking center, but Austrian banking groups control significant shares of the banking markets in Central, Eastern and Southeastern

Europe. According to the 2004 IMF Financial Stability Assessment report, Austria also has one of the highest numbers of per capita bank and branches in the world, with about 900 banks and one bank branch for every 1500 people. Austria does not have a reputation as a major money laundering country. However, like any financial marketplace, Austria's financial and nonfinancial institutions are vulnerable to money laundering. The percentage of undetected organized crime is thought to be enormous, with much of it coming from the former Soviet Union. Money that organized crime launders derives primarily from serious fraud, corruption, narcotics trafficking and trafficking in persons.

Money laundering occurs within the Austrian banking system as well as in nonbank financial institutions and businesses. 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 offenses include terrorist financing and many other serious crimes. Regulations are stricter for money laundering by criminal organizations and terrorist "groupings," because in such cases the law requires no proof 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 currency and monetary instruments from illicit sources. Austrian customs authorities do not automatically screen all persons entering Austria for cash or monetary instruments. However, if asked, anyone carrying 10,000 euros (approximately $12,400) or more must declare the funds and provide information on their source and use. To implement the new European Union (EU) regulation on controls of cash entering or leaving the EU, the Government of Austria (GOA) recently amended the Customs Procedures Act and the Tax Crimes Act, lowering the threshold for the "if asked" declaration obligation to 10,000 euros from 15,000 euros ($18,600) as of August 1, 2006. Spot checks for currency at border crossings will continue. Customs officials have the authority to seize suspect cash at the border. An increasing problem is the use of prepaid cards and credit cards loaded with cash.

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 law requires identification of all customers when entering an ongoing business relationship. This would include all cases of opening a checking account, a passbook savings account, a securities deposit account, etc. In addition, the Banking Act requires customer identification for all transactions of more than 15,000 euros ($18,600) for customers without a permanent business relationship with the bank. The law also requires banks and other financial institutions to keep records on customers and account owners. The Securities Supervision Act of 1996, which covers trade of securities, shares, money market instruments, options and other instruments listed on an Austrian stock exchange or any regulated market in the EU, refers to the Banking Act's identification regulations. The Insurance Act of 1997 includes similar regulations for insurance companies underwriting life policies. 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 Banking Act protects bankers and all other reporting individuals (auctioneers, real estate agents, lawyers, notaries, etc.) 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), however, regularly provides 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 must 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 secure electronic signature or a copy of a picture ID and a legal business declaration submitted by registered mail.

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

Amendments in 2003 to the Austrian Gambling Act, the Business Code, and the Austrian laws governing lawyers, notaries, and accounting professionals introduced additional money laundering regulations. The legislation concerns 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.

During Austria's EU Presidency in the first half of 2006, the GOA, in various EU committees and bodies, facilitated the implementation of guidelines for the Financial Action Task Force's (FATF) Special Recommendation VII on wire transfers as well as the EU's Third Money Laundering Directive (Directive 2005/60/EC). The EU regulation on wire transfers entered into force on January 1, 2007, and became immediately and directly applicable in Austria. The GOA also hosted a workshop on nonprofit organizations, terrorism financing and financial sanctions.

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). According to Interpol's General Secretariat, 40 percent of queries that Austria sends have resulted in positive leads. During the first nine months of 2006, the AFIU received 521 suspicious transaction reports from banks and fielded requests for information from Interpol, Europol, members of the Egmont Group, and other authorities. This represents an increase from the 467 suspicious transactions reported in 2005, which led to three convictions for money laundering. Criminals are often convicted for other crimes, however, with money laundering serving as additional grounds for conviction. In 2005, authorities instituted legal proceedings for money laundering in 13 cases, but data on convictions are not yet available. According to the AFIU, the increase in suspicious transaction reports in the first nine months of 2006 is due to higher sensitivity to money laundering, an improved reporting attitude, and the reporting of problems with "phishing" e-mails.

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. In connection with money laundering, organized crime and terrorist financing, all assets are subject to seizure and forfeiture, including bank assets, other financial assets, cars, legitimate businesses, and real estate. Courts may freeze assets in the early stages of an investigation. In the first eight months of 2006, Austrian courts froze assets worth 24 million euros (approximately $30 million). In 2005, courts froze assets worth 99.2 million euros (approximately $124.0 million).

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 bank secrecy regulations, though bank secrecy can be lifted in cases of suspected money laundering. Moreover,

bank secrecy does not apply in cases in which banks and other financial institutions must report suspected money laundering. Such cases are subject to instructions of the authorities (i.e., AFIU) with regard to processing such transactions.

The 2002 Criminal Code Amendment introduced the following new criminal offense categories: terrorist "grouping," terrorist criminal activities, and financing of terrorism. The Criminal Code defines "financing of terrorism" 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. Furthermore, 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, the list of Specially Designated Global Terrorists that the United States has designated pursuant to E.O. 13224, and EU lists. According to the Ministry of Justice and the AFIU, no accounts found in Austria ultimately have shown any links to terrorist financing. The AFIU immediately shares all reports on suspected terrorism financing with the Austrian Interior Ministry's Federal Agency for State Protection and Counterterrorism (BVT). Figures on suspected terrorism financing transaction reports in 2005 and 2006 are not yet available. There were no convictions for terrorism financing in 2005.

The GOA has undertaken important efforts that may help thwart the misuse of charitable or nonprofit entities as conduits for terrorist financing. The GOA has generally implemented the FATF's Special Recommendation on Terrorist Financing regarding nonprofit organizations. The Law on Associations (Vereinsgesetz, published in Federal Law Gazette No. I/66 of April 26, 2002), which has been in force since July 1, 2002, covers charities and all other nonprofit associations in Austria. The law regulates the establishment of associations, bylaws, organization, management, association registers, appointment of auditors, and detailed accounting requirements. On January 1, 2007, special provisions will become effective for associations whose finances exceed a certain threshold. Each association must appoint two independent auditors and must inform its members about its finances and the auditors' report. Associations with a balance sheet exceeding 3 million euros ($3.72 million) or annual donations of more than 1 million euros ($1.24 million) have to appoint independent auditors to review and certify the financial statements. Public collection of donations requires advance permission from the authorities. Since January 1, 2006, the newly established Central Register of Associations (Zentrales Vereinsregister) offers basic information on all registered associations in Austria free of charge via the Internet. The FMA recently announced intentions to employ 45 additional auditors to focus on combating money laundering, terrorist financing, as well as to better monitor offshore banking and charitable foundations.

Another law, the Law on Responsibility of Associations (Verbandsverantwortlichkeitsgesetz, published in Federal Law Gazette No.I/151 of December 23, 2005), came into force on January 1, 2006, and introduced criminal responsibility for all legal entities, general and limited commercial partnerships, registered partnerships and European Economic Interest Groupings, but not charitable or nonprofit entities. The law covers all crimes listed in the Criminal Code, including corruption, money laundering and terrorist financing.

Austria has not yet enacted legislation that provides for sharing forfeited narcotics-related assets with other governments. A bilateral U.S.-Austria agreement on sharing of forfeited assets remains under negotiation. In addition to the exchange of information with home country supervisors permitted by 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), as well as Bulgaria and Croatia. Austria has also given assistance to countries needing guidance in developing effective AML/CFT regimes: in March 2006, under the auspices of the EU, Austria assisted the FYROM with discussions highlighting Austria's experience, and best practices in AML, confiscation and seized assets management.

Austria is a party to the 1988 UN Drug Convention, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. The GOA ratified the UN Convention against Corruption on January 11, 2006. Austria is a member of the EU and FATF, and a FATF mutual evaluation of Austria will take place in 2008. The AFIU is a member of the Egmont Group.

The Government of Austria has implemented a viable anti-money laundering and counterterrorist financing regime, and is generally cooperative with U.S. authorities in money laundering cases. However, certain deficiencies remain. There is a need for identification procedures for customers in non-face-to-face banking transactions. The GOA should amend its criminal code to penalize negligence in reporting money laundering and terrorist financing transactions. In spite of increases in suspicious transaction reporting and money laundering convictions in 2006, the AFIU and law enforcement require sufficient resources to adequately perform their functions. Finally, AFIU and other government personnel should be protected against damage claims because of delays in completing suspicious transactions until sufficient resources are provided to ensure timely reporting. The GOA should also ensure that it enhances inspections at its borders to protect against the cross-border transport of cash and negotiable instruments in concert with FATF Special Recommendation IX on Terrorist financing.

Bahamas

The Commonwealth of The Bahamas is an important regional and offshore financial center. The financial services sector provides vital economic contribution to The Bahamas, accounting for approximately 15 percent of the country's 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, drug traffickers store 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, as well as 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, one in Freeport/Lucaya, and one in Great Exuma. Cruise ships that overnight in Nassau may operate casinos. Reportedly, there are over ten internet gaming sites based in The Bahamas, although internet gambling is illegal in The Bahamas. Under Bahamian law, Bahamian residents are prohibited from gambling. Freeport is home to The Bahamas' only free trade zone. There are no indications that it is used to launder money.

The Central Bank of The Bahamas is responsible for the licensing, regulation, and supervision of banks and trust companies operating in 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 and provide the Central Bank with extensive information gathering powers, including on-site inspection of banks and 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. These expanded rights include the right to deny licenses to banks or trust companies deemed 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 a registered 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 is complete. Some industry sources have suggested that this requirement has contributed to a decline in banks and trusts from 301 in 2003 to 250 at the end of 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 agents, registered offices, nominee shareholders, and officers and directors for IBCs.

Money laundering is criminalized under the Proceeds of Crime Act 2000. The Financial Transaction Reporting Act 2000 (FTRA) 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 October 2006, the Central Bank reported full compliance with KYC requirements. All nonverified accounts have been frozen.

The FTRA requires financial and nonfinancial institutions to report suspicious transactions to the financial intelligence unit (FIU) when the institution suspects or has reason to believe that any transaction involves the proceeds of crime. The FIU Act 2000 protects obligated entities from criminal or civil liability for reporting transactions. Financial institutions are required by law to maintain records related to financial transactions for no less than five years. Established by the FIU Act 2000, The Bahamas FIU operates as an independent administrative body under the Office of the Attorney General, and is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs). The FIU is also responsible for publishing guidelines to advise entities of their reporting obligations. Presently, the FIU is in the process of revising its guidelines to incorporate terrorist financing reporting requirements, and is expected to publish the new guidelines in early 2007.

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. In 2005 there were nine cases of asset restraint as a result of suspicious transactions. From January to September 2006, the FIU received 124 STRs, of which 60 were being analyzed and 15 were forwarded to the police for investigation. If money laundering is suspected, the FIU will disseminate STRs to the Tracing and Forfeiture/Money Laundering Investigation Section (T&F/MLIS) of the Drug Enforcement Unit (DEU) of the Royal Bahamas Police Force for investigation and prosecution in collaboration with the Office of the Attorney General.

Between January 2000 and September 2006, 17 individuals were charged with money laundering by the T&F/MLIS, leading to seven convictions. Seven defendants await trail, while two defendants fled the jurisdiction prior to trial. As a matter of law, the Government of the Commonwealth of the Bahamas (GOB) seizes assets derived from international drug trade and money laundering. The banking community has cooperated with these efforts. During 2006, nearly two million dollars in cash and assets were seized or frozen. The seized items are in the custody of the GOB. Some are in the

process of confiscation while some remain uncontested. Seized assets may be shared with other jurisdictions on a case-by-case basis.

In 2004, the Anti-Terrorism Act (ATA) was enacted 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. To date, there have been no suspicious transactions or prosecutions for violation of the ATA.

The Bahamas is a party to the UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The Bahamas has signed, but has not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOB has neither signed nor ratified the UN Convention against Corruption. The Bahamas is a member of the Caribbean Financial Action Task Force (CFATF) and recently underwent a Mutual Evaluation in June 2006. The FIU has been an active participant within the Egmont Group since becoming a member in 2001, and is currently one of the two regional representatives for the Americas. 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. The Bahamas FIU has the ability to sign memoranda of understanding with other FIUs for the exchange of information.

The GOB has enacted substantial reforms to reduce its vulnerability to money laundering and terrorist financing. The GOB should continue to enhance its supervision of financial institutions, especially investment funds. The Bahamas should also provide adequate resources to its law enforcement, prosecutorial and judicial entities 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 Gulf Cooperation Council (GCC). In contrast to most of its neighbors, oil accounted for only 11.1 percent of Bahrain's gross domestic product (GDP) in 2005. Bahrain has promoted itself as an international financial center in the Gulf region. It hosts a mix of 375 diverse financial institutions, including 187 banks, of which 51 are wholesale banks (formerly referred to as off-shore banks or OBUs); 39 investment banks; and 25 commercial banks, of which 17 are foreign-owned. There are 31 representative offices of international banks. In addition there are 21 moneychangers and money brokers, and several other investment institutions, including 85 insurance companies. The vast network of Bahrain's conventional banking system—coupled with a vibrant Islamic banking sector—attracts a high volume of financial activity. With its strategic geographical location in the Middle East, close ties to neighboring Saudi Arabia, and as a transit point and communication hub along the Gulf into Southwest Asia, Bahrain may attract money laundering activities. It is thought that the greatest risk of money laundering stems from questionable foreign proceeds that transit Bahrain. Other sources of money laundering in Bahrain include hawala, trade fraud, real estate, and smuggling.

Bahrain criminalized money laundering in January 2001, with punishment of up to seven years in prison, and a fine of up to one million Bahraini dinars (approximately $2.65 million). 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 Bahraini dinars (approximately $265,000) and a prison term of not less than five years.

In August 2006, Bahrain passed Law 54/2006, which amended certain provisions of the 2001 anti-money laundering law to include banning and combating money laundering and terrorist financing. Law 54 criminalizes the undeclared transfer of money across international borders for the purpose of money laundering or supporting terrorism. Shortly after the passage of Law 54, Bahrain passed Law No. 58 of 2006 pertaining to the "Protection of the Community against Terrorist Acts." Under these laws, persons convicted of collecting or contributing funds, or otherwise providing financial support to a group or persons who practice terrorist acts, whether inside or outside Bahrain, will be subject to imprisonment for a minimum of ten years in prison up to a maximum of a life sentence. Notably, the AML law allows Bahrain to prosecute a money laundering violation regardless of whether the underlying act is a crime in Bahrain. For example, although there is no income tax system in Bahrain, someone engaging in illicit financial transactions for the purpose of evading another nation's tax system may be prosecuted for money laundering in Bahrain.

A controversial feature of the new law is a revised definition of terrorism that is based on the definition as set forth by the Organization of the Islamic Conference. Article 2 excludes from the definition of terrorism acts of struggle against invasion or foreign aggression, colonization, or foreign supremacy in the interest of freedom and the nation's liberty.

Under the original anti-money laundering law, the Bahrain Monetary Agency (BMA), the principal regulator of the financial sector, 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. The current requirement for filing STRs stipulates no minimum thresholds. In 2005, the BMA established a secure online website, by which banks were enabled to file STRs. Immunity from criminal or civil action is given to those who report suspicious transactions. The law further provides for the confiscation of assets and allows for greater international cooperation.

In June 2001, the Policy Committee for the Prohibition and Combating of Money Laundering and Terrorist Financing was established, as an interagency committee to oversee and coordinate Bahrain's anti-money laundering efforts. The committee, which is under the chairmanship of the Deputy Governor of BMA, includes members from the Bahrain Stock Exchange, the Ministries of Finance and National Economy, Interior, Justice, Commerce, Social Development, and Foreign Affairs.

The Anti-Money Laundering Unit (AMLU) was established in 2002 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 as well as suspicious operations; conduct investigations; disseminate information to local law enforcement; share information with international counterparts; 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, moneychangers, insurance firms, real estate agents, gold dealers, financial intermediaries, and attorneys. Financial institutions file copies of the STRs with the BMA. Nonfinancial institutions are required under a Ministry of Industry and Commerce (MOIC) directive to also file STRs with that ministry. 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. The BMA does not independently investigate the STRs, since responsibility for investigation rests with the AMLU. However, BMA may assist the AMLU with its investigations, particularly in cases where special banking expertise is required.

The BMA is the regulator for other nonbanking financial institutions including insurance companies, exchange houses, and capital markets. BMA inspected four insurance companies in 2005 and had conducted six more inspections by November 2006. More insurance industry inspections are

scheduled for 2007. Anti-money laundering regulations for investment firms and securities brokers were revised in April 2006.

In November 2003, the MOIC published new anti-money laundering guidelines, which govern designated nonfinancial businesses and professions (DNFBPs). The MOIC has also announced an increased focus on enforcement, noting some 300 visits to DNFBPs in 2005, including car dealers, jewelers, real estate agencies, etc. By November 2006, the MOIC had conducted an additional 274 enforcement follow-up visits. A total of 140 of these have been assigned an MOIC compliance officer as a result. The MOIC has also increased its inspection team staff from four to seven.

