United Nations S/2006/69

Security Council

Distr.: General
3 February 2006

Original: English

Letter dated 31 January 2006 from the Chairman of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council

The Counter-Terrorism Committee has received the attached fourth report from the United States of America submitted pursuant to paragraph 6 of resolution 1373 (2001) (see annex).

I would be grateful if you could arrange for the present letter and its annex to be circulated as a document of the Security Council.

(*Signed*) Ellen Margrethe **Løj**
Chairman
Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism

06-23516 S (E) 080506

0623516

Annex

Letter dated 26 January 2006 from the Permanent Representative of the United States of America to the United Nations addressed to the Chairman of the Counter-Terrorism Committee

I am pleased to respond to your letter, dated 21 October 2005, on behalf of the Counter-Terrorism Committee. That letter asked the United States to follow up its third report to the Committee, dated 1 April 2004. Enclosed please find the fourth report of the United States to the Counter-Terrorism Committee (see enclosure).

The United States looks forward to continued cooperation with the Committee.

(*Signed*) John R. **Bolton**
Permanent Representative

Enclosure

Response of the United States to the Counter-Terrorism Committee, 26 January 2006

Security Council Resolution 1373 (2001)

Question 1.2

The Committee notes the extensive measures applicable to persons and organizations which provide support to designated "foreign terrorist organizations" under United States law, including the application of criminal sanctions and the freezing of assets. Does the United States have any plans to broaden the concept used in its domestic law to include all terrorist organizations, regardless of their country of origin and of where their terrorist intentions are directed?

An entity's being designated as a "Foreign Terrorist Organization" (FTO) under Section 219 of the Immigration and Nationality Act (INA) results in significant legal ramifications:

1. It is unlawful for a person in the United States or subject to the jurisdiction of the United States to knowingly provide "material support or resources" to a designated FTO. (The term "material support or resources" is defined in 18 U.S.C. § 2339A(b)(1) as "any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials." 18 U.S.C. § 2339A(b)(2) provides that for these purposes "the term 'training' means instruction or teaching designed to impart a specific skill, as opposed to general knowledge." 18 U.S.C. § 2339A(b)(3) further provides that for these purposes the term 'expert advice or assistance' means "advice or assistance derived from scientific, technical or other specialized knowledge.")

2. Representatives and members of a designated FTO, if they are aliens, are inadmissible to and, in certain circumstances, removable from the United States (see 8 U.S.C. §§ 1182 (a)(3)(B)(i)(IV)-(V), 1227 (a)(1)(A)).

3. Any U.S. financial institution that becomes aware that it has possession of or control over funds in which a designated FTO or its agent has an interest must retain possession of or control over the funds and report the funds to the Office of Foreign Assets Control of the U.S. Department of the Treasury. Because of these significant ramifications and the extensive detailed evidence needed to support the administrative record demonstrating that the statutory criteria for designation have been satisfied, the United States must prioritize its designations of Foreign Terrorist Organizations and use its resources to target the most significant groups.

Country of origin is only one factor that the USG takes into account in determining whether an organization is considered “foreign” for the purposes of designation. Other important considerations include the location of the group’s activities, leadership, and sources of material support. Similarly, a group can be designated as a Foreign Terrorist Organization if its activities threaten the security of U.S. nationals or the national security (national defense, foreign relations, or the economic interests) of the United States, regardless of where its terrorist intentions are directed.

The United States does not intend to expand the INA to allow for designation of domestic organizations. Currently, however, all organizations designated as Foreign Terrorist Organizations under the INA are also designated under Executive Order (EO) 13224. EO 13224 applies to all persons (whether foreign or domestic) determined (i) to be owned or controlled by, (ii) to act for or on behalf of, or (iii) to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, either (a) acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy or economy of the United States, or (b) any person previously designated under the EO.