The MOIC system of requiring dual STR reporting to both it and the AMLU mirrors the BMA's system. Reportedly, good cooperation exists between MOIC, BMA, and AMLU, with all three agencies describing the double filing of STRs as a backup system. The AMLU and BMA's compliance staff analyze the STRs and work together on identifying weaknesses or criminal activity, but it is the AMLU that must conduct the actual investigation and forward cases of money laundering and terrorist financing to the Office of Public Prosecutor. From January through November 2006, the AMLU has received and investigated 118 STRs, 26 of which have been forwarded to the Office of Public Prosecutor for prosecution. The GOB completed its first successful money laundering prosecutions in May 2006. The prosecutions resulted in two convictions with sentences of one and three years and fines of $380 and $1,900 respectively.

Bahrain is moving ahead with plans to establish a special court to try financial crimes. The court is expected to begin hearing cases in May 2007, and Bahraini judges are undergoing special training to handle such cases.

There are 51 BMA licensed wholesale Banks, which formerly were referred to as offshore banking units (OBUs) that are branches of international commercial banks. Such new licenses allow wholesale banks to accept deposits from citizens and residents of Bahrain, and undertake transactions in Bahraini dinars. Wholesale banks are regulated and supervised in the same way as the domestic banking sector, and are subject to the same regulations, on-site examination procedures, and external audit and regulatory reporting obligations.

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.

In January 2002, the BMA issued circular BC/1/2002, which implemented the Financial Action Task Force (FATF) Nine Special Recommendations on Terrorist Financing as part of the Central Bank's AML regulations. Subsequently, the BMA froze two accounts that had been designated by the UNSCR 1267 Sanctions Committee, and one account that was listed under U.S. Executive Order 13224.

Circular BC/1/2002 also 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 Central Bank 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 are required to file suspicious transaction reports (STRs) if they suspect that the funds being transferred are linked to suspicious activities or terrorist financing. Licensees must also maintain records of the identity of their customers in accordance with the Central Bank'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 Recommendations plus Nine Special Recommendations. Revised

and updated BMA regulations were issued in mid- 2005. The BMA is drafting new regulations to be issued in 2007 intended to enhance existing circulars regarding requirements for money changers.

Legislative Decree No. 21 of 1989 governs the licensing of nonprofit 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, MSD 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. Banks must report to BMA any transaction by a charitable institution that exceeds 3,000 Bahraini dinars (approximately $8,000). MSD has the right to inspect records of the societies to insure their compliance with the law.

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 32 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 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 November 2004, Bahrain hosted the inaugural meeting of the Middle East and North Africa Financial Action Task Force (MENAFATF). Bahrain also serves as the headquarters for the MENAFATF Secretariat.

In October 2006, the Policy Committee for the Prohibition and Combating of Money Laundering and Terrorist Financing announced the formation of two new sub-committees: the U.N. Sub-Committee, which will head a new inter-agency framework for disseminating and reviewing international financial crimes designations; and the Legal Sub-Committee, which will coordinate the drafting of any future financial crimes legislation.

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

The Government of Bahrain has demonstrated a commitment to establish a strong anti-money laundering and terrorist financing system and appears determined to engage its large financial sector in this effort. The Anti-Money Laundering Unit should maintain its efforts to obtain and solidify the necessary expertise in tracking suspicious transactions. However, there should not be an over-reliance on suspicious transaction reporting. Bahraini law enforcement and customs authorities should take a more active role in recognizing, initiating and pursuing investigations in anti-money laundering and counterterrorist financing cases. The Ministry of Social Development should expand and provide training for its staff with NGO/charities oversight responsibilities. Bahrain should become a party to the UN Convention against Corruption.

Bangladesh

Bangladesh is not an important regional or offshore financial center.

While there is evidence of funds laundered through the official banking system, there is no indication of large-scale abuse. Money transfers outside the formal banking and foreign exchange licensing system are illegal. The principal money laundering vulnerability remains the widespread use of the underground hawala or "hundi" system to transfer money and value outside the formal banking network. The vast majority of hundi transactions in Bangladesh are used to repatriate wages from Bangladeshi workers abroad.

The Central Bank has reported a considerable increase in remittances since 2002 through official channels. The figure has more than doubled from $2 billion to the current level of $4.3 billion in fiscal year 2006 (July 1-June 30). The increase is due to competition from the government and commercial banks through improved delivery time and valued-added services, such as group life insurance. Hundi, however, will probably never be completely eradicated as it is used to avoid taxes, customs duties and currency controls. The nonconvertibility 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.

In Bangladesh, hundi primarily uses trade goods to provide counter valuation or a method of balancing the books in transactions. It is part of trade-based money laundering and a compensation mechanism for the significant amount of goods smuggled into Bangladesh. An estimated $1 billion dollars worth of dutiable goods are smuggled every year from India into Bangladesh. A comparatively small amount of goods are 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. For the past five years (2001-2005) Bangladesh has been ranked by Transparency International's Corruption Perception Index as the country with the highest level of perceived corruption in the world. In 2006, Bangladesh was ranked 156 out of 163 countries surveyed.

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 has conducted training for commercial banks' headquarters around the county in "know your customer" practices. Since Bangladesh does not have a national identity card and because the vast majority of 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 slowly changing, especially in head offices. Accounting procedures used by the Central Bank may not achieve international standards in every respect. In 2004, the Central Bank issued "Guidance Notes on Prevention of Money Laundering" and designated anti-money laundering compliance programs as a "core risk" subject to the annual bank supervision process of the Central 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 Central Bank conducts regular training programs for compliance officers based on the Guidance Notes. In December 2005, the Central Bank called all compliance officers to Dhaka for a discussion about their obligations and heightened police interest in money laundering and terrorist financing. During 2006, the Central Bank continued to work with compliance officers around the country, sending their instructors to regional workshops.

Currently, Bangladesh is working to formalize operations for a Financial Intelligence Unit (FIU). Under the 2002 Money Laundering Prevention Act (MLPA), the Anti-Money Laundering Unit (AMLU) of the Central 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 Central Bank has approved the purchase of hardware for

the nascent FIU, which will be coupled with link analysis software provided by the U.S. Department of Justice.

The Central Bank has received approximately 236 suspicious transaction reports since the MLPA was enacted in 2002. To date, there have been no successful prosecutions in part due to procedural problems in adjusting to inter-agency cooperation. A major setback occurred in December 2005 when the newly created Anti-Corruption Commission (ACC) advised the bank that it would not investigate these cases and returned them. The Criminal Investigation Division of the country's police force agreed to take the cases. During 2006, the bank and police hammered out a procedure to investigate cases initiated by the bank through suspicious transactions reports. With the approval of the Law Minister, dedicated government attorneys will handle the prosecutions. Officials expect prosecutions to begin in spring 2007.

The Anti-Money Laundering and Terrorist Financing Act 2005 (AMLTF), drafted to replace the MLPA from 2002, was shelved due to political issues related to upcoming national elections expected in January 2007. The draft AMLTF provided powers required for a FIU to meet most of the international recommendations set forth by the Egmont Group, including sharing information with law enforcement at home and abroad. The draft legislation also provided for the establishment of a Financial Investigation and Prosecution Office wherein law enforcement investigators and prosecutors would work as a team from the beginning of the case to trial. The 2005 draft legislation addressed asset forfeiture and provided that assets, substitute assets (without proving the relation to the crime) and instrumentalities of the crime can be forfeited. It did not, however, address the nuts and bolts of asset forfeiture, which the Central Bank asserts can be addressed administratively and via regulatory procedures. Changes following cabinet review weakened the draft by, for example, deleting provisions for the establishment of an enforcement group that would be comprised of Central Bank analysts, police and prosecutors.

The AML draft also criminalized terrorism financing. The government announced that it wanted a separate Anti-Terrorism law that would criminalize terrorist financing, stipulating that the Anti-Terrorism Act (ATA) would have to be passed before the AML. The ATA law was not sent to Parliament in 2006. A worrying development in the initial review stage of the ATA was the removal of the section providing for international cooperation.

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, the Central Bank fined two local banks for failure to comply with Central 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 and protocols 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 some advancement, the Government of Bangladesh's anti-money laundering/terrorist financing regimes should be strengthened to comply with international standards. Bangladesh should criminalize terrorist finance. Legislation should provide for safe harbor provisions in order to protect reporting individuals, due diligence programs, and banker negligence accountability that would make individual bankers responsible under certain circumstances if their institutions launder money. Bangladesh should create a financial intelligence collection system and establish a viable Financial Intelligence Unit to analyze the intelligence. A lack of training, resources and computer technology, including computer links with the outlying districts, continue to hinder progress. Bangladesh law enforcement and customs should examine forms of trade-based money laundering. Bangladesh should further efforts to combat pervasive corruption, which is intertwined with money laundering,

smuggling, and tax evasion. Bangladesh should ratify the UN Convention against Transnational Organized Crime.

Barbados

A transit country for illicit narcotics, Barbados remains attractive for money laundering, which primarily occurs through the formal banking system. There is also evidence of proceeds being directed to financial institutions in Barbados by criminals abroad.

As of July 30, 2006, there were six commercial banks and 14 nonbank financial institutions in Barbados. The offshore sector consists of 54 offshore banks, 4,635 international business companies (IBCs), 178 exempt insurance companies (a significant reduction from 2005), 57 qualified exempt insurance companies, nine mutual funds companies, one exempt mutual fund company, seven trust companies, and six finance companies. According to the Central Bank, it is estimated that there is approximately $32 billion worth of assets in Barbados's offshore banks. There are no free trade zones, casinos, or internet gaming sites in Barbados.

The Central Bank regulates and supervises both on and offshore banks, trust companies, and finance companies. The Ministry of Finance issues banking licenses after the Central Bank receives and reviews applications, and recommends applicants for licensing. The International Financial Services Act 2002 incorporates fully the standards established in the Basel Committee's Core Principles for Effective Banking Supervision and provides for on-site examinations of offshore banks. On-site examinations of licensees use a comprehensive methodology that seeks to assess the level of compliance with legislation and guidelines. Offshore banks must submit quarterly statements of assets and liabilities and annual balance sheets to the Central Bank. Additionally, the Central Bank conducts off-site surveillance, which consists of reviewing financial data as well as other documents submitted by financial institutions. The Central Bank revised its Anti-Money Laundering Guidelines in 2001. The revised "know your customer" guidelines provide detailed guidance to financial institutions regulated by the Central Bank.

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 permitted, 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 more information than was previously provided for IBC license applications or renewals.

The Government of Barbados (GOB) criminalized drug money laundering in 1990 through the Proceeds of Crime Act. The Act 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 1998 (MLPCA) extends the offense of money laundering beyond drug-related crimes, and criminalizes the laundering of illicit proceeds from unlawful activities that are punishable by at least one year's imprisonment. Under the MLPCA, money laundering is punishable by a maximum of 25 years in prison and a maximum fine of $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 extend to other financial institutions, including money remitters, investment services, and 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 $5,000 for a period of five years, and establish internal auditing and compliance procedures.

The Anti-Money Laundering Authority (AMLA) was created to supervise financial institutions' compliance with the MLPCA. Financial institutions must also report suspicious transactions to the

AMLA through the Barbados Financial Intelligence Unit (FIU). There are no laws that prevent disclosure of information to relevant authorities, and individuals reporting to the FIU are protected by law. The AMLA is also responsible for issuing anti-money laundering training requirements and regulations for financial institutions. However, staff constraints limit the direct supervisory capacity of the AMLA.

The FIU is housed in the Office of the Attorney General within the AMLA. The FIU was established in September 2000 and is fully operational as an independent agency. From January 1-June 30, 2006, the FIU received 41 suspicious activity reports (SARs)—half of the amount received the previous year—and referred two cases to the Commissioner of Police. The FIU reports that though there has been a decrease in SARs, the quality of SARs received has improved. The FIU forwards information to the Financial Crimes Investigation Unit of the police if it has reasonable grounds to suspect money laundering. Government entities and financial institutions are required to provide additional information to the FIU upon request by the FIU Director. The FIU also has the ability to negotiate memoranda of understanding (MOUs) with foreign counterparts.

The MLPCA only provides for criminal asset seizure and forfeiture, not civil 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. Legitimate businesses and other financial institutions are subject to criminal sanctions and the termination of operating licenses. Tracing, seizing and freezing assets may be done by the FIU and the police. Freezing orders are usually granted for six months at a time after which they need to be reviewed. Frozen assets may be confiscated on application by the Director of Public Prosecutions and are paid into the National Consolidated Fund. No asset sharing law has been enacted, but bilateral treaties as well as the Mutual Assistance in Criminal Matters Act, have provisions for asset tracing, freezing and seizure between countries.

The Barbados Anti-Terrorism Act 2002, as well as provisions of the Money Laundering Financing of Terrorism (Prevention and Control) Act (MLFTA), criminalize the financing of terrorism. The MLFTA has a provision for information sharing between the Barbados Customs Department and the FIU, and is also designed to control bulk cash smuggling and the use of cash couriers. 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. To date, the GOB has found no evidence of terrorist financing. The GOB has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and nonprofit entities.

Barbados has bilateral tax treaties that eliminate or reduce double taxation with fourteen countries including the United States. The United States and the GOB ratified amendments to their bilateral tax treaty in 2004. 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 Caribbean Financial Action Task Force (CFATF) and underwent a Mutual Evaluation in December 2006. Barbados is also a member of the Offshore Group of Banking Supervisors, the Caribbean Regional Compliance Association, 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. Barbados is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GOB has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the Inter-American Convention against Terrorism.

Although the GOB has strengthened the anti-money laundering legislation, it must steadfastly enforce the laws and regulations it has adopted. The GOB should adopt civil forfeiture and asset sharing legislation. Barbados should be more aggressive in conducting examinations of the financial sector and maintaining strict control over vetting and licensing of offshore entities. The GOB should ensure adequate supervision of nongovernmental organizations and charities. It should also work to improve information sharing between regulatory and enforcement agencies. In addition, Barbados should continue to provide adequate resources to its law enforcement and prosecutorial personnel, to ensure Mutual Legal Assistance Treaty requests are efficiently processed.

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, but Belarus has many vulnerabilities, including organized crime. Due to inflation, excessively high taxes, underground markets, 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. Smuggling is prevalent. Corruption is a severe problem in Belarus, which exacerbates financial crimes enforcement and retards needed reforms.

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 the Republic of Belarus (NBRB), and even market forces. Under the decree, legislation that contradicted the decree became void in June. On January 28, 2006 the President issued a decree granting him powers to confiscate at will any plot of land for agricultural, environmental, recreational, historical, and cultural uses. The President subsequently relinquished some of his nominal power in June by abolishing for banks the "golden share" rule that permits the government to interfere in the decision-making of any company formerly owned by the government. Moreover, the President canceled a requirement that foreign capital must account for 25 percent of the total authorized capital stock of the country's banks. However, the government imposed penalties on 107 government-owned enterprises that failed to transfer accounts from private banks to government-owned financial institutions per a 2005 presidential directive.

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. On January 31, 2006, President Lukashenko signed degree 66, which tightened FEZ regulations on transaction reporting and security, including mandatory video surveillance systems.

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 nonbank 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; leasing and estate agents; post

offices; dealers in precious stones and metals; attorneys conducting financial transactions on behalf of clients; 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 nondrug 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 NBRB has issued suggested anti-money laundering and counterterrorist financing (AML/CFT) regulations, including know your customer (KYC) and due diligence requirements. Although these are not legally binding, they are treated as mandatory by the institutions overseen by the NBRB.

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, or DFM); 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; the Ministry on Taxes and Duties (MTD); and other state bodies. The MTD also provides oversight and has released binding regulations on its subject institutions.

On March 17, 2006 a series of amendments to the AML Law passed by parliament in December 2005 to enhance money laundering prevention came into effect. Under the new law, individual and corporate financial transactions exceeding approximately $27,000 and $270,000, respectively, are subject to special inspection. Banks that violate the new law face fines of up to one percent of their registered capital and suspension of their licenses for up to one year. However, this is a threshold reporting requirement. A 2005 International Monetary Fund (IMF) Financial System Stability Assessment pointed out that the AML/CFT framework, including that of suspicious transaction reporting, needed to be significantly upgraded to meet FATF standards. Additionally, the new law exempts most government transactions and transactions sanctioned by the President from extraordinary inspection. Moreover, the government used the anti-money law as a pretext for preventing several pro-democracy NGOs from receiving foreign assistance.

In January 2005, the President signed a decree on the regulation of the gaming sector, making the owners of gambling businesses subject to stricter tax regulations. In addition, a provision intended to combat money laundering requires those participating in gaming activities to produce identification in order to receive a monetary winnings.

On February 9, 2006, the government abolished 1997 identification requirements for all foreign currency exchange transactions at banks. The Belarusian banking sector consists of 31 banks. Of these, 27 have foreign investors and nine banks are foreign owned. As of May 1, 2006 the capital base of Belarus' banks totaled almost $10 billion. The state-owned Belarus Bank is the largest and most influential bank in Belarus. In 2005, Belarus Bank conducted $2.7 million dollars in financial transactions with Russian clients, 28 percent more than 2004. In April, Russia's Burbank opened a $2 million credit line to Belarus Bank for trade finance on an unsecured basis. By 2006, total credit lines to Belarus Bank from foreign financial institutions amounted to $220 million. 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. In April 2006, President Lukashenko signed ordinance 259, which granted the DFM the power to suspend the financial operations of any company suspected of money laundering or financing terrorism.