Economic sanctions imposed upon entities designated pursuant to EO 13224 are broader than those imposed on entities designated solely under the INA. Designation pursuant to EO 13224 subjects all property – not just the financial assets – of designated persons to blocking measures, and U.S. persons are prohibited from transacting or dealing with designated persons. The International Emergency Economic Powers Act, pursuant to which EO 13224 was issued, also provides for both civil and criminal penalties for its violation (i.e., transacting with designated persons). Willful violations are subject to criminal penalties of up to ten years’ imprisonment and a fine. Taken together, the INA and EO 13224 comprise a comprehensive regime providing for

criminal prosecution and economic sanctions against terrorists and their supporters, both foreign and domestic.

Question 1.3

The Committee notes the United States' explanation that organizations which target other States would be likely to 'easily meet the threshold level of threat' to its own security and thus to be classified as a "foreign terrorist organization" under Executive Order 13224 or EO 12947 (second report page 8). Has any such group been so classified to date?

The United States has designated several such groups, including Armed Islamic Group (GIA), Asbat al-Ansar, Aum Shinrikyo, Basque Fatherland and Liberty (ETA), Continuity Irish Republican Army, HAMAS (Islamic Resistance Movement), Harakat ul-Mujahidin (HUM), Kahane Chai (Kach), Kongra-Gel (KGK, formerly Kurdistan Workers' Party, PKK, KADEK), Lashkar-e Tayyiba (LT) (Army of the Righteous), Liberation Tigers of Tamil Eelam (LTTE), National Liberation Army (ELN), Palestinian Islamic Jihad (PIJ), Popular Front for the Liberation of Palestine (PFLF), PFLP-General Command (PFLP-GC), Real IRA, Salafist Group for Call and Combat (GSPC), Shining Path (Sendero Luminoso, SL), and the United Self-Defense Forces of Colombia (AUC).

Question 1.4

The Committee notes the categories of institutions required to report under the Banking Secrecy Act and associated Federal regulations and the expanded nature of these categories pursuant to the issued Final rules as listed in the website of the Financial Crimes Enforcement Network of the United States Department of the Treasury (www.fincen.gov/reg_bsaregulations.html). How many suspicious transaction reports (STRs) are generated annually? What has been the outcome of investigations into these STRs? Have any prosecutions been initiated as a result of these investigations?

In the United States, a Suspicious Activity Report or SAR form is used to track suspicious transactions and activities. According to the latest information available, 507,217 SARs were reported to the U.S. Treasury Department's Financial Crimes

Enforcement Network (FinCEN) in 2003; in 2004, SAR filings increased to 689,414. Although final figures for 2005 have not been released, the 2005 figure for SARs filed is expected to meet or exceed the 2004 figure. See FinCEN: SAR Activity Review—Trends, Tips, Issues (Issue 9, October 2005).

SARs (or STRs) are a critical tool in conducting financial investigations of all types. SARs can be used proactively to start an investigation or after a financial investigation begins, either to support the ongoing investigation by confirming existing information or to identify new leads or investigative avenues. Because financial investigations are complicated and often time consuming, it is difficult to quantify the correlation of SARs – particularly individual SARs – to investigations and prosecutions.

Nevertheless, FinCEN periodically provides highlights of significant cases and prosecutions in which SAR information played a critical role. Recent cases highlighted by FinCEN demonstrate the utility of SARs in a wide variety of law enforcement investigations, cases, and prosecutions. Public accounts of such investigations and prosecutions include: “Operation Chequemate” (International Financial Fraud), “Business Accused of Structuring” (evading reporting requirements), “Suspicious Activity Report Leads to Conviction of Chief Executive,” Suspicious Activity Report Initiates Bank Failure Investigation,” “Identity Thief Receives Nearly 4 Years in Prison,” “Former Executive in Prison for Tax Evasion,” “Attorney Sentenced to Fraud Case,” and “Money Laundering Scheme Transferred over $12 Million to South American Countries,” available at the FinCEN website, http://www.fincen.gov/sarreviewissue9.pdf or http://www.fincen.gov/le_success_stories.html.

Question 1.5

The Committee notes that the United States provided information on its implementation of the Financial Action Task Force (FATF) recommendations after its second FATF mutual evaluation. The Committee would welcome further information on how the United States has implemented FATF's Nine Special Recommendations on Terrorist Financing.

The United States is currently undergoing its third round FATF Mutual Evaluation, which will be completed and approved by the FATF Plenary this year. This third round evaluation will discuss the U.S. implementation of the Nine Special Recommendations in detail. The information below highlights some U.S. efforts at compliance with the Special Recommendations. A more detailed analysis will be available at the conclusion of the mutual evaluation.

Together with our counterparts in the FATF, the United States Department of the Treasury has covered tremendous ground since 9/11 in developing international standards to combat terrorist financing, building from the international community's experience in combating money laundering. These standards have mobilized the international community to take action on important terrorist financing issues such as: freezing terrorist-related assets; regulating and monitoring alternative remittance systems; ensuring accurate and meaningful originator information on cross-border wire transfers; and protecting non-profit organizations from terrorist abuse. The FATF 40 + 9 represent a comprehensive framework for combating money laundering and terrorist financing and **the U.S. regards itself as in full compliance with the FATF Special Recommendations on Terrorist Financing (SRs).**

Special Recommendation IX, which took effect in October 2004, calls on countries to set cross-border currency reporting requirements and confiscate funds transported in violation of such requirements, including funds related to terrorist financing and money laundering. To implement **SR IX**, U.S. authorities developed a list of "red flag" indicators to aid border control authorities in detecting cash couriers and provided training on using the list through bilateral and multilateral workshops. Given the cross-border nature of **SR IX**, the U.S. encourages other countries to adopt and implement the recommendations in the immediate term.

On non-profit organizations, the U.S. Treasury Department first released the *Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities* ("Guidelines") in November 2002. In November 2005, Treasury revised these

Guidelines, based on extensive review and comment by public and private sector interested parties, to improve the utility of the Guidelines in protecting the sector from abuse by terrorists and their support networks. The Guidelines further enhance awareness in the donor and charitable communities of the kinds of practices that charities may adopt to reduce the risk of terrorist financing. These Guidelines, as presented by Treasury, are voluntary and do not supersede or modify current or future legal requirements applicable to all U.S. persons, including non-profit institutions. Rather, the Guidelines are intended to assist charities in developing a risk-based approach to guard against the threat of diversion of charitable funds for use by terrorists and their support networks. The U.S. encourages other countries to adopt similar guidance for the non-profit sector to ensure compliance with **SR VIII.**

U.S. financial institutions, under the "Travel Rule," are required to include full originator information on all wire transfers, domestic and international, above $3,000, bringing the U.S. in compliance with SR VII. The U.S. has participated in FATF's on-going discussions on implementation of **SR VII**, including reducing the threshold to $1,000.

The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) is working with other offices within Treasury, the IRS and, increasingly, law enforcement in an effort to comply with **SR VI** by better identifying money services businesses operating underground, whether intentionally or ignorantly. For example, FinCEN is working with the IRS and law enforcement to develop "red flags" for legitimate financial institutions to help FinCEN identify money services businesses that choose to operate outside the regulatory regime. This builds on FinCEN's prior work to educate the financial community about alternative remittance systems in Advisory 33, issued in March of 2003. While it is theoretically possible for these systems to operate wholly outside of the banking system, it is not often the case. Instead, such systems often utilize an account within the formal banking system to clear and settle transactions internationally. By providing U.S. banks and other financial institutions with red flags and other indicia of such clearing accounts, they will be better able to assist in identifying systems operating outside of the regulations. FinCEN has worked on a variety of international initiatives not only to educate other jurisdictions about the need for a comprehensive regulatory regime, but also to learn from the experience of other jurisdictions as they attempt to address the problem of underground value transfer.