The DFM cooperates with its counterparts in foreign states and with international organizations to combat money laundering. In 2005, the DFM fielded 19 inquiries from other FIUs, and requested information 34 times from other FIUs. The DFM is not a member of the Egmont Group, but it has applied for membership. The DFM's counterpart FIUs from Russia and Poland are the DFM's sponsors for Egmont membership.

Financial institutions are obligated to report to the DFM transactions subject to special monitoring, including: transactions whose suspected purpose is money laundering or terrorism financing; 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 reported 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 and examine the internal rules and enforcement mechanisms of any financial institution. The DFM also has the authority to initiate its own investigations.

Failure to report and transmit the required information on financial transactions may subject a bank or other financial institution to criminal liability. The National Bank of the Republic 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. In February 2006, the Interior Ministry announced the establishment of a new counterterrorism department within its Main Office against Organized Crime and Corruption.

Belarusian legislation provides for broad seizure powers and for law enforcement to identify and trace assets. Seizure based on a criminal conviction is in the Criminal Code for all serious offenses, including money laundering. Seizure of assets from third parties appears to be possible but is not specifically codified. 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 2006, Belarus has not identified any assets as belonging to individuals or entities included on the UNSCR 1267 Sanctions Committee's consolidated list.

Domestically, Belarus has made an effort to ensure cooperation and coordination between state bodies through the Interdepartmental Working Group; this Group has been established specifically to address these AML/CFT issues. This Working Group includes representatives of the Prosecutor's office, the National Bank, MTD, State Security Committee, Department of Financial Investigation, and the DFM. The Director of the DFM serves as the head of this Group.

Belarus has signed bilateral treaties on law enforcement cooperation with Bulgaria, India, Lithuania, the People's Republic of China, Poland, Romania, Turkey, the United Kingdom, and Vietnam. In September, 2006 Belarus signed an anti-money laundering agreement with the People's Bank of China. 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 also assumed international commitments to combat terrorism as a member of the Collective Security Treaty Organization (CSTO), which includes Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan.

Belarus is a party to the UN International Convention for the Suppression of the Financing of Terrorism. However, over the past year, Belarus has significantly expanded its economic relations with state sponsors of terrorism. In May, 2006 President Lukashenko hosted senior officials of Syria's governing Baath Party and signed several economic cooperation agreements. In October, following Foreign Minister Sergey Martynov's visit to Tehran, Belarus and Iran began formal negotiations to open Iranian banks in Minsk. In November, 2006, President Lukashenko visited Iran.

Belarus is a party to the 1988 UN Drug Convention and to the UN Convention against Transnational Organized Crime. On September 15, 2005, Belarus became a signatory to the UN International Convention for the Suppression of Acts of Nuclear Terrorism.

Belarus is a party to the UN Convention against Corruption. 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. On January 31, the Belarusian State Customs Committee unveiled an anticorruption plan that included stiffer penalties for bribery and closer cooperation with law enforcement authorities. On July 20, 2006 President Lukashenko signed an anticorruption law to comply with the Council of Europe's 1999 Criminal Law Convention on Corruption, which Belarus ratified in 2004. The law expanded Belarus' existing anticorruption legislation by defining professions and individuals vulnerable to and capable of corruption to include senior government officials; members of parliament and local councils; presidential, parliamentary, and local council candidates; foreign officials; officials of private organizations that perform administrative and control functions; and volunteers assisting law enforcement agencies in maintaining public order. However, corruption remains a serious obstacle to enforcing laws dealing with financial crimes. Belarus is 151 out of 163 countries listed in Transparency International's 2006 International Corruption Perception Index.

The Government of Belarus (GOB) has taken 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, and ensure that the regulations and guidance provided are legally binding. The GOB should implement strict regulation of its offshore industries and those operating within the FEZ areas. The GOB needs to reinstate the identification requirement for foreign currency exchange transactions. It should hone its guidance and enforcement of suspicious transaction reporting and provide adequate resources to its FIU so that it can operate effectively. The GOB must work to further improve the coordination between agencies responsible for enforcing anti-money laundering measures. The GOB also needs to take steps to ensure that the anti-money laundering framework that does exist is used in a manner consistent with the reason for which it was implemented, rather than using it in a political manner. The GOB should take serious steps to combat corruption in commerce and government.

Belgium

The banking industry of Belgium is of medium size, with assets of over $1.9 trillion dollars in 2005. Strong legislative and oversight provisions are in place in the formal financial sector to combat money laundering and terrorist financing. Belgian officials have noted that criminals are increasing their use of the nonfinancial professions to facilitate access to the official financial sector.

Belgium criminalized money laundering through the Law of 11 January 1993, On Preventing Use of the Financial System for Purposes of Money Laundering. This law outlined the customer due diligence and reporting requirements. These are applicable to nonfinancial business and professions as well. Obligated entities include estate agents, private security firms, funds transporters, diamond merchants, notaries, bailiffs, auditors, chartered accountants, tax advisors, certified accountants, and casinos, when customers seek to execute a financial transaction in connection with their gambling. Additional laws made the requirements applicable to other sectors as well: the Law of 22 March 1993, On the Legal Status and Supervision of Credit Institutions; and the Law of 6 April 1995, On Secondary Markets, On Legal Status and Supervision of Investment Firms, On Intermediaries and Investment Advisors. Article 505 of the Penal Code sets penalties of up to five years of imprisonment for money laundering convictions. Any unlawful activity may serve as the predicate offense.

The Law of 12 January 2004 amended Belgian domestic legislation by making it applicable to attorneys, and implementing the Second European Union (EU) Directive on Money Laundering, or Council Directive 2001/97/EC On Prevention of the Use of the Financial System for Money Laundering, which broadened the scope of money laundering predicate offenses beyond drug trafficking to include the financing of terrorist acts or organizations. This Law was challenged by the Belgian bar association and taken to the Court of Arbitration, which referred the challenge to the

European Court of Justice. The bar has argued that the Second EU Directive violates the right to a fair trial by the obligated attorneys, because the reporting obligations prejudice the lawyers against fully and independently representing their clients.

In June 2005 Belgium underwent a mutual evaluation by the Financial Action Task Force (FATF). Although the report concluded that Belgium's anti-money laundering and counterterrorism financing (AML/CFT) regime is effective, the assessment team found it partially compliant or noncompliant in certain areas. These areas include: due diligence and regulation requirements for designated nonfinancial businesses and professions, licensing or registration of businesses providing money or value transfer services, allocation of adequate resources to the authorities charged with combating financial crimes, elimination of bearer bonds, development of an independent authority to freeze assets, and implementation of a system to monitor cross-border currency movements. Belgium is currently working to address these deficiencies. In 2007 Belgium must report back to FATF regarding its progress in implementing these recommendations.

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. In 2006 further raids uncovered numerous counterfeit phone cards and illegal or undocumented workers in addition to evidence of money laundering activities in some locations. Since 2004, more than 130 such shops have been closed by Belgian authorities, who estimate that the Belgian state may be deprived of up to $256 million in lost tax revenue each year through tax evasion by these businesses. Authorities report that phone shops often declare bankruptcy and later reopen under new management, making it difficult for officials to trace ownership and collect tax revenues. Authorities believe that 3,000- 5,000 phone shops may be operating in Belgium. Only an estimated one-quarter 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.

Belgium's robust diamond industry presents special challenges for law enforcement. Despite some diffusion in recent years, Belgium continues to be the world's diamond-trading center. Fully 90 percent of the world's crude diamonds and 50 percent of cut diamonds pass through Belgium. Most of the "blood" or "conflict diamonds" from long-running African civil wars were processed in Antwerp. 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 introduced much-needed transparency into the global diamond trade. However, diamonds of questionable origin continue to appear on the Belgium market. 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. 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.

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. Belgian law mandates reporting of suspicious transactions by a wide variety of financial institutions and nonfinancial entities, including notaries, accountants, bailiffs, real estate agents, casinos, cash transporters, external tax consultants, certified accountant-tax experts, and lawyers. Lawyers in particular do not consistently comply with reporting requirements. Belgian lawyers, for example, did not report any suspicious transactions to the FIU in 2005. 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. As of October 2006, a decision from the court of arbitration was still pending.

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 $13,250). 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 $1.56 million.

Money laundering legislation imposes prohibitions on cash payments for real estate, except for an amount not exceeding 10 percent of the purchase price or approximately $18,800, whichever is lower. Cash payments over $18,800 for goods are also illegal.

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 cease the issuance of bearer bonds beginning on January 1, 2008. Bearer bonds issued before that date will still be valid, however. Bearer shares are permitted for individuals as well as for banks and companies.

Currently, Belgium has no reporting requirements on cross-border currency movements. However, 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 expects to implement this regulation by June 15, 2007, as required. Belgian customs officials and CTIF-CFI will verify cross-border currency movements, and irregularities may be forwarded to judicial authorities.

Belgium and other EU member states must implement the Third EU Money Laundering Directive by December 15, 2007. As for nonprofit organizations, the European Commission adopted a communication on November 29, 2005, that includes recommendations for EU member states and a framework for a code of conduct for the sector. Belgian officials are working to increase transparency in the nonprofit sector through better enforcement of registration and reporting procedures. Requirements for nonprofit organizations include registering, furnishing copies of their statutes and list of members, providing minutes from council meetings, and filing budget reports.

The Belgian financial intelligence unit (FIU), known as the Cellule de Traitement des Informations Financières and in Flemish as Cel voor Financiële Informatieverwerking (CTIF-CFI), was created by the Royal Decree of 11 June 1993, on the Composition, Organization, Operation and Independence of the FIU. 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. CTIF-CFI's primary mission is to receive, analyze, and disseminate all suspicious transaction reports submitted by regulated entities. Operating as a filter between obligated entities and judicial authorities, CTIF-CFI reports possible money laundering or terrorist financing transactions to the public prosecutor. 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. CTIF-CFI also acts as the supervisory body for professions not supervised by CBFA or other authorities. CTIF-CFI has also been very active in analyzing the diamond industry and working to eliminate its potential for money laundering and terrorist financing. 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 and how diamond traders apply this legislation.

Financial experts, including three magistrates (public prosecutors) appointed by the King compose the CTIF-CFI. A magistrate presides over the body. Terms of service are for six years and may be renewed. In addition to administrative and legal support, the investigative department consists of inspectors/analysts. There are also three liaison police officers, one customs officer, and one officer of the Belgian intelligence service to maintain contact with the various law enforcement agencies in Belgium.

From its founding in 1993 until the end of 2005, CTIF-CFI received 104,537 disclosures and opened a total of 21,959 individual case files (numerous disclosures may be linked to a single case). Of these, the FIU has transmitted 7,114 cases to the public prosecutor aggregating approximately $15.48 billion. In 2005, the FIU received 10,148 disclosures, opened 3,051 new cases, and transmitted 686 cases to the public prosecutor, up from 664 cases transmitted in 2004. Nearly 75 percent of disclosures on files transmitted to the federal prosecutor were made by credit institutions. Foreign exchange offices and foreign counterpart units accounted for an additional 18 percent of the files transmitted, with notaries, casinos, and other entities also reporting.

Since the creation of CTIF-CFI in 1993, Belgian courts and tribunals have pronounced sentences in at least 837 of the 7,114 cases transmitted to the Federal Prosecutor (some of these convictions are still under appeal). From 1993-2005, the conviction rate was 12 percent. To date, Belgian courts have convicted 1,880 individuals for money laundering on the basis of cases forwarded by the FIU. These convictions have yielded combined total sentences of 2,819 years. Whereas five years is the maximum sentence for money laundering, the length of the sentence may increase if the financial crime is compounded by another type of crime such as drug trafficking. The cumulative fines levied for money laundering total approximately $91 million. Belgian authorities have confiscated more than $788 million connected with money laundering crimes. The majority of convictions related to money laundering are based upon disclosures made by the financial institutions and others to CTIF-CFI.

As with Belgium's FIU, the federal police are required to transmit suspected money laundering cases to the public prosecutor. In 2005 the federal police referred a total of 2,241 individuals to the public prosecutor for various crimes. More than 20 percent of these (450 individual cases) involved money laundering, fraud, and corruption. Other offenses were: narcotics (28 percent); aggravated theft in homes (13 percent); stolen vehicles (12 percent); armed robbery (12 percent); and trafficking in persons (10 percent). In 2005, the federal police referred 10 individuals to the public prosecutor for suspected links to terrorism. The FATF evaluation team found that the criminal prosecution authorities have the necessary power to carry out their functions; however, in some places or at some times, the prosecutors and police seem to lack resources to properly perform their AML/CFT duties.

The federal police enjoy good cross-border cooperation with other police and investigative services in neighboring countries. Belgium does not require an international treaty as a prerequisite to lending mutual assistance in criminal cases. 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 2005, Project Cash Watch, carried out under the auspices of the federal police in Belgium's international airports and other transit venues, netted seizures of more than $2.45

million. The federal police established a special bureau to combat VAT fraud shortly after 2001, when estimates of lost revenue topped $1.4 billion. In 2005, losses to the Belgian Treasury through VAT fraud were an estimated $230 million.

According to the FATF mutual evaluation report, Belgium has created a sophisticated and comprehensive confiscation and seizure regime, including the 2003 establishment of the Central Office for Seizure and Confiscation (COSC). Belgian law allows for civil as well as criminal forfeiture of assets. A law passed in July 2006 allows for the possibility, on a reciprocal basis, of the sharing of seized assets from serious crimes, including those related to narcotics, with affected countries. The COSC operates under the auspices of the Belgian Ministry of Justice and ensures that confiscations and seizures in Belgium are carried out smoothly and efficiently in accordance with Belgian law. In Belgium, confiscations and seizures can only be carried out by a judicial order.

Belgian authorities attempt to sell confiscated items such as cars, computers, and cell phones soon after confiscation in order to minimize the loss of the market value of the goods over time. If a suspect is later found innocent, he or she receives the cash equivalent of the item(s) sold, plus accrued interest. COSC has a commercial account for the deposit of confiscated funds. As of October 2006, the fund held more than $165 million. COSC also maintains safe deposit boxes for the storage of high value items, such as jewelry. Beginning in 2005, a verification program has been in place to check the legal records of suspects who have been found innocent and are about to have confiscated proceeds returned to them. If it is discovered that the person owes taxes or has overdue fines, for example, COSC can intervene and ensure that the Belgian government is paid before proceeds are returned. Through October 2006, this program has netted $1.65 million for federal coffers.

Seizures in Belgium can be direct or indirect. Direct seizures involve the seizure of items linked directly to a crime. Noncash items are held in the clerks' offices in one of Belgium's 27 judicial districts. Indirect seizures are "seizures by equivalence," usually of homes, cars, jewels, etc., not directly linked to the crime in question. Money from seizures and from the sale of seized goods is deposited in the Belgian Treasury. According the COSC, information concerning the value of seizures is not available publicly.

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 law transposed the Second European Money Laundering Directive and implemented eight of FATF's Special Recommendations. Article 140 of the Penal Code criminalizes participation in the activity of a terrorist group, and Article 141 specifically penalizes the provision of material resources, including financial assistance, to terrorist groups; the penalty is five to ten years' imprisonment.

Under Belgium's 1993 anti-money laundering and terrorist finance law (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 2005, CTIF-CFI temporarily froze assets in 29 cases, representing approximately $175 million.

Under the January 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.

In Belgium, the Ministry of Finance can administratively freeze assets of individuals and entities associated with al-Qaeda, the Taliban and Usama Bin Laden on the United Nations 1267 Sanctions Committee's consolidated list and/or those 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. Belgium is working on legislation to permit the administrative freeze of terrorist assets in the absence of a judicial order or UN or EU designation.

Belgium's FIU is active with its European colleagues in sharing information. CTIF-CFI has signed a memorandum of understanding with the United States that governs their collaborative work. CTIF-CFI was a founding member of the Egmont Group and headed the secretariat from 2005 to 2006. Belgium is a cooperative and reliable partner in law enforcement efforts. In 2005, Belgium collaborated with several countries on a criminal case resulting in nearly $20 million being frozen in accounts held in another European country.

Belgium is a party to the 1988 UN Drug Convention and the UN Convention for the Suppression of the Financing of Terrorism. 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. A mutual legal assistance treaty (MLAT) between Belgium and the United States has been in force since 2000, and an, an extradition treaty between the two countries has been operative since September 1997. The MLAT process is used for all information requests related to criminal cases, with careful consideration of privacy rights of parties involved. Bilateral instruments amending and supplementing these treaties, in implementation of the U.S.-EU Extradition and Mutual Legal Assistance Agreements, were signed with Belgium in December 2004.

Belgium's continuing work on implementing the FATF recommendations complements an already solid anti-money laundering regime and a clear official commitment to fighting against financial crimes, including the financing of terrorism. However, the Government of Belgium should continue to work through proposed legislation that pursues tougher and faster independent asset-freezing capability as well as the optimal disposition of seized assets. The Government of Belgium should continue its efforts to uncover, investigate, and prosecute illegal banking operations, including those connected to its diamond and real estate sectors, as well as the informal financial sector and nonbank financial institutions. Belgium should continue to enact reforms in the diamond market that will promote increased transparency. The GOB should strengthen adherence to reporting requirements by some nonfinancial entities in Belgium, such as lawyers and notaries. To be even more effective in its efforts, Belgium may need to devote more resources, including investigative personnel, to police, prosecutors and 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. Belizean officials suspect that money laundering occurs primarily within the country's offshore financial sector. 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.

Offshore banks, international business companies (IBCs) 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. Presently, there are eight licensed offshore banks, approximately 32,800 active registered IBCs, one licensed offshore insurance company, one mutual fund company, and 30 trust companies and agents operating in Belize. Local money exchange houses, which were suspected of money laundering, were closed effective July 11, 2005. There are also a number of undisclosed internet gaming sites operating from within the country. These gaming sites are unregulated at this time. Currently there are no offshore casinos operating from within Belize. Government of Belize (GOB) 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.

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. 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. GOB legislation 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.

There is one free trade zone presently operating in Belize, at the border with southern Mexico. There are also designated free trade zones in Punta Gorda, Belize City and Benque Viejo, 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. 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, in collaboration with the Customs Department and the Central Bank of Belize, monitors the operations of CFZ business activities. There is no indication that the CFZ is presently being used in trade-based money laundering schemes or by financiers of terrorism.

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.

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. Other legislation to combat money laundering include the Money Laundering Prevention Guidance Notes; the Financial Intelligence Unit Act, 2002; the Misuse of Drugs Act; The International Financial Services Practitioners Regulations (Code of Conduct), 2001 (IFSCR); Money Laundering Prevention Regulations, 1998 (MLPR); and the Offshore Banking Act, 2000, renamed the International Banking Act, 2002 (IBA). In 2006, there were no major money laundering cases to report, and the effectiveness of the anti-money laundering regime in Belize remains unclear.

The Central Bank of Belize supervises and examines financial institutions for compliance with anti-money laundering and counterterrorist financing 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 legislation and must adhere to the same anti-money laundering and counterterrorist financing requirements. To legally operate from within Belize, all offshore banks must be licensed by the Central Bank and be registered as 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 Central Bank issued Supporting Regulations and Guidance Notes in 1998. Licensed banks and financial institutions are required to establish due diligence ("know-your-customer") provisions, monitor their customers' activities and report any suspicious transactions to the financial intelligence unit (FIU). Belize law obligates banks and other financial institutions to maintain business transactions records for at least five years when the transactions are complex, unusual or large. Money laundering controls are also applicable to nonbank financial institutions, such as exchange houses, insurance companies, lawyers, accountants and the securities sector, which are regulated by the International Financial Services Commission. Financial institution employees are exempt 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.

The reporting of all cross-border currency movement is mandatory. All individuals entering or departing Belize with more than $10,000 in cash or negotiable instruments are required to file a declaration with the authorities at Customs, the Central Bank and the FIU.

The FIU of Belize is an independent agency presently housed at the Central Bank. Current laws do not provide for the funding of the FIU, and the FIU has to apply to the Ministry of Finance for funds. The funding allocated to the FIU for fiscal year 2006 was approximately $200,000. Due to financial constraints, the FIU is not adequately staffed and existing personnel lack sufficient training and experience. On November 5, 2005 the director of the FIU resigned, leaving the FIU with only four employees; the new FIU director did not begin until July 2006.

As of October 15, 2006, the FIU had received 34 suspicious transaction reports (STRs) from obligated entities. Of the 34 STRs filed, 13 became the subject of investigations. The Director of the Public Prosecutions Office and the Belizean Police Department are responsible for investigating all crimes. However, the FIU also has administrative, prosecutorial and investigative responsibilities for financial crimes, such as money laundering and terrorist financing. Although the FIU has access to records and databanks of other GOB 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. On several occasions, the FIU has cooperated with the United States' FIU and other U.S. law enforcement agencies.

Belize criminalized terrorist financing via amendments to its anti-money laundering legislation, The Money Laundering (Prevention) (Amendment) Act, 2002. GOB authorities have circulated 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 to all financial institutions in Belize. There are no indications that charitable or nonprofit 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 nonprofit entities from aiding in the financing of terrorist activities.

Alternative remittance systems are illegal in Belize. However, Belizean authorities acknowledge the existence and use of indigenous alternative remittance systems that bypass, in whole or in part,

financial institutions. Therefore, Belizean authorities monitor such activities at the borders with Mexico and Guatemala.

Belizean law makes no distinctions between civil and criminal forfeitures. All forfeitures resulting from money laundering or terrorist financing 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, and the Ministry of Finance can also confiscate frozen assets. With prior court approval, Belizean authorities have the power to identify, freeze and seize assets related to terrorist financing or money laundering. Currently, the GOB's legislation does not specify the length of time assets can be frozen. There are no limitations to the kinds of property that may be seized, including any property—tangible or intangible—which may be related to a crime or is shown to be from the proceeds of a crime. This includes legitimate businesses. However, Belizean law enforcement lacks the resources necessary to trace and seize assets.

The Belize Police Department reported that during 2006, the only assets forfeited or seized were firearms and ammunition, on which no value is placed. Assets forfeited and/or seized in 2005 totaled approximately $120,000. GOB 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. Currently, the GOB is not engaged in any bilateral or multilateral negotiations with other governments to enhance asset tracing and seizure. 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 with the United States, which provides for mutual legal assistance in criminal matters. Amendments to the MLPA preclude the necessity of a Mutual Legal Assistance Treaty for exchanging information or providing judicial and legal assistance to authorities of other jurisdictions in matters pertaining to money laundering and other financial crimes. 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. The GOB has signed, but not yet ratified, the Inter-American Convention against Terrorism, and has neither signed nor ratified the UN Convention against Corruption. Belize is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Working Group to Control Money Laundering and the Caribbean Financial Action Task Force. Its FIU became a member of the Egmont Group of financial intelligence units in 2004.

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

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 nonbank 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 formal financial sector consists of approximately 13 commercial banks, six private financial funds, nine mutual funds, 23 savings and credit cooperatives, 14 insurance companies and one stock exchange, all of which are subject to the same anti-money laundering controls. The Bolivian system is highly dollarized, with close to 90 percent of deposits and loans denominated in dollars rather than bolivianos, the local currency. Free trade zones exist in the cities of El Alto, Cochabamba, Santa Cruz, Oruro, Puerto Aguirre and Desaguadero.

Several entities that move money in Bolivia remain unregulated. Hotels, currency exchange houses, illicit casinos, cash transporters, and wire transfer businesses can be used to transfer money freely into and out of Bolivia but are not subject to anti-money laundering controls. Informal exchange businesses, particularly in the department of Santa Cruz, are also used to transmit money in order to avoid law enforcement scrutiny.

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 (FIU), 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 of July 31, 1997.

Although Law 1768 established the UIF as an administrative financial intelligence unit in 1997, the UIF did not become operational until July 1999. As Bolivia's FIU, the UIF is responsible for collecting and analyzing data on suspected money laundering and other financial crimes. Under Decree 24771, obligated entities-which include only 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 designated threshold, nor is there a requirement that persons entering or leaving the country declare the transportation of currency over a designated threshold, as is commonplace in many countries' anti-money laundering regimes.

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. The Special Group for Investigation of Economic Financial Affairs (GIAEF), created in 2002 within Bolivia's Special Counter-Narcotics Force (FELCN), is responsible for investigating 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 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. Given the size of Bolivia's financial sector, compliance with reporting requirements is extremely low, as the UIF receives, on average, less than 50 suspicious transaction reports per year. Seventy percent of those reports are filed by a single bank.

Corruption is a serious issue in Bolivia. According to estimates by the U.S. Agency for International Development (USAID), corruption costs Bolivians approximately $115 million per year, equal to half of the GOB's budget deficit. 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.

In order to further combat corruption, the GOB promulgated Supreme Decree 28695, the Organizational Structure for the Fight against Corruption and Illicit Enrichment, on April 26, 2006. Among a number of other provisions, the decree provides for the creation of a "Financial and Property Intelligence Unit," which would replace the UIF. Decree 28695 also repealed Decree 24771, which gave the UIF its authority. However, given that the repeal of Decree 24771 would eliminate the UIF before its replacement was operational, the GOB then passed Decree 28713 on May 13, 2006, reinstating the UIF's functions and duties until January 2007 and placing the UIF under the Ministry of Finance. On November 29, 2006, the GOB passed Decree 28956, eliminating the portion of Decree 28695 that had repealed Decree 24771 and allowing the UIF to continue to operate until the Financial and Property Intelligence Unit becomes a functioning entity.

The Constitution Commission of the Bolivian Chamber of Deputies has drafted a new anti-money laundering law that would establish the Financial and Property Intelligence Unit as Bolivia's sole financial intelligence unit. However, the law does not include provisions to bring Bolivia's anti-money laundering regime into greater compliance with international standards, in spite of suggestions and input from the Financial Action Task Force for South America (GAFISUD), the International Monetary Fund (IMF), the UIF, and the Government of the United States. The draft was presented to Chamber of Deputies in early December 2006, but is not yet under consideration by the Chamber.

Although the draft law in effect provides a mission for the Financial and Property Intelligence Unit, there are concerns regarding the functions and authorities of the new entity, and the current operations of the UIF. As a result of the new decree and the plans to establish Financial and Property Intelligence Unit, the UIF has undergone two changes in leadership since April 2006 and many staff members have left, bringing the number of personnel to only five. Limitations in its reach, a lack of resources, and weaknesses in its basic legal and regulatory framework have traditionally hampered the UIF's effectiveness as a financial intelligence unit. There is no indication that the establishment of the Financial and Property Intelligence Unit will resolve these problems and allow for a more effective FIU.

There are also concerns that the new legislation will not improve the GOB's overall anti-money laundering regime, which is undermined by the lack of a legal and bureaucratic framework 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 involving money laundering.

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.

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, but not ratified, 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, the bill has not yet been presented to Congress. There have been no cases of terrorist financing to date.

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 on Money Laundering and GAFISUD. Bolivia 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 Corruption and the UN Convention against Transnational Organized Crime. The GOB and the United States signed an extradition treaty in June 1995, which entered into force in November 1996.

While the Government of Bolivia's efforts to combat corruption are necessary, the GOB should take steps to ensure that any changes in its anticorruption legislation will strengthen its anti-money laundering regime. The GOB should also improve its current money laundering legislation so that it conforms to the standards of the Financial Action Task Force and GAFISUD by making money laundering an autonomous offense without requiring a connection to other illicit activities; criminalizing terrorist financing; allowing the blocking of terrorist assets; and, requiring currently unregulated sectors to be subject to anti-money laundering and counterterrorist financing controls. Bolivia should ensure that, with the creation of a new financial intelligence unit, the unit has sufficient staff and resources, as well as the authority to receive suspicious transaction reports on activities indicative of terrorist financing and reports from nonbank financial institutions. Bolivia should also continue to strengthen the relationships and cooperation between all government entities involved in the fight against money laundering and other financial crimes in order to create a more effective regime capable of preventing and combating money laundering and terrorist financing.

Bosnia and Herzegovina

Bosnia and Herzegovina (BiH) has a cash-based economy and is not an international, regional, or offshore financial center. International observers believe the laundering of illicit proceeds from criminal activity including the proceeds from smuggling, corruption, and tax evasion is widespread. Due to its porous borders and weak enforcement capabilities, BiH is a significant market and transit point for illegal commodities including cigarettes, narcotics, firearms, counterfeit goods, lumber and fuel oils. BiH authorities have had some recent success in clamping down on money laundering through the formal banking system, which has resulted in suspect nongovernmental organizations (NGOs) increasing their use of direct cash transfers from abroad as a source of funding.

There are multiple jurisdictional levels in Bosnia and Herzegovina, including the State, the two entities (the Federation of Bosnia and Herzegovina and the Republika Srpska), and Brcko District. The Federation is further divided into ten cantons. New criminal and criminal procedure codes from the State, the two entities and Brcko District were enacted and harmonized in 2003, although the jurisdictions maintain their own enforcement bodies. Although state-level institutions are becoming more firmly grounded and are gaining increased authority, there remains a fair amount of confusion regarding jurisdictional matters between the entities and state-level institutions. Unless otherwise specified, relevant laws and institutions are at the state level.

Money laundering of all kinds is a criminal offense in all state and entity criminal codes. The new criminal procedure and criminal codes enacted in 2003 included tougher provisions against money laundering. At the state level, the Law on the Prevention of Money Laundering came into force in December 2004. The law determines the measures and responsibilities for detecting, preventing, and investigating money laundering and terrorist financing. The law also prescribes measures and responsibilities for international cooperation and establishes a financial intelligence unit (FIU) within the State Investigative and Protection Agency (SIPA). The law requires banks to submit reports on suspicious financial transactions to the state-level FIU. The Prosecutor's office must also share data on money laundering and terrorist financing offenses with the FIU.

The Law on the Prevention of Money Laundering applies to any person who "accepts, exchanges, keeps, disposes of, uses in commercial or other activity, otherwise conceals or tries to conceal money or property he knows was acquired through perpetration of criminal offence, 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 money laundering convictions covering amounts above the equivalent of $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. SIPA and the Federation and Republika Srpska (RS) police bodies are responsible for the investigation of financial crimes. BiH has not enacted bank secrecy laws which prevent the disclosure of client and ownership information to bank supervisors and law enforcement authorities.

Banks and other financial institutions are required to know, record, and report the identity of customers engaging in significant transactions, including currency transactions above the equivalent of $18,000. Obliged entities are also required to maintain records for twelve years in order to respond to law enforcement requests. The money laundering law applies to all individuals and several nonbank financial institutions including, but not limited to, post offices, investment and mutual pension companies, stock exchanges and stock exchange agencies, insurance companies, casinos, currency exchange offices and intermediaries such as lawyers and accountants. There is, however, no formal supervision mechanism in place for nonbank financial institutions and intermediaries. It is mandatory for all banks and financial institutions to report suspicious transactions, and there is no mandated reporting threshold for reporting suspicious transactions. Banking authorities have supervision responsibility for all covered sectors. However, reportedly there is little supervision of nonbank financial institutions and intermediaries. The law also requires that customs administration authorities report cross-border transportation of cash and securities in excess of $6,000 to the FIU. The Indirect Taxation Authority (ITA), which has responsibility for customs, suffers, like other BiH state-level agencies, from a lack of resources and sufficiently trained personnel.

The banking community cooperates with law enforcement efforts to trace funds and freeze accounts. Bosnian law protects reporting individuals with respect to law enforcement cooperation. Although there is no state-level banking supervision agency, entity level banking supervision agencies oversee and examine financial institutions for compliance with anti-money laundering and counter terrorist financing laws and regulations.

The Financial Intelligence Department (FID), Bosnia-Herzegovina's FIU, is a hybrid body, performing analytical duties with some limited criminal investigative responsibilities. The FID receives, collects, records, analyzes, and forwards information related to money laundering and terrorist financing to the State Prosecutor. It also provides expert support to the Prosecutor regarding financial activities, and is responsible for international cooperation on money laundering issues. The FID has access to the records of other government entities, and formal mechanisms for inter-agency information sharing are in place. The FID is empowered to freeze accounts for five days; when its preliminary analysis is complete, it may forward the case to the Prosecutor. At that point, the freeze on the accounts may be extended. The FIU reports that it froze approximately $1,468,604 in the first nine months of 2006.

The September 2006 International Monetary Fund's Financial System Stability Assessment report praised Bosnia-Herzegovina for the progress made since the MONEYVAL 2005 mutual evaluation report. It cited in particular "the development of an effective state-level FIU." However, according to a European Commission report, fewer than half of FID's planned positions have been filled. There are also reported problems with information-sharing, coordination, and communication, as well as jurisdictional issues between the Financial Police and other State agencies.

For the first nine months of 2006, FID received 145,071 currency reports from banks and other financial institutions. Of these, 14 were identified as suspicious and nine were investigated. Of these nine investigations, two cases were dropped, four have been sent to the prosecutor's office, and three are still under investigation. Since BiH established its anti-money laundering regime, there have been nineteen convictions for money laundering. However, because of the appeals process, only one conviction has been finalized.

BiH has no asset forfeiture law, with the exception of the Persons Indicted for War Crimes (PIFWC) support laws which allow for the seizure of PIFWC assets or assets of those providing material support to them. Articles 110 and 111 of the BiH Criminal Code (along with similar laws in the harmonized entity and Brcko Criminal Codes) are the only legal provisions that might be used in place of an actual asset forfeiture law. These provisions authorize the "confiscation of material gain" (or a sum of money equivalent to the material gain if confiscation is not feasible) from illegal activity. The tools used in committing those crimes are not subject to seizure. Confiscation can only be done as part of a verdict in a criminal case, and is administered by the courts, not law enforcement agencies. The courts decide whether the articles will be "sold under the provisions applicable to judicial enforcement procedure, turned over to the criminology museum or some other institution, or destroyed. The proceeds obtained from sale of such articles shall be credited to the budget of Bosnia and Herzegovina." Prosecutors 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. 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 forfeiture. There are no laws for sharing seized assets with other governments. BiH authorities have the authority to identify, freeze, seize, and forfeit terrorist-finance-related and other assets. The banking agencies (Federation and RS Banking Agencies) in particular have the capability to freeze assets without undue delay.