The United States has worked diligently to implement **SR III** by: (i) identifying and designating terrorists and support structures related to all terrorist organizations (including those parties designated by the UN 1267 Committee and related to al Qaeda,

Usama bin Laden, and the Taliban); (ii) prohibiting U.S. persons from having dealings with these designated parties; and (iii) requiring that U.S. persons freeze assets related to these designated parties and report these actions to the Department of the Treasury's Office of Foreign Assets Control (OFAC). These actions, taken under the authority of EO 13224, effectively fulfill the U.S. obligations to target, designate, and implement financial sanctions against terrorists, terrorist organizations, and terrorist supporters in accordance with UNSCR 1373 and the UNSCRs related to UNSCR 1267. In addition, Section 806 of the USA PATRIOT Act (Patriot Act), enacted two months after the 9/11 attacks, amended the authority in 18 U.S.C. § 981(a)(1) to include a new subparagraph (G), which made the terrorist-related property subject to civil forfeiture.

The Patriot Act contains an entire title devoted to financial issues – many of which are aimed at strengthening and expanding the reach of the Bank Secrecy Act and serves many of the goals of the FATF Special Recommendations. For example, Section 314 of the Patriot Act represents a good example of how effective information sharing can be facilitated through legislation. Section 314 authorizes the U.S. Government to share information with and within its financial sector; that is, both vertically – between the government and the industry – and horizontally – providing a safe harbor that allows industry members to share with each other. The Treasury Department has implemented this section by creating a "pointer" system for law enforcement. The system gives the appropriate authorities, in the right circumstances, the ability to work with FinCEN to transmit the names of persons of interest to the financial sector to determine whether those institutions possess any relevant transaction or account information. If there are any "hits," law enforcement can then follow up with a subpoena to obtain specific information.

U.S. law enforcement has consistently reinforced the fact that relevant information collected from financial institutions is critical to understanding, detecting, investigating, prosecuting, and deterring terrorist financing and financial crimes. For example, U.S. law enforcement authorities have reported that over 88,000 Currency Transaction Reports and Suspicious Activity Reports filed have been relevant to terrorism investigations.

The Patriot Act has also provided us with the benefits derived from Sections 313 and 319, both of which are aimed at preventing money laundering and terrorist financing through correspondent accounts maintained by U.S. banks and securities brokers on behalf of foreign banks. Specifically, Section 313 helps make America safer by expressly prohibiting shell banks from participating in the U.S. financial system and insisting upon strict record keeping regarding the ownership of each non-U.S. bank that

maintains a correspondent account with a U.S. institution. Section 319 allows the U.S. to seize criminal assets through interbank accounts when foreign bank secrecy laws prevent law enforcement cooperation.

Certain Patriot Act provisions and the Bank Secrecy Act provide valuable anti-money laundering/countering terrorist financing (AML/CFT) tools to both financial institutions and the government. However, establishing a framework of rules and regulations is only the first step. Another primary goal is to use the information gleaned from effective AML/CFT systems to freeze illicit assets, shut down channels used to transfer funds, form prosecutions against terrorist financiers or financial criminals, and deal other blows that make it costlier, riskier, and less efficient for the ill-intentioned to move their assets. A vital component of this effort, we have found, must be the application of targeted financial sanctions.

Endorsed by the United Nations through UN Security Council Resolutions (UNSCR) 1373 and 1617, targeted financial sanctions are preventive measures quite different from criminal or regulatory action. These endorsements are an acknowledgment that countries need the ability to move without delay to deprive terrorists of resources that may lead to terrorist attacks, and that those who provide financial support to terrorists must be isolated from our financial systems immediately, separate from any efforts to prosecute them criminally.

Question 1.6

The Committee notes that in recent years, there has been considerable reorganization of United States departments and agencies dealing with counter-terrorism and that new initiatives have been taken in order to provide for cross-agency sharing of information and coordination. The committee would be grateful to receive more information on the implementation of these initiatives. In particular, how are they meeting the challenge of providing coordination across the various departments and agencies involved in combating terrorism?