Terrorist financing was criminalized in article 202 of the criminal procedure code. BiH is a party to the 1999 International Convention for the Suppression of the Financing of Terrorism. The entity banking agencies are cognizant of the requirements to sanction individuals and entities listed by the UNSCR 1267 Sanctions Committee's consolidated list. However, the state authorities do not circulate this list to entity authorities on a regular basis. In July 2006, BiH adopted a "Strategy against Terrorism," but SIPA needs to be strengthened to meet its designated responsibilities in the Strategy.

In 2006, after a cooperative investigation between BiH and law enforcement authorities in several European Union countries, BiH authorities initiated a prosecution at the Court of Bosnia and Herzegovina against five people suspected of terrorist crimes. And in 2004, the government disrupted the operations of Al Furqan (aka Sirat, Istikamet), Al Haramain & Al Masjed Al Aqsa Charity Foundation, and Taibah International, organizations listed by the UNSCR 1267 Committee as having direct links with al-Qaida. Authorities continue to investigate other organizations and individuals for links to terrorist financing.

Nonbank financial transfers are reportedly very difficult for BiH law enforcement and customs officials to deal with due to a lack of reporting as well as a lack of understanding of indigenous methodologies, many of which are found in the underground economy and are enabled by smuggling and the misuse of trade. Currently there are six Free Trade Zones in BiH. However, only three of the zones are active, with production based mainly on automobiles and textiles.

Bosnia and Herzegovina has no Mutual Legal Assistance Treaty with the U.S., although an extradition treaty signed by the Kingdom of Serbia in 1902 has carried over into BiH; some financial crimes are covered, but not contemporary forms of money laundering. There is no formal bilateral agreement between the United States and BiH regarding the exchange of records in connection with narcotics investigations and proceedings. Authorities have made good faith efforts to exchange information informally with officials from the United States. BiH is a party to the 1988 UN Drug Convention (by way of succession from the former Yugoslavia), the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the UN International Convention for the Suppression of the Financing of Terrorism. Unfortunately, on many occasions, BiH has not passed implementing legislation for the international conventions to which it is a signatory.

The Government of Bosnia and Herzegovina (GOBH) should continue to strengthen institutions with responsibilities for money laundering prevention, particularly those at the state level. Due to a lack of resources and bureaucratic politics, SIPA and the FIU, like many state institutions, remain under-funded and under-resourced. Efforts should be made to increase funding for its anti-money laundering and counterterrorist finance programs and enhance cooperation between concerned departments and agencies. Prosecutors, financial investigators, and tax administrators have received training on tax evasion, money laundering and other financial crimes. However, significant additional training may be necessary to ensure that they understand diverse methodologies and aggressively pursue investigations. BiH law enforcement and customs authorities should take additional steps to control the integrity of the border and limit smuggling. Efforts should be made to understand the illicit markets and their role in trade-based money laundering and alternative remittance systems. BiH should study the formation of centralized regulatory and law enforcement authorities. Specific steps should be taken to combat corruption at all levels of commerce and government.

Brazil

Brazil is the world's fifth largest country in both size and population, and its economy is the tenth largest in the world. Due to its size and significant economy, Brazil is considered a regional financial center, although it is not an offshore financial center. Brazil is also 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 to domestic crime, especially drug-trafficking, corruption, organized crime, and trade in contraband, all of which generate funds that may be laundered through the banking system, real estate investment, financial asset markets, luxury goods or informal financial networks. 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 2006 the Government of Brazil (GOB) continued investigations into a series of corruption scandals of unusual scope that emerged in 2005. Parallel investigations by Brazilian Congressional committees and law enforcement authorities revealed illicit financing by several political parties of their 2002 presidential campaigns and a related scheme involving vote-buying in Congress by elements within the ruling party and the executive branch, financed by kickbacks on contracts. Two medium-sized regional banks served as conduits for illicit payments, making use of a publicity firm's bank accounts, while some payments were made into bank accounts overseas. Fourteen senators and federal deputies either resigned or were expelled from office, including the President's former Chief of Staff, due to their involvement in the scheme. Prosecutors have brought criminal charges in the case as well, which are now pending before the Supreme Court. A separate corruption case implicating multiple members of Congress involved inflated billing for ambulances purchased with public funds. Brazil's anti-money laundering mechanisms and institutions have played useful roles in the investigation of these cases.

A primary source of criminal activity and contraband is the Triborder Area (TBA) shared by Argentina, Brazil, and Paraguay. Brazilian authorities have expressed particular concern over the trafficking in arms and drugs in the TBA. Brazilian authorities note that the proceeds of domestic drug trafficking and organized crime feed a regional arms trade, operating in the TBA. In addition, a wide variety of counterfeit goods, including cigarettes, CDs, DVDs, and computer software, are smuggled across the border from Paraguay into Brazil; a significant portion of these counterfeit goods originate in Asia. The U.S. government believes the TBA to be a source of terrorist financing, although the GOB maintains that it has not seen any evidence of such. In 2006 Brazilian customs authorities continued a campaign launched in 2005 to combat contraband in the TBA given the significant loss of tax revenues that result from the contraband trade (estimated at $1.2 billion per year). The campaign has featured enhanced controls at border crossing point and frequent 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 $4,600) 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, establishes 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 Brazil's financial intelligence unit, the Conselho de Controle de Atividades Financeiras (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.

Since 1999, the COAF has 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.

In addition to filing SARs, banks are also required to report cash transactions exceeding 100,000 reais (approximately $48,000) to the Central Bank. 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. COAF Resolution 14 of October 23, 2006, further extended these anti-money laundering requirements to the real estate sector. Separately, the insurance regulator, SUSEP, clarified its reporting requirements for insurance companies and brokers in Circular 327 from May 29, 2006, which requires these entities to have an anti-money laundering program and report large insurance policy purchases, settlements or otherwise suspicious transactions to both SUSEP and COAF.

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 gained 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. In 2006, the COAF received roughly 13,000 cash transaction reports and 2000 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 institutionalized its national strategy for combating money laundering, holding its fourth annual high-level planning and evaluation session in December 2006. 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. Given the GOB's emphasis on and need for fighting corruption, the main goal for 2006 was 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 has reported substantial growth in the number of money laundering investigations, trials and convictions since 2003. The annual number of investigations grew from 198 in 2003 to 310 in 2004, 449 in 2005, and 625 in the first three quarters of 2006. These investigations led to 26 trials in 2003, 74 in 2004, 75 in 2005, and 41 in the first three quarters of 2006, while convictions ranged from 172 in 2003 to 87 in 2004, 183 in 2005 and 866 in 2006 to date. 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). The GOB credits the creation of specialized money laundering courts, founded in 2003, for the increasing number of successful money laundering prosecutions. 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 aimed to build on the success of the specialized courts by creating complementary specialized federal police financial crimes units in the same jurisdictions. Another reason for the increased prosecutions was the large number of money laundering cases from the Banestado bank scandal of the late 1990's, which began to move to trial during the 2004-2005 period.

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.

In 2005, the GOB drafted a bill to update its anti-money laundering legislation. If passed, this bill, which has not yet been presented to Congress, 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 such as the Central Bank. The COAF would also be able to request additional information directly from the reporting entities.

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 planned 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.

Brazil has drafted, but not yet presented to Congress, legislation overhauling Brazil's antiterrorism legislation, including specific provisions criminalizing the financing of terrorism. Passage of this legislation would address a fundamental weakness in Brazil's legislative regime to counter money laundering and terrorism finance. 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 nonprofit 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 nonprofit status, including money laundering. These regulations would apply to nongovernmental organizations, churches and charitable organizations.

The GOB has generally 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 Brazil. In November 2003, the GOB extradited Assad Ahmad Barakat, designated by the United States under E.O. 13224 as a Specially Designated Global Terrorist, to Paraguay on charges of tax evasion; he was convicted in May 2004 for tax evasion (Paraguay has not criminalized terrorist financing), and sentenced to six and one-half years in prison.

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

Brazil is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the UN International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention on Terrorism. Brazil is a member of the Financial Action Task Force (FATF), was a founding member of the Financial Action Task Force Against Money Laundering in South America (GAFISUD), and held 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 U.S. Immigration and Customs Enforcement in 2006 established a trade transparency unit (TTU) to detect money laundering via trade transactions. The GOB also participates in the "3 Plus 1" Security Group (formerly the 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. 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). The BVI remains vulnerable to money laundering, primarily due to its financial services industry. The BVI has approximately 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 reportedly 61,000 international business companies (IBCs)—an extraordinary diminution of some 483,000 IBCs reportedly registered in the BVI in 2004.

The Financial Services Commission (FSC) is the independent regulatory authority responsible for the licensing and supervision of regulated entities, which include banking and fiduciary businesses, investment businesses, insolvency services, insurance companies, and company management and registration businesses. Money remitters, however, are not subject to licensing or supervision. The FSC is also responsible for on-site inspections of these entities. The FSC cooperates with its foreign counterparts and law enforcement agencies. In 2000, the Information Assistance (Financial Services) Act (IAFSA) was enacted to increase the scope of cooperation between the BVI's regulators and regulators from other countries.

According to the International Business Companies Act of 1984, IBCs registered in the BVI 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). All IBCs must be registered in the BVI by a registered agent, and the IBC or the registered agent must maintain an office in the BVI. The BVI has approximately 90 registered agents that are licensed by the 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. Although procedures exist for the freezing and confiscation of assets linked to criminal activity, including money laundering and terrorist financing, the procedures for the forfeiture of assets that are not directly linked to narcotics-related crimes are unclear.

The Proceeds of Criminal Conduct Act also created a financial intelligence unit (FIU). The Financial Investigation Agency Act 2003 reorganized and renamed the FIU, now called the Financial Investigation Agency (FIA). The FIA, generally referred to as the Reporting Authority, is responsible for the collection, analysis, and dissemination of financial information.

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 suspicious transactions and report them to the FIA. Obligated entities are protected from liability for reporting 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 United Kingdom's Terrorism (United Nations Measures) (Overseas Territories) Order 2001 and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002 extend to the BVI. The Afghanistan (United Nations Sanctions) (Overseas Territories) Order 2001 and the Al-Qaida and Taliban (United Nations Measures) (Overseas Territories) Order 2002 also apply to the BVI. However, the BVI has not specifically criminalized the financing of terrorism.

The BVI is a member of the Caribbean Financial Action Task Force (CFATF). The 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. The BVI should also extend the provisions of its anti-money laundering and counterterrorist financing to a wider range of entities, including money remitters. The BVI should establish the financing of terrorism as an autonomous offense.

Bulgaria

Bulgaria is neither considered an important regional financial center nor an offshore financial center. Its significance in terms of money laundering stems from its geographical position, its well-developed financial sector relative to other Balkan countries, and its 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 is 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 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 duty free shops used to violate customs and tax regimes. The duty free shops may be used to facilitate other crimes, including financial crimes. Credible allegations have linked many duty free shops in Bulgaria to organized crime interests involved in fuel smuggling, 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 procedures for identifying unlawful activity 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.

Article 253 of the Bulgarian Penal Code criminalizes money laundering. The 2006 amendments increase penalties (including in cases of conspiracy and abuse of office), clarify that predicate crimes committed outside Bulgaria can support a money laundering charge brought in Bulgaria, and allow prosecution on money laundering charges without first obtaining a conviction for the predicate crime. Article 253 criminalizes money laundering related to all crimes; as such, drug-trafficking is but one of many recognized predicate offenses

The Law on Measures against Money Laundering (LMML), adopted in 1998 and amended most recently in 2006, is the legislative backbone of Bulgaria's anti-money laundering regime. 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. While the financial intelligence unit (FIU) is not bound by the secrecy provisions, they apply to all other government institutions and are often cited as an impediment to law enforcement functions. In an effort to lessen the impact of secrecy laws on law enforcement functions, in 2006 the GOB issued amendments to both the LMML and the Law on Credit Institutions. The amendments to the Law on Credit Institutions facilitated the investigation and prosecution of financial crimes by giving the Prosecutor General the right to request financial information from banks without a court order in cases involving money laundering and organized crime.

Banks and the 29 other reporting entities under the LMML are required to apply "know your customer" (KYC) standards. Since 2003, all reporting entities are required to ask for the source of funds in any transaction greater than $19,000 or foreign exchange transactions greater than $6,500. Reporting entities are also required to notify the FIA of any cash payment greater $19,000.

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 Financial Intelligence Agency (FIA) serves as Bulgaria's FIU and is located within the Ministry of Finance. The LMML guarantees the independence of the FIA director, allows the agency to perform onsite compliance inspections, and authorizes it to obtain information without a court order, share all information with law enforcement, and receive reports of suspected terrorism financing. The agency has a supervisor within the MOF who oversees the activities of the FIA. However, the supervisor is prohibited by law from issuing operational commands. The FIA remains handicapped technologically, but it is working on improving its databases to improve analytical efficiency.

The FIA is an administrative unit and does not participate in criminal investigations. In 2006, the Ministry of the Interior (MOI), the Prosecutor's Office, and the FIA established new procedures for closer cooperation when following leads contained in a suspicious transaction report (STR). The FIA forwards reports to the Prosecutor, and sends to the MOI a copy of each. The MOI is subsequently required to produce a report on the enforcement potential of the case within 30 days of receipt.

Between January and November 2006, the FIA received 310 STRs, on transactions totaling $175 million, and 134,241 currency transaction reports (CTRs). On the basis of the forwarded reports, 276 cases were opened, 74 cases were referred to the Supreme Prosecutor's Office of Cassation, and 207 cases were referred to the Ministry of Interior. The FIA forwarded 32 reports to supervisory authorities for administrative action.

A May 2006 report from the European Union (EU) regarding the status of Bulgaria's application for admission to the EU called Bulgaria's enforcement of anti-money laundering provisions an area of "serious concern," requiring "urgent action". This issue was one of several, resulting in a potential delay of entry date into the EU. In response, Bulgaria's Parliament tightened the LMML with further amendments. The 2006 LMML amendments expanded the definition of money laundering and the list of reporting entities; allowed FIA to obtain bank records without a court order; outlawed anonymous bank accounts; expanded the definition of "currency"; and required the disclosure of source for currency exported from the country. Overall, these amendments are expected to strengthen the investigative capabilities of both the FIA and law enforcement when dealing with money laundering cases. Experts view this legislation as comprehensive and in line with international standards. All financial sectors are considered susceptible to money laundering and subject to anti-money laundering regulations. Under the LMML, 30 categories of entities, including lawyers, real estate agents, auctioneers, tax consultants, and security exchange operators, are required to file suspicious transactions reports. To date, only the banking sector has substantially complied with the law's filing

requirement. Lower rates of reporting compliance by exchange bureaus, casinos, and other nonbank 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 nonbank financial sector.

Although money laundering has been pursued in court cases, there had not been a conviction until recently. In October 2006, the courts rendered the country's first two convictions for money laundering. On October 9, the Ruse District Court sentenced a defendant to 11 months in prison and three years of probation after he admitted to receiving a 350,000 Euro (approximately $464,000) bank transfer in 2004. The FIA initiated the investigation. In another case, the Varna District Court sentenced a defendant to an eighteen-month imprisonment and a fine of 4,000 BGL (approximately $2,600) for the predicate crime of drug trafficking and distribution

There are few, if any, indications of terrorist financing connected with Bulgaria. Article 108a of the Penal Code criminalizes terrorism and terrorist financing. Article 253 of the Criminal Code qualifies terrorist acts and financing as predicate crimes under the "all crimes" approach to money laundering. In February 2003, the GOB enacted the Law on Measures Against Terrorist Financing (LMATF), which links counterterrorism measures with financial intelligence and compels all covered entities to report a suspicion of terrorism financing or pay a penalty of approximately $15,000. The law is consistent with Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing and authorizes the FIA to use its resources and financial intelligence to combat terrorism financing along with money laundering.

Under the LMATF, the GOB may freeze the assets of a suspected terrorist for 45 days. 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 FIA and the Bulgarian National Bank circulate the names of suspected terrorists and terrorist organizations, as found on the UNSCR 1267 Sanctions Committee's consolidated list, as well as the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224, and those designated by the relevant EU 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 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 nonprofit legal status is occasionally used to conceal money laundering. In 2006, the GOB somewhat strengthened its nonbank financial institution oversight by instituting compliance checks on casinos and exchange offices. Between January and October 2006, the FIA inspected 23 casinos and 548 exchange offices, imposing fines in 15 cases.

The Bulgarian Penal Code provides legal mechanisms for forfeiting assets (including substitute assets in money laundering cases) and instrumentalities. Both the money laundering and the terrorist financing laws 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 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.

The United States does not have a mutual legal assistance treaty with Bulgaria. However, the 2005 ratification of the UN Convention Against Transnational Organized Crime by the U.S. established an MLAT-type relationship between the two countries, and the U.S.-EU Agreement on Mutual Legal Assistance, once ratified, will lay the basis for a more comprehensive MLAT relationship. Currently, the FIA has bilateral memoranda of understanding (MOU) regarding information exchange relating to money laundering with 29 countries. Negotiations with three 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 October 2006, the FIA sent 285 requests for information to foreign FIUs and received 65 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; the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the UN Convention against Transnational Organized Crime; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention against Corruption.

In 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 enacted legislative changes consistent with international anti-money laundering standards, lax enforcement remains problematic. The GOB must take steps to improve and tighten its regulatory and reporting regime, particularly with regard to nonbank sectors. The GOB should improve the consistency of its customs reporting enforcement and should also establish procedures to identify the origin of funds used to acquire banks and businesses during privatization. The GOB needs to provide sufficient resources to the Financial Intelligence Agency so that the agency can incorporate technological improvements. The FIA should also continue to improve inter-agency cooperation in order to ensure effective implementation of Bulgaria's anti-money laundering regime and to improve prosecutorial effectiveness in money laundering cases.

Burma

Burma, a major drug-producing country, has taken steps to strengthen its anti-money laundering regulatory regime in 2005 and 2006. The country's economy remains dominated by state-owned entities, including the military. Agriculture and extractive industries, including natural gas, mining, logging and fishing provide the major portion of national income, with heavy industry and manufacturing playing minor roles. The steps Burma has taken over the past two years have reduced vulnerability to drug money laundering in the banking sector. However, with an underdeveloped financial sector and large volume of informal trade, Burma remains a country where there is significant risk of drug money being funneled into commercial enterprises and infrastructure

investment. The government has addressed most key areas of concern identified by the international community by implementing some anti-money laundering measures, and in October 2006, the Financial Action Task Force (FATF) removed Burma from the FATF list of Non-Cooperative Countries and Territories (NCCT).

The United States maintains other sanctions on trade, investment and financial transactions with Burma under Executive Order 13047 (May 1997), Executive Order 13310 (July 2003); the Narcotics Control Trade Act, the Foreign Assistance Act, the International Financial Institutions Act, the Export-Import Bank Act, the Export Administration Act, the Customs and Trade Act, the Tariff Act (19 USC 1307), and the 2003 Burmese Freedom and Democracy Act (P.L. 108-61).

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 fairly high level of 100 million kyat (approximately $75,000). Burma adopted a "Mutual Assistance in Criminal Matters Law" in 2004, added fraud to the list of predicate offenses, and established legal penalties for leaking information about suspicious transaction reports. The GOB's 2004 anti-money laundering measures amended regulations instituted in 2003 that set out 11 predicate offenses, including narcotics activities, human trafficking, arms trafficking, cyber-crime, and "offenses committed by acts of terrorism," among others. The 2003 regulations, expanded in 2006, require banks, customs officials and the legal and real estate sectors to file suspicious transaction reports (STRs) and impose severe penalties for noncompliance.

The GOB established a Department Against Transnational Crime in 2004. Its mandate includes 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 produced regular progress reports in 2005 and 2006. In 2005, the government also increased the size of the FIU to 11 permanent members, plus 20 support staff. In August 2005, the Central Bank of Myanmar issued guidelines for on-site bank inspections and required reports that review banks' compliance with AML legislation. Since then, the Central Bank has sent teams to instruct bank staff on the new guidelines and to inspect banking operations for compliance.

The United States maintains the separate countermeasures it adopted against Burma in 2004, which found the jurisdiction of Burma and two private Burmese banks, Myanmar Mayflower Bank and Asia Wealth Bank, to be "of primary money laundering concern." These countermeasures prohibited U.S. banks 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. These rules were issued by the Financial Crimes Enforcement Network within the Treasury Department, pursuant to Section 311 of the 2001 USA PATRIOT Act.

Myanmar Mayflower and Asia Wealth Bank had been linked directly to narcotics trafficking organizations in Southeast Asia. In March 2005, following GOB investigations, the Central Bank of Myanmar revoked the operating licenses of Myanmar Mayflower Bank and Asia Wealth Bank, citing infractions of the Financial Institutions of Myanmar Law. The two banks no longer exist. In August 2005, the Government of Burma also revoked the license of Myanmar Universal Bank (MUB), and convicted the bank's chairman under both the Narcotics and Psychotropic Substances Law, and the Control of Money Laundering Law. Under the money laundering charge, the court sentenced him to one 10-year and one unlimited term in prison and seized his and his bank's assets.

Burma also remains under a separate 2002 U.S. Treasury Department advisory stating that U.S. financial institutions should give enhanced scrutiny to all financial transactions related to Burma. The Section 311 rules complement the 2003 Burmese Freedom and Democracy Act (renewed in July 2006) and Executive Order 13310 (July 2003), which impose additional economic sanctions on Burma

following the regime's May 2003 attack on a peaceful convoy of the country's pro-democracy opposition led by Nobel laureate Aung San Suu Kyi. The sanctions prohibit the import of most Burmese-produced goods into the United States, ban the provision of financial services to Burma by any U.S. persons, freeze assets of the ruling junta and other Burmese institutions, and expand U.S. visa restrictions to include managers of state-owned enterprises as well as 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 that placed these sanctions on Burma.

Burma became a member of the Asia/Pacific Group on Money Laundering in January 2006, and is a party to the 1988 UN Drug Convention. Over the past several years, the Government of Burma has expanded its counternarcotics cooperation with other states. The GOB has bilateral drug control agreements with India, Bangladesh, Vietnam, Russia, Laos, the Philippines, China, and Thailand. These agreements include 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. The government signed a cooperative MOU with Indonesia's FIU in November 2006.

Burma is a party to the UN Convention against Transnational Organized Crime and ratified the UN Convention on Corruption in December 2005 and the UN International Convention for the Suppression of the Financing of Terrorism in August 2006. Burma signed the ASEAN Multilateral Assistance in Criminal Matters Agreement in January 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. To fully implement a strong anti-money laundering/counterterrorist financing regime, Burma must provide the necessary resources to administrative and judicial authorities who supervise the financial sector, so they can apply and enforce the government's regulations to fight money laundering successfully. Burma must also continue to improve its enforcement of the new regulations and oversight of its banking system, and end all government policies that facilitate the investment of drug money into the legitimate economy. It also must monitor more carefully the widespread use of informal remittance or "hundi" networks, and should criminalize the funding of terrorism.

Cambodia

Cambodia is neither an important regional financial center nor an offshore financial center. While there have been no verified reports of money laundering in Cambodia, it serves as a transit route for heroin from Burma and Laos to international drug markets such as Vietnam, mainland China, Taiwan, and Australia. Its very weak anti-money laundering regime, a cash-based economy with an active informal banking system, porous borders with attendant smuggling, casinos, and widespread official corruption also contribute to money laundering in Cambodia.

The National Bank of Cambodia (NBC) has made some strides in recent years by beginning to regulate the small official banking sector, but other nonbank financial institutions, such as casinos, remain outside its jurisdiction. While the Ministry of Interior has legal responsibility for oversight of the casinos and providing security, it exerts little supervision. In July 2006, the Council of Ministers approved draft legislation that would criminalize money laundering and the financing of terrorism and forwarded the bill to the National Assembly for ratification. However, the National Assembly had not taken action as of mid-November 2006.

Cambodia's banking sector is small but expanding, with fifteen general commercial banks, five commercial banks, and numerous microfinance institutions. However, overall lending and banking activity remains limited as most Cambodians keep their assets outside the banking system. Economists

note that while a typical country would have a bank deposit to GDP ratio of roughly 60 percent, Cambodia's ratio is only 16 percent—low even by developing economy standards. Cambodia's banking system is highly consolidated, with two banks—Canadia Bank and Foreign Trade Bank (FTB)—accounting for more than 40 percent of all bank deposits. Moreover, during the October 2005 privatization of the Foreign Trade Bank, Canadia gained a 46 percent share in FTB, further strengthening Canadia's large role in the financial services sector.

The NBC has regulatory responsibility for the banking sector. The NBC regularly audits individual banks (that have a small numbers of transactions and deposits) to ensure compliance with laws and regulations. There is a standing requirement for banks to declare transactions over 42,000,000 riel (approximately $10,000). The NBC says its audits reveal that this requirement is generally followed. While there are no reports to indicate that banking institutions themselves are knowingly engaged in money laundering, government audits would likely not be a sufficient deterrent to money laundering through most Cambodian banks. However, questions from correspondent banks about large transfers and Cambodia's relatively high 0.15 percent tax on financial transactions might discourage money laundering within the formal banking sector

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 such as casinos. The vulnerability of Cambodia's financial sector is further exacerbated because of the intersection of the casino and banking interests with four companies having whole or partial shares in both banks and casinos,

With increased political stability and the gradual return of normalcy in Cambodia after decades of war and instability, bank deposits have risen by 12-15 percent per year since 2000 and the financial sector shows some signs of deepening as domestic business activity continues to increase in the handful of urban areas. Foreign direct investment, while limited, is increasing after several years of contraction.

Reportedly, 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 reportedly no evidence that smuggling is funded primarily by drug proceeds, including the importing and local production of the methamphetamine (ATS). 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 its proceeds. Cambodia has a cash-based and dollar-based economy, and the smuggling trade is usually conducted in dollars. 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.

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 nonbank 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 nonbank financial institutions in Cambodia are the casinos, where foreigners are allowed to gamble but 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 financial operations.

There are currently more than 20 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 in Phnom Penh that has avoided the regulation that all casinos be at least 200 kilometers from the capital city. Casino patrons placing small bets simply hand-carry their money across borders, while others use either bank transfers or junket operators. There is no effective oversight of cash movement into or out of Cambodia. Cambodian casinos have accounts with major Thai or Vietnamese banks and patrons can wire large amounts of money to one of these foreign accounts. After a quick phone call to verify the transfer, the Cambodian casino issues the appropriate amount in chips. Casinos also work with junket operators who, despite their name, only facilitate money transfers and do not serve as travel or tour operators. Players deposit money with a junket operator in Vietnam or Thailand, the casino verifies the deposit and issues chips to the player—typically up to double the amount of the deposit. After the gambling session ends, the junket operator then has 15 days to pay the casino for any losses. Because the junket operator is responsible for collecting from the patrons, casinos see little need to investigate the patron's ability to cover his/her potential debt or the source of his/her wealth.

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 and in fulfilling "Know Your Customer" best practices, though no suspicious transactions have yet been reported to the NBC. 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.

In 2005, Cambodia became a party to the 1988 UN Drug Convention, the UN Convention Against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. No existing laws currently address terrorism financing, although it is specifically addressed in the draft law on money laundering. The NBC does circulate to financial institutions the list of individuals and entities included on the UNSCR 1267 Sanction Committee's consolidated list, and 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 conducts mutual evaluations of members' anti-money laundering and terrorism financing efforts. An APG evaluation of Cambodia originally scheduled for 2005 has been delayed at the government's request until early 2007 to permit passage of the draft Law on the Prevention of Money Laundering and Financing of Terrorism before the evaluation. According to the draft law, a new financial intelligence unit (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.

A Working Group, including the NBC and the Ministries of Economy and Finance, Interior, and Justice, the National Authority for Combating Drugs was formed on November 26, 2003 to draft anti-money laundering legislation that meets international standards. 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 (including in free trade zones); 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. While the draft anti-money laundering legislation was being considered, the NBC planned to issue a series of regulations that have the force of law (parkas) and that will criminalize money laundering and terrorism financing, as well as update existing financial rules and regulations. However, these prakas were not issued due to concerns that they would set stricter rules than would be included in the new legislation

Making progress on the long-awaited draft anti-money laundering legislation and becoming a party to the UN conventions on drugs, organized crime, and terrorism financing are positive steps. The Government of Cambodia should pass the draft anti-money laundering and counterterrorist financing legislation as soon as possible. Questions remain regarding the government's ability to implement and enforce the measures once they are in place. To this end, Cambodia should engage fully with the Asia/Pacific Group on Money Laundering and implement all recommendations of its upcoming mutual evaluation in order to develop a comprehensive viable anti-money laundering/counterterrorist financing regime that comports with international standards.

Canada

With $1.5 billion in trade crossing the border each day, both the United States and Canadian governments are concerned about the criminal cross-border movements of currency, particularly the illicit proceeds of drug trafficking. Significant amounts of U.S. currency derived through illegal drug sales in the United States are subsequently laundered through the Canadian financial system each year.

The Government of Canada (GOC) enacted the Proceeds of Crime (Money Laundering) Act in 2000 to assist in the detection and deterrence of money laundering, facilitate the investigation and prosecution of money laundering, and create the 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 to cover all indictable offenses, including terrorism and the trafficking of persons. In addition to amending the PCMLTFA, the 2001 reforms made it a crime under the Canadian Criminal Code to knowingly collect or give funds to carry out terrorism, denied or removed charitable status from those supporting terrorism and facilitated freezing and seizing their assets.

The PCMLTFA created 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 10,000 Canadian dollars (approximately $9,000) or more. Failure to report cross-border movements of currency and monetary instruments could result in seizure of funds or penalties ranging from approximately $225 to $4,500. Failure to file a suspicious transaction report (STR) could result in up to five years' imprisonment, a fine of approximately $1.8 million, or both. The law protects those filing suspicious transaction reports

from civil and criminal prosecution. There has been no apparent decline in deposits made with Canadian financial institutions as a result of Canada's revised laws and regulations.

Canada's FIU, the Financial Transactions and Reports Analysis Center of Canada (FINTRAC), was established in July 2001. FINTRAC is an independent agency within the GOC that receives and analyzes reports from financial institutions and other financial intermediaries (such as money service businesses, casinos, accountants, and real estate agents) as mandated by the PCMLTFA, and makes disclosures to law enforcement and intelligence agencies. Guidelines explaining the PCMLTFA and its requirements were published by FINTRAC in 2002; further additions were made in 2003. The guidelines provide an overview of FINTRAC's mandate and responsibilities, and include background information about money laundering and terrorist financing, including their international scope and nature. The guidelines also provide an outline of the Canadian legislative requirements for a compliance regime, record keeping, client identification and reporting transactions.

FINTRAC currently has over 37.4 million financial transaction reports contained within its database. During 2005-2006, FINTRAC received nearly 15 million reports from reporting entities. FINTRAC produced a total of 168 case disclosures in 2005-2006, totaling approximately $4.5 billion, more than double the value of the previous year. The case disclosures represented nearly $4.3 billion in transactions of suspected money laundering, and $230 million in transactions of suspected terrorist financing activity and other threats to the security of Canada. Thirty-two domestic law enforcement agencies and 10 foreign counterparts have received disclosures from FINTRAC.

FINTRAC has the authority to negotiate information exchange agreements with foreign FIUs. It has signed over 35 memoranda of understanding (MOUs) to establish the terms and conditions to share intelligence with FIUs—including an MOU with FinCEN, the FIU of the United States—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.

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 of involving the commission of a terrorist financing offense. 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. The GOC has also listed and searched financial records for suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list. There are currently more than 500 individuals and entities associated with terrorist activities designated by the GOC. This designation effectively freezes their assets and prohibits fund-raising on their behalf in Canada.

In a 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." United States 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 United States and Canadian law enforcement officers to exchange information promptly concerning suspicious sums of money found in the possession of individuals attempting to cross the United States-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 October 2006, Bill C-25 was introduced to Parliament to amend the PCMLTFA. Bill C-25 is designed to make Canada's anti-money laundering and antiterrorist financing regime consistent with

the Financial Action Task Force (FATF) recommendations. Canada will undergo a FATF Mutual Evaluation in early 2007. The new legislation will expand the coverage of Canada's anti-money laundering and antiterrorist financing regime by bringing additional business sectors, including lawyers and dealers in precious metals and stones, under the authority of the PCMLTFA and related regulations. Bill C-25 also mandates that FINTRAC create a national registry for money service businesses and establish a system of administrative monetary penalties. The proposed measures will improve compliance with the reporting, record keeping and client identification provisions of the PCMLTFA. The Bill permits FINTRAC to include additional information in the intelligence product that FINTRAC can disclose to law enforcement and national security agencies, as recommended in the 2004 Auditor General's Report. Bill C-25 received final Parliamentary approval in December 2006

In addition to new legislation, the GOC is undertaking other initiatives to bolster its ability to combat money laundering and terrorist financing. In May 2006, the GOC announced that it had added in the 2006 budget approximately $58 million over the next two years for FINTRAC, the Royal Canadian Mounted Police (RCMP), and the Department of Justice. The new funding will increase the number of RCMP officers working in the antiterrorist financing and anti-money laundering units; increase the capabilities of the Canada Border Services Agency (CBSA) to detect unreported currency at airports and border crossings; enable Canada's Department of Justice to handle the expanding litigation workload that will result from increasing the enforcement resources of other GOC agencies; and ensure that FINTRAC can better analyze transactions reports and monitor compliance of unregulated financial sectors such as money remitters.

Canada is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. The GOC has also ratified the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, the Inter-American Convention against Terrorism, and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The GOC has signed, but not yet ratified, the UN Convention against Corruption.