With the 2003 merger of 22 agencies to create the Department of Homeland Security (DHS), the United States Government underwent its largest reorganization in over 50 years. Among the key reforms were the creation of the Director of National Intelligence (DNI) and the establishment of the National Counterterrorism Center (NCTC).

The DNI serves as the President's chief intelligence advisor and oversees the entire Intelligence Community, closely coordinating efforts and resources among the U.S. Government's 15 intelligence agencies. NCTC, established in December 2004, serves as a multi-agency intelligence fusion center, integrating and analyzing all intelligence pertaining to terrorism. NCTC also develops and coordinates strategic operational planning that takes into account the intelligence input of all agencies and departments, and utilizes the capabilities and authorities of all agencies and departments. The National Security Council coordinates the development of policy.

Legal obstacles to the ability of federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI), to share with the intelligence community information generated during a criminal investigation have been removed. A number of new law enforcement bodies have been created to meet the needs of the global war on terrorism. In 2003, the Terrorist Screening Center (TSC) was established to consolidate terrorist watchlists and provide around-the-clock support for law enforcement in the United States and around the world. The National Joint Terrorism Task Force (NJTTF) was established to enhance communication, coordination, and cooperation among federal, state, local, and tribal law enforcement communities.

The U.S. National Targeting Center (NTC) screens travelers and cargo destined to the U.S. to identify persons or shipments that may pose a high risk for terrorism. The NTC works closely with other federal agencies, including the TSC, to identify and process any watchlisted persons in coordination with those agencies.

The USG has also begun to harmonize databases and procedures across law enforcement, intelligence, and homeland security departments and agencies to facilitate information sharing. The President has named a Program Manager for Information Sharing and directed the development and implementation of an Information Sharing Environment that links federal, state, and local governments, the private sector, and potentially eventually foreign partners to facilitate cooperation and collaboration in responding to the challenges of terrorism.

Question 1.7

In its third report, the United States reported that new legislation and regulations mandating the submission of all manifest information electronically had yet to be adopted (third report, p. 21). Has there been any progress in this area?

On December 5, 2003, U.S. Customs and Border Protection (CBP) published rules required by the Trade Act of 2002, mandating the submission of advanced electronic data on all shipments entering and leaving the United States. The rules address the operational requirements for submitting and collecting advanced cargo information electronically to identify high-risk shipments that could threaten the safety and security of the United States.

In collaborating closely with the trade community to formulate CBP's strategy for implementing the Trade Act, CBP, working with importers, brokers, carriers, and exporters, has transformed the way CBP processes trade, and enabled CBP to realize a new level of supply chain security and efficiency.

Under the 24-hour rule and subsequently the Trade Act, sea carriers and automated non-vessel-operating common carriers are required to provide CBP with detailed descriptions of the contents of sea containers bound for the United States 24 hours before the container is loaded on board a vessel.

As a part of the Container Security Initiative (CSI), the United States is entering into partnerships with other governments to target and inspect high-risk sea containers in foreign ports, before they are shipped to the United States. An essential element of CSI is the advance electronic transmission of vessel cargo information to Customs. Analysis of the cargo information prior to lading enables overseas Customs personnel to identify high-risk containers effectively and efficiently, while ensuring prompt processing of lower risk containers. As of December 2002, the 24-hour advance reporting requirement has been in effect nationwide for all providers of sea cargo information.

Implementation of the Trade Act for rail carriers was phased in through three timeframes between July and October 2004, and required manifest information two hours prior to the conveyance's arrival to the United States. As is the case across all modes of transportation, the focus is on the timely filing of accurate trade data that identifies the shipper, consignee, and mode dependent conveyance and trip information.

Trade Act requirements for Air Carriers and other traders in this mode, including Express Consignment Carrier Facilities (ECCF) and Container Freight Stations (CFS) took place between August and December 2004. The air implementation was approached through a regionally phased timeframe that required Eastern ports to be operational by August 2004, Central ports by October 2004, and Western ports of entry by December 2004.