Canada is a member of the Financial Action Task Force and assumed the FATF Presidency for a one-year term beginning in July 2006. Canada became a member of the Asia/Pacific Group on Money Laundering (APG) in July 2006. Canada also belongs to the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. FINTRAC became a member of the Egmont Group in 2002. In June 2006, Toronto was selected as the permanent location of the Secretariat of the Egmont Group. The GOC will contribute approximately $4.5 million over the next five years to help establish the Secretariat

Canada has demonstrated a strong commitment to combat money laundering and terrorist financing both domestically and internationally. In 2006, the GOC made strides in enhancing its anti-money laundering regime and reducing its vulnerability to money laundering and terrorist financing, and should continue to expand these efforts in 2007. The GOC should consider taking the necessary steps to permit FINTRAC to disclose timely and meaningful information to Canadian law enforcement agencies on suspicious financial transactions. Were the GOC to do so, both Canada and the United States might see a significant decrease in the illegal cross-border movement of cash and narcotics, as well as a significant increase in successful prosecutions and convictions.

Cayman Islands

The Cayman Islands, a United Kingdom (UK) Caribbean overseas territory, continues to make strides in strengthening its anti-money laundering program. However, the islands remain vulnerable to money laundering due to their significant offshore sector. The Cayman Islands is home to a well-developed offshore financial center that provides a wide range of services, including banking, structured finance,

investment funds, various types of trusts, and company formation and management. At the end of 2006, The Cayman Islands Monetary Authority (CIMA) reported over 450 banks and trust companies, 8,143 funds, 740 captive insurance companies, and 62,572 exempt companies licensed or registered in the Cayman Islands.

The CIMA is responsible for the licensing, regulation and supervision of the Cayman Islands' financial industry, which includes banks, trust companies, investment funds, fund administrators, insurance companies, insurance managers, money service businesses, and corporate service providers. The CIMA received independence to issue and revoke licenses and enforce regulations through the Monetary Authority Law 2003. Supervision of licensees is carried out through on-site and off-site examinations, which include monitoring for anti-money laundering and counter financing terrorism compliance. A 2001 amendment to The Companies Law institutes a custodial system in order to immobilize bearer shares. There are no shell banks in the Cayman Islands. The CIMA has a statutory function under the Monetary Authority Law to provide assistance to overseas regulatory authorities, and is able to share information with such authorities with or without a memorandum of understanding (MOU). In June 2005, the CIMA signed an MOU with the U.S. Securities and Exchange Commission (SEC). The CIMA also has several other MOUs with regulatory counterparts in a number of countries, including Brazil, Canada, Jamaica and Panama.

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 15,000 Cayman Islands dollars (approximately $18,000), or who may be engaging in money laundering.

The Misuse of Drugs Law criminalized narcotics-related money laundering. The Proceeds of Criminal Conduct Law (PCCL) criminalized money laundering related to all other serious crimes. The PCCL provides for the offense of money laundering where a person or business has engaged in criminal conduct or has benefited from criminal conduct; tax offenses are not included. The PCCL requires mandatory reporting of suspicious transactions, and makes failure to report a suspicious transaction a criminal offense that could result in fines or imprisonment. There is no threshold amount for the reporting of suspicious activity. A suspicious activity report (SAR) must be reported once it is known or suspected that a transaction may be related to money laundering or terrorism financing.

Established under PCCL (Amendment) Law 2003, the Financial Reporting Authority (FRA) replaces the former financial intelligence unit of the Cayman Islands. The FRA began operations on January 12, 2004. FRA staff consists of a director, a legal advisor, a senior 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 2005 to June 2006, the FRA developed 221 new cases, which consisted of suspicious activity reports received from reporting entities as well as information requests from foreign FIUs.

The Cayman Islands is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001. 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 provision on money laundering related to terrorist financing. However, the United Kingdom has yet to extend the application of the International Convention for the Suppression of the Financing of Terrorism to the Cayman Islands.

In 1986, the United States and the United Kingdom signed a Treaty concerning the Cayman Islands relating to Mutual Legal Assistance in Criminal Matters. By a 1994 exchange of notes, Article 16 of that treaty has been deemed to authorize asset sharing between the United States and the Cayman Islands. The Cayman Islands is a member of the Caribbean Financial Action Task Force (CFATF), and the FRA is a member of the Egmont Group.

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

Chile

Chile's large and 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. Some Chilean officials believe these increased flows do not, at the same time, create a significant money laundering threat. However, the combination of Chile's irregular regulatory oversight and favorable financial reputation might make it attractive to criminal organizations and other potential 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, Law 19.913 of December 2003, and Law 20.119 of August 2006. 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 rate of 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 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. The new UAF is part of the Ministry of Finance.

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 (financing 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 card 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, 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. Under Law 20.119, which went into effect on August 31, 2006, pension funds and sports clubs are now also subject to reporting requirements.

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 (UF) (approximately $12,000). 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. The Chilean tax service

(Servicio de Impuestos Internos) 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 UF 450 into or out of Chile must be reported to Customs, 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 legally empowered to seize or otherwise stop the movement of funds, and the entry or exit of these funds is not subject to taxation.

On August 31, 2006, Law 20.119 went into effect. This law restores several powers of the UAF that had been previously removed from the original draft of Law 19.913 by Chile's constitutional tribunal, including the UAF's ability to impose sanctions for noncompliance. Law 19.913 did not grant any government or supervisory entity the authority to impose penalties for partial or noncompliance, resulting in only voluntary-not compulsory-reporting of suspicious or unusual financial transactions. Additionally, while the UAF could previously only exact information from institutions which had already submitted suspicious transaction reports (STRs), it can now demand information to pursue leads received through any official avenue, be it an STR, a cash transaction report (CTR), cross border report, or a request for information from a foreign FIU. The UAF may also now access any government information (police, taxes, etc.) not covered by secrecy or privacy laws. Article 154, paragraph 1 of the Chilean General Banking Law establishes bank secrecy on all types of bank deposits, and prohibits the institution from providing background information related to such operations to any individual except the person making the deposit, or to a third party expressly authorized by the client. Records covered by secrecy protection can now be obtained by the UAF with permission from a judge, usually obtained within 48 hours. One deficiency of Law 19.913 that was not corrected with the passage of Law 20.119, however, is the lack of a definition of "suspicious activity" in the reporting requirements for nonbank and nonfinancial institutions.

The UAF began operating in April 2004, and began receiving STRs from reporting entities in May 2004. In 2005 the UAF received an average of 13 STRs per month. The average number per month increased to 19 in 2006. The average breakdown per month was 14.6 STRs from banks, 1.6 from exchange houses, 1.8 from money transfer and courier services, and 1 from other obliged institutions. By October 1, 2006, the UAF had received 170 STRs, 131 of which were from banks. STRs from nonbank institutions comprise about 23 percent of the total STRs received by October 2006.

Cash transaction reports are also requested regularly by the UAF. In May 2005 money exchange houses were instructed by the UAF to submit CTRs every three months. In September 2005, banks were instructed to submit CTRs every three months. In March 2006 the rest of the obliged institutions were instructed to submit CTRs every 3 months, though some specific institutions without a high amount of cash transactions (e.g. notaries) may submit every 6 months. In all cases, institutions must report CTRs dating from May 2004, when the obligation to record cash transactions over 450 UF went into effect. The UAF received approximately 1000 CTRs in 2006.

The UAF has two STR forms—one for banks, and the other for nonbanking institutions. As of November 2006 it became possible to submit STRs and CTRs through the Internet. Suspicious transaction reports from financial institutions can also be received electronically, via a system known as SINACOFI (Sistema Nacional de Comunicaciones Financieras) that is used by banks to distribute encrypted information among themselves and the Superintendence of Banks.

Banks in Chile are supervised formally by the Superintendence of Banks and Financial Institutions (SBIF) and informally by the Association of Banks and Financial Institutions. Banks are obliged 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 noncurrent accounts. Stock brokerages, securities firms and insurance companies are under the supervision and regulation of the Superintendence of Securities and Insurance. The Superintendence of Securities and Insurance is an

autonomous corporate agency affiliated to the Chilean Government through the Ministry of Finance, and enforces compliance with all laws, regulations, by-laws and other provisions governing the operation of securities, stock exchange and insurance companies in Chile.

In March 2006, the SBIF developed new rules establishing the norms and standards for banks and financial institutions (including leasing companies, securities companies and agents, factoring companies, insurance companies, stock brokerages, general funds-managing companies, and investment fund-managing companies) to prevent money laundering and terrorism financing. These rules also require financial institutions to keep records with updated background information on their clients throughout the period of their commercial relationship. Additionally, Chilean law requires that banks and financial institutions maintain records for a minimum of five years on any case reported to the UAF.

One weakness in Chile's efforts to combat money laundering is that nonbank financial institutions, such as money exchange houses and cash couriers, currently do not fall under the supervision of any regulatory body for compliance with anti-money laundering and counterterrorist financing standards. In Santiago alone there are approximately 55 exchange houses, many of which do not record or share with other exchange houses any information about their customers. Discerning suspicious activity is more difficult without due diligence on clients or good record-keeping. An attempt to self-regulate was undertaken by six exchange houses that formed the Chamber of Exchange Houses and Couriers in 1999, and registered with the Ministry of Economy. However, the Association dissolved in October 2006. Exchange houses as well as cash courier companies are also requested by Law 19,913 to report any suspicious transaction and any cash transaction over UF 450 to the UAF. The lack of supervision, definition of "suspicious activity," and a harmonized system to keep record of daily transactions diminishes useful reporting to the UAF, and undermines the effectiveness of the system. This sector appears particularly vulnerable to abuse by money launderers.

Chile's gaming industry falls under the supervision of the Superintendence of Casinos, which is in charge of drafting regulations about casino facilities, and the administration, operation and proper development of the industry. There are currently seven casinos located throughout the country. The SCJ has oversight powers over the industry but no law enforcement or regulatory authority. Under Law 19.995, the Superintendence of Casinos granted authorization for 10 casinos to operate in Chile after participating in an international and domestic bidding process to assign 17 permits during 2005 and 2006. Seven of these permits are still under a revision process; it is expected that their permits will be issued by December 2006. In total, 22 casinos, including the 7 already in operation, will be fully operating by 2008 under the oversight authority of the Superintendence of Casinos. There is currently no legal framework for supervising the money moving through the gaming industry. However, Article 3 of Law 19.913 requires casinos to report to the UAF any transaction in cash for over UF 450 (approximately $12,000) and any suspicious operation, to present them with balance sheets, to provide financial reports, to keep historical accounting records, and to designate a compliance official to relate to the UAF. Currently the Superintendence of Casinos has focused on analyzing the integrity of the bidding companies. They have investigated these companies with the support of domestic and international police and financial institutions.

When the UAF determines that an account or a case requires further investigation, it passes the information to the Public Ministry (the public prosecutor's office). The Public Ministry has been responsible for receiving and investigating all cases from the UAF since June 2005 (prior to June 2005, all cases deemed by the UAF to require further investigation were sent to the Consejo de Defensa del Estado or CDE). Of the 170 STRs received as of October 1, 2006, the UAF sent 27 of to the Public Ministry for further investigation. Under Law 20.119, 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 begin prosecution.

The Chilean investigative police (PICH) work in conjunction with the Public Ministry on money laundering investigations. The PICH investigators appear to be very competent and well-trained, but complain about insufficient access to information. Chilean law prohibits the UAF from giving information directly to law enforcement, and allows the sharing of information only with the Public Ministry and foreign FIUs. Currently PICH and other law enforcement must request financial information from the Public Ministry, which in turn requests it from the UAF. The police and prosecutors have expressed concern about the lack of timely access to information.

No money laundering cases have been prosecuted to date in Chile. The first such case is scheduled to go to trial in July 2007. The case was brought to the attention of the Chilean authorities when local press ran articles about a Chilean arrested in Germany for drug trafficking. The articles also detailed the suspect's business dealings in Chile, which led to the decision to investigate the case in Chile as well. Through cooperation with the German government, the Government of Chile (GOC) discovered the suspect's brother had been laundering money in Chile tied with the drug trafficking in Germany. The Public Ministry and PICH continue to cooperate with U.S. and regional law enforcement in money laundering investigations.

Two free trade zones exist in Chile, in Punta Arenas and Iquique. The Iquique free trade zone, the larger of the two, also has an extension in Arica, near Chile's border with Peru. The physical borders of the free trade zone are porous and largely uncontrolled. There are indications that money laundering schemes are rampant in the Iquique-Arica free trade zone. Chilean resources to combat this issue are extremely limited. Police investigative efforts suggest possible criminal links between Iquique and the Triborder Area (Brazil, Paraguay and Argentina), involving both terrorist financing and money laundering. In December 2006, the U.S. Department of Treasury designated nine individuals and two businesses in the Triborder Area that have provided financial and logistical support to Hizballah; one of those individuals, Hatim Ahmad Barakat, had traveled to Chile to collect funds intended for Hizballah, and was reported to be a significant shareholder in at least two businesses in Iquique. Hatim Barakat has been in prison in Paraguay since 2004.

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, financing a terrorist act and the provision (directly or indirectly) of funds to a terrorist organization are punishable by five to ten years in prison. 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 which allow 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 CONACE, the National Drug Control Commission, to fund drug abuse prevention and rehabilitation programs. Under the present law, forfeiture is possible for real property and financial assets. Civil forfeiture is not permitted.

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. On September 13, 2006, the GOC 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). GAFISUD conducted a mutual evaluation of Chile's efforts to combat money laundering in September 2006. 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 was nominated in 2006 to serve as the representative for the Americas on the Egmont Committee. The UAF has signed memoranda of understanding (MOUs) for the exchange of financial information with the United States FIU and FIUS of 25 other jurisdictions. Chile is also in the process of establishing MOUs with Belgium, British Virgin Islands, Gibraltar, Holland, Italy, Luxembourg, St. Kits and Nevis, United Kingdom, and Venezuela.

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. Chile took a major step in addressing some limitations of the UAF in the passage of Law 20.119. The new law should strengthen the ability of the UAF to aggressively track potential money laundering, but is too new at this point to determine if that has yet occurred. There continues to be no government oversight or standardization of most nonbank financial institutions, and anecdotal evidence that money laundering is occurring in money exchange houses makes this lack of oversight an issue of greater concern. The laws and institutions in Chile which combat money laundering are relatively new, and the system is still developing. The Public Ministry, the investigative police (PICH), and the uniformed national police (Carabineros) are trying to find effective ways to work together, but there are complaints of limited access to information and inter-agency conflict. Chile should take all necessary steps to ensure sufficient government oversight of nonfinancial institutions, aggressive action on the part of the UAF and other key agencies, and inter-agency cooperation, so that Chile is capable of effectively combating money laundering and terrorist financing.

China, People's Republic of

Money laundering remains a major concern as China 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 currently 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 China disguised as foreign investment, and as such, receive tax benefits. Continuing speculation following the July 2005 adjustment of the renminbi (RMB) exchange rate system also fueled illicit capital flows into China throughout 2006. Hong Kong-registered companies figure prominently in schemes to transfer corruption proceeds and in tax evasion recycling schemes. The International Monetary Fund estimated that money laundering in China may total as much as $24 billion annually.

On October 31, 2006, the National People's Congress passed a new Anti-Money Laundering Law, which came into effect January 1, 2007. This new law broadens the scope of existing anti-money laundering regulations to include any institution involved in money laundering. It mandates that financial and some nonfinancial institutions maintain records on accounts and transactions, and that they report large and suspicious transactions. The law more firmly establishes the Central Bank's authority over national anti-money laundering efforts, but does not clearly define "nonfinancial institutions" for this purpose. The law also increases the number of predicate offenses for money

laundering, to include fraud, bribery, and embezzlement. 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.

Additional regulations were announced in 2006 aimed at further strengthening China's anti-money laundering efforts. In December, 2006, China's central bank issued two new regulations—"Rules for Anti-Money Laundering by Financial Institutions", which will come into effect January 1, 2007, and "Administrative Rules for Reporting of Large-Value and Suspicious Transactions by Financial Institutions", which will come into effect March 1, 2007. Together, these regulations revise earlier PBC regulations implemented in March, 2004. The new regulations will require all financial institutions—including securities, trust companies and futures dealers—to report large and suspicious transactions. Any cash deposit or withdrawal of over RMB 200,000 or foreign-currency withdrawal of $10,000 in one business day must be reported within five days if electronically or within 10 days in writing to the PBC. Money transfers between companies exceeding RMB 2 million or US$200,000 in one day or between an individual and a company greater than RMB 500,000 or US$100,000 must also be reported. The regulations are slated for implementation between January and March of 2007.

These regulations enhance a prior 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 in particular were required to report suspicious foreign exchange transactions—but not all transactions, as in the new regulations—of more than $10,000 per person in a single transaction or cumulatively per day in cash, or noncash foreign exchange transactions of $100,000 per individual or $500,000 per entity either in a single transaction or cumulatively per day. Under the regulation, banks were further required to submit monthly reports to the PBC outlining suspicious activity and to retain transaction records for five years. Banks which failed to report on time can be fined up to the equivalent of approximately $3,600. Under the December 2006 regulations, financial institutions that fail to meet reporting requirements in a timely manner can have their licenses or business operations suspended.

On April 12, 2006, the PBC proposed a series of measures aimed at curbing money laundering in the insurance, banking and securities sectors. The proposed regulations, which were circulated for comment until May 8 2006, would require institutions to report all "block transactions"-defined as transactions worth more than 50,000 RMB (approximately $6,241) or $10,000 per day-to the PBC's anti-money laundering center for review. The proposal would also define the following as "block transactions": noncash transactions of more than 200,000 RMB or $100,000 per day and transactions between institutional accounts amounting to more than 1 million RMB or $500,000 per day. However, the current status of these proposed regulations is unclear.

The new Anti-Money Laundering Law passed in 2006 builds on China's 1997 Criminal Code. The 2006 law amended Article 191 of the Criminal Code to criminalize money laundering for seven predicate offenses, expanded from the original three predicate offenses, which were narcotics trafficking, organized crime, and smuggling. In 2001, Article 191 was amended to add terrorism as a fourth predicate offense. Article 191, however, still does not encompass all of the twenty designated categories of offenses identified by the Financial Action Task Force (FATF), even after passage of the 2006 law. Additionally, the 2006 law amended Article 312 to make it an offense to launder the proceeds of any crime through a variety of means. Article 312 criminalizes complicity in concealing

the proceeds of criminal activity. Article 174 criminalizes the establishment of an unauthorized financial institution.

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 $2,500) or, in foreign currency, up to $5,000, into 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, RMB-denominated, credit cards overseas. Such cards can now be used in Hong Kong, Macau, Singapore, Thailand, and South Korea. To address online fraud, the PBC 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, while enforcement is handled by the Ministry of Public Security.

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. According to the China Anti-Money Laundering Monitoring and Analysis Center, 683 suspicious money laundering cases had been reported to the police by the end of 2005. They involved 137.8 billion yuan ($17.2 billion) and over one billion U.S. dollars.

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 PBC 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. 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. In December, 2006, authorities in Shanghai announced they were investigating the country's largest-ever money laundering case, totaling about five billion yuan ($633 million). The case involves underground banks, according to Chinese media reports.

To remedy information deficiencies, the PBC 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. PBC

rules obligate financial institutions to perform customer identification, due diligence and record keeping. SAFE implemented a new regulation on March 1, 2004 requiring nonresidents, 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.

China supports international efforts to counter the financing of terrorism. Terrorist financing is now a criminal offense in China, 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, Chinese 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 Xinjiang Uighur Autonomous Region. 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.

China is a party to the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. China became as party to UN Convention against Corruption, and to the UN International Convention for the Suppression of the Financing of Terrorism in 2006.

China has signed mutual legal assistance treaties with 24 countries. The United States and China 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 United States and China cooperate and discuss money laundering and other enforcement issues under the auspices of the U.S.-China Joint Liaison Group's (JLG) subgroup on law enforcement cooperation. JLG meetings are held annually in either Washington, D.C., or Beijing. In addition, the United States and China have established a Working Group on Counterterrorism that meets on a regular basis. The PRC has established similar working groups with other countries as well.

In late 2004, China joined the Eurasian Group (EAG), a Financial Action Task Force (FATF)-style regional group which includes Russia, Belarus, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. In January 2005, China became an observer to the FATF and seeks to become a full member of the FATF. The FATF conducted a mutual evaluation of China in November, 2006.

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, terrorist financing and other criminal financial activity.

The Chinese Government 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 will 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 suspicious transaction reporting (STR) 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 noncompliance with requirements that financial institutions perform customer identification, due diligence, and record keeping. China should also ensure effective implementation of the many regulatory changes it has put in place over the past three years in seeking to build a highly functional anti-money laundering regime.

Colombia

The Government of Colombia (GOC) is a regional leader in the fight against money laundering. Comprehensive anti-money laundering 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. Although progress has been made in recent years, a complex legal system and limited resources for anti-money laundering programs have constrained 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 terrorist organizations. The GOC and U.S. law enforcement agencies are closely monitoring transactions that could disguise terrorist finance activities. 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 significant export sectors that ship 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 not related to money laundering or terrorist financing, such as bank fraud, has not been widely seen in Colombia. However, criminal elements have used the banking sector to launder money, under the guise of licit transactions. Money laundering has occurred via trade and the nonbank 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.

Money launderers in Colombia employ a wide variety of techniques. Money launderers frequently use such alternative laundering methods as the Black Market Peso Exchange and contraband trade to launder the proceeds of illicit funds. Colombia's financial intelligence unit, the Unidad de Información y Análisis Financiero (Financial Information and Analysis Unit, or UIAF) has identified more than ten techniques alone for laundering money via contraband trade. In 2005, the GOC asserted that illicit funds were being laundered by imports of under-valued Chinese manufactured goods via Panama's Colon Free Trade Zone, and implemented specific controls on Panamanian re-exports to Colombia. Panama countered with a complaint to the World Trade Organization (WTO), and eventually the controls were dropped in October 2006. Colombian industry reaction to the decision was negative, reflecting in part the realities of increasing Chinese competition, but as well the very negative impact that laundering via contraband trade has on legitimate businesses.

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 (carrying currency on a person) of U.S. and other foreign currencies and an increase in the number of shell companies operating in Colombia. Pre-paid debit cards, internet banking, and the dollarization of the economy of neighboring Ecuador represent some of the growing challenges to money laundering enforcement in Colombia.

Casinos in Colombia lack adequate regulation and transparency. Free trade zones in some areas of the country 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 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 and 2001, Colombia criminalized the laundering of the proceeds of extortion, illicit enrichment, rebellion, narcotics trafficking, 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 is itself an offense punishable under the criminal code, with penalties increased in 2002 to imprisonment of two to five years.

Established in 1999 within the Ministry of Finance and Public Credit, 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 (FIUs) in Central and South America. The UIAF currently has approximately 45 personnel, and a new director took over leadership of the unit in August 2006.

The UIAF has broad authority to access and analyze financial information from public and private entities in Colombia. Obligated entities, which include banks, stock exchanges and brokers, mutual funds, investment funds, export and import intermediaries, credit unions, wire remitters, exchange houses, public agencies and entities that fall under the supervision of the Superintendence of Notaries, are required to report suspicious transaction to the UIAF, and are barred from informing their clients of their reports. Most obligated entities are also required to establish "know-your-customer" provisions. With the exception of exchange houses, obligated entities must report to the UIAF cash transactions over $5,000. Through December 2004, the UIAF had also required exchange houses provide bulk data for all transactions above US$ 700. A change in January 2005 extended this requirement to all financial institutions for bulk data on transfers, remittances and currency transactions, and lowered the threshold transaction value to US$ 200. This considerably broadened the data which UIAF examines, enhancing their analytical coverage.

Financial institutions are required by law to maintain records of account holders and financial transactions for five years. Secrecy laws have not been an impediment to bank cooperation with law enforcement officials, since under Colombian law there is a legal exemption to client confidentiality when a financial institution suspects money laundering activity. Colombia's banks have strict compliance procedures, and work closely with the GOC, other foreign governments and private consultants to ensure system integrity. General negligence laws and criminal fraud provisions ensure the financial sector complies with its responsibilities while protecting consumer rights. Obligated entities are supervised by the Superintendence of Finance, which was created in November 2005 by combining the former Superintendence of Banks and the former Superintendence of Securities into a

single organization. The fusion was generally welcomed as providing more consistent and comprehensive oversight of the financial industry.

Following UIAF's inception in 1999, the number of STRs grew rapidly as financial institutions strived to comply with the reporting requirement, peaking at 13,488 STRs in 2002. The UIAF analysts noted, however, that the quality of reports was lacking, and subsequently began an outreach program to educate reporting institutions on what type of financial activity merited an STR. The quantity of STRs fell to 9,074 in 2005, but UIAF is generally pleased that the overall quality of reporting has improved. Currently, 20 percent of STRs are deemed by UIAF to merit further investigation by their analysis unit, and between five and seven percent of cases are forwarded to an enforcement division for further action. In 2006, 6,120 STRs were filed through the month of October. The prosecutor's office reported 87 successful convictions for money laundering in 2005, and 66 convictions between January and October 2006.

In June 2006, the UIAF inaugurated a new centralized data network connecting 17 governmental entities as well as the banker's association (Asobancaria). The network allows these entities to exchange information online and share their databases in a secure manner, and should facilitate greater cooperation among government agencies in preventing money laundering and other financial crimes. The pilot phase of the project had been made possible by USG financial contributions.

Given past concerns about bulk cash smuggling, in October 2005, the GOC made it illegal to transport more than the equivalent of US$ 10,000 in cash across Colombian borders, inbound or outbound. Such transactions must now be handled through the formal financial system, which is subject to the UIAF reporting requirements. Colombia has criminalized cross-border cash smuggling and defines it as money laundering. In spite of improvements, 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, and it has been noted that customs officials lack the proper technical equipment necessary to do their job. The GOC has been slow to make needed changes in this area.

Colombian law provides for both conviction-based and nonconviction 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, including Law 30 of 1986 and Law 333 of 1996; however, procedural and other difficulties led to only limited forfeiture successes, with substantial assets tied up in proceedings for years. In 2002, the GOC enacted Law 793, which 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, places obligations on claimants to demonstrate their legitimate interest in property, 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. Law 785 of 2002 also strengthened the GOC's ability to administer seized and forfeited assets. 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.

Laws 793 and 785 have helped streamline the asset forfeiture process, resulting in a tenfold increase in sentences. Yet problems remain: concerns about personal liability have discouraged official action in some cases, exceptions in proceedings can still cause cases to drag on for years, and the pace of final

decisions remains slow compared to new seizures. Prosecutors also have limited discretion on assets seizures, and must seize all assets associated with a case, including those of minimal value or those which clearly risk loss under state administration, such as livestock.

In 2006, the Colombian media criticized DNE's asset management, citing losses to the GOC from poor maintenance or even loss of assets under their administration. Prior to the fourth quarter of 2006, only a very limited number of assets were disposed of or transferred to government entities, due to the huge task of managing the assets. At the end of 2006, DNE was managing 75,000 assets, some 75 percent of which were seized before 2002. With limited resources and only 45 staff dedicated to asset management, the DNE must rely on outside contractors to store or manage assets. The GOC has established priorities for the proceeds of disposed assets; however, DNE's management task will only be reduced when the pace of judicial decisions and disposals exceeds new seizures.

The Colombian government has been aggressively pursuing the seizure of assets obtained by drug traffickers through their illicit activities. For the last three years the Sensitive Investigations Unit (SIU) of the Colombian National Police (CNP), in conjunction with U.S. law enforcement and the Colombian Fiscalia (prosecutor's office) have been investigating the Cali and North Valle cartels' business empires under the Rodriguez Orejuela brothers and the Grajales family, respectively. The Cali and Norte Valle cartels, as well as their leaders and associated businesses, are on the U.S. Department of the Treasury Office of Foreign Asset Control (OFAC) list of Specially Designated Narcotics Traffickers (SDNTs), pursuant to Executive Order 12978. Colombian and U.S. law enforcement agencies have cooperated in 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. These joint actions to apply economic sanctions have gravely affected the Colombian drug cartels' abilities to use many of the financial assets they derived from their narcotics trafficking activities and have assisted the Colombian government in creating cases in order to seize narcotics related assets. Recent seizures include those of the Drogas La Rebaja drug store chain owned by the Rodriguez Orejuela brothers in 2004, and the Grajales' agricultural companies and Casa Estrella department stores in June 2005 and August 2006 respectively.

In September 2006, 28 family members of the Rodriguez-Orejuelas brothers entered into a plea agreement with the United States. Under the terms of the agreement, the family members agreed to forfeit their right, title, and interest in all Rodriguez-Orejuela business entities and other assets worldwide, as well as all assets of any nature in the United States, up to a maximum of $ 2.1 billion in value. Approximately $ 260 million in assets related to this judgment have been identified in Colombia.

Bilateral cooperation between the GOC and the USG remains strong and active. In 2006, several major investigations by DEA and the sensitive investigation unit (SIU) of the Department of Administrative Security (DAS) resulted in arrests and seizures of major money laundering organizations operating between the countries. These include Operation Common Denominator, which led to the arrests of money launderers that utilized the black market peso exchange to launder drug proceeds from the U.S. and Europe, and the seizure of over 17 million euros and 2,000 kilograms of cocaine in Spain; Operation Hoyo Verde, which resulted in 88 arrests for money laundering in the United States, Curacao, the Dominican Republic, Puerto Rico, the Netherlands and Colombia, and the seizure of $ 8.6 million in cash, $ 5.8 million in assets and 100 kilograms of cocaine; and Operation Plata Sucia, which led to 28 money laundering arrests in Colombia, New York and Florida, and the seizure of over $5 million in currency, 65 kilograms of heroin and 60 kilograms of cocaine. Extradition requests to the United States are pending in many of the arrests.

In January 2007, the Colombian National Police in cooperation with the DEA recovered approximately $80 million in primarily U.S. currency and gold on raids on houses used to stash drug

proceeds. Reportedly, the total value is probably the most ever seized by law enforcement in a single operation anywhere in the world.

The U.S. Department of Homeland Security's Immigration and Customs Enforcement (ICE) division has also worked closely with Colombian authorities. In 2002, ICE supported the CNP establishment of a financial investigative unit within the organization's intelligence and investigations unit (DIJIN). ICE also helped Colombia establish a Trade Transparency Unit (TTU) to analyze trade data for customs fraud and money laundering. The TTU analysis showed a direct financial relationship between the narcotics cartels and the Revolutionary Armed Forces of Colombia (FARC), the primary armed guerilla group also designated as an international terrorist organization

Significant strides have been made in the past year to close a loophole in Colombian law to make terrorist financing an autonomous crime. A law was approved by the Colombian Congress (Project 208) which amended the penal code to define and criminalize direct and indirect financing of terrorism, of both national and international terrorist groups. In accordance with the Financial Action Task Force of South America (GAFISUD) and Egmont Group recommendations, the UIAF will receive STRs 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 with either of these regulations, but many had complied regardless. The bill was passed by the Colombian Senate in September 2006, and by the Colombian House of Representatives in December 2006. Presidential approval is expected in 2007.

Colombian law is unclear on 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's publication of Specially Designated Terrorists. Charities and nongovernmental organizations (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 STR reporting. Reportedly, the GOC acknowledges that monitoring NGOs and charities is an issue that needs continued work and vigilance.

Colombia is a member of GAFISUD and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group, which it chaired in 2005. The UIAF is a member of the Egmont Group, and has signed memoranda of understanding with 27 FIUs around the world. Colombia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. The GOC has signed, but not ratified, the Inter-American Convention against Terrorism. Colombia formally ratified the UN Convention against Corruption in October 2006.

In 2006, the Government of Colombia has seen additional progress in the development of its financial intelligence unit, regulatory framework and interagency cooperation within the government. The passage of a formal terrorist finance law within the year is another development in fighting terrorism and financial crime. International cooperation with the U.S. and other countries has led to several high-profile seizures and prosecutions. However, weaknesses remain. The growth in contraband trade to launder illicit drug proceeds will require even greater interagency cooperation within the GOC, including coordination between the UIAF and DIAN, the tax and customs authority. Congestion in the court system, procedural impediments and corruption are also problems. Limited resources for prosecutors, investigators, and the judiciary hamper their ability to close cases and dispose of seized assets. Streamlined procedures for the liquidation and sale of seized assets under state management

could help provide funds available for Colombia's anti-money laundering and counterterrorist financing regime.

Comoros

The Union of the Comoros (Comoros) consists of three islands: Grande Comore, Anjouan and Moheli. An ongoing struggle for influence continues between the Union and island presidents. 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, Comoran authorities lack the capacity to effectively implement and enforce the legislation, especially on the island of Anjouan. In May 2006, Muslim cleric Ahmed Abdallah Mohamed Sambi was elected President in the first peaceful change of power in Comoros' post-independence history. He won the election with 58 percent of the vote after campaigning on promises to fight corruption and unemployment. The presidency of the union rotates between the three islands. The former incumbent, Azali Assoumani, represented Grand Comore; Sambi is from Anjouan. The three islands in the Comoros 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: requires financial and related records to be maintained for five years; permits assets generated or related to money laundering activities to be frozen, seized and forfeited; requires residents to declare all currency or financial instruments upon arrival and departure, and nonresidents to declare all financial instruments upon arrival and all financial instruments above Comoran francs 500,000 (approximately $1,250) on departure; 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; requires nonbank financial institutions to meet the same customer identification standards and reporting requirements as banks; 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 francs 5 million (approximately $12,500); and, criminalizes the provision of material support to terrorists and terrorist organizations. Although there is a suspicious activity filing requirement in the Union's AML law, there does not appear to be an independent financial intelligence unit in either Anjouan or the Union. As of February 2006, no suspicious transaction reports had been filed with the Comorian Central Bank in Grand Comore as required under the existing Union law, and the branch of the Central Bank located in Anjouan had no knowledge of the shell bank entities that have been licensed by Anjouan's Offshore Finance Authority, which apparently operates independently from the Union's Central Bank and has licenced some 300 offshore banks, many of which appear to be shell banks.

Foreign remittances from Comorans abroad in France, Mayotte (claimed by France) and elsewhere remain the most important influx of funds for most Comorons. Until recently most remittances came via informal channels, but in 2006 Western Union established a presence to capture part of this market.

Union authorities have 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 appears Anjouan does have an AML law (the Money Laundering Prevention Act, Government Notice 008 of 2005) but reportedly the law applies to Anjouan and not to the offshore entities it licenses. Little is known about: (i) the procedures that have been established to review and approve offshore licenses issued before the