Trade Act requirements at our nation's land borders are currently being phased in across three periods of time to address three border processes: Inbond, Pre-Arrival Processing System (PAPS), and Border Release Advanced Screening and Selectivity (BRASS).

The inbond programs include Customs Automated Forms Entry System (CAFES) and (QP), an Automated Broker Interface format, which were implemented between November 2004 and March 2005. The PAPS process was implemented between December 2004 and March 2005. The Brass process began implementation in December 2004 and was fully implemented by May 2005.

The approach for implementation across all ports and modes of transportation has included a time period where informed compliance was used to initiate extensive outreach efforts using various public forums including CBP websites, trade association publications, meetings, and information updates coordinated through CBP's Public Affairs office. At the completion of these efforts, enforced compliance is activated and penalties are issued for not filing advanced electronic information within the mandated filing requirements prior to arriving at the border, and/or providing incomplete information to support the necessary level of screening and targeting to identify potentially high-risk cargo.

Question 1.8

The Committee notes that the United States authorities apprehend significant numbers of persons who attempt to enter the country without lawful authority. It notes also the difficulties previously acknowledged by the United States in regulating its borders with Canada and Mexico. What progress has been made in decreasing this vulnerability by applying border controls and screening procedures? In relation to the use of lists of persons to be denied entry on grounds

of association with terrorism (such as the databases administered within the National Targeting Center) what procedures are in place to verify the information contained in such lists?

The United States has taken numerous steps to reduce vulnerabilities along its shared borders with Canada and Mexico, and has made overall strengthening of our nation's border security a top priority. To this end, the U.S. has improved existing border operations, established international partnerships, and developed new approaches to control our borders.

Even before September 11, 2001, the United States was working on the development of an entry/exit system for foreign travelers visiting our country. The efforts intensified after September 11. One of the first initiatives begun was the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program.

Through the US-VISIT Program, the Department of Homeland Security (DHS) has intensified the screening of international travelers arriving at our ports of entry. US-VISIT has been deployed to 115 airports, 15 seaports, and 154 land border crossings across the country. The US-VISIT program is part of a continuum of security measures that begins outside our nation's physical borders. The program is a critical component of DHS's strategy to prevent terrorist attacks on the U.S. and facilitate the movement of legitimate travel and trade. US-VISIT represents a major achievement in creating an integrated border screening system that enhances our nation's security and our efforts to reform our immigration and border management systems. Through US-VISIT, DHS has increased its ability to manage the information collected about foreign visitors during the pre-entry, entry, status management, and departure processes. The backbone of the US-VISIT Program is the use of biometrics (fingerprints and digital photos) to verify the identity of known international travelers. Between January 2004 and December 2005, more than 45 million visitors have been processed through US-VISIT biometric procedures with no impact on wait times. During this same period, DHS has intercepted more than 980 known criminals and immigration law violators based on biometrics alone at our ports of entry.

In March 2005, the U.S., Canada, and Mexico announced the Security and Prosperity Partnership of North America (SPP), a trilateral commitment to keep our common borders closed to terrorists and open to legitimate trade and travel. The security pillars of the SPP focus on developing a plan to prioritize future port of entry related

infrastructure improvements, to strengthen information sharing related to terrorists and criminals, and to establish compatible standards for traveler and cargo screening. Through the SPP, we have established plans to develop and implement compatible screening methods for goods and cargo prior to departure from a foreign port and at the first port of entry into North America. Additionally, the SPP member countries will test technology and make recommendations to enhance the use of biometrics in screening travelers destined to North America with a view to develop compatible biometric border and immigration systems.

To further secure the U.S. borders, in November 2005 the U.S. announced the Secure Border Initiative (SBI), a comprehensive strategy to gain operational control of the U.S. borders. SBI will address these challenges with an integrated mix of increased staffing, more robust interior enforcement, greater investment in detention technology and infrastructure, and enhanced coordination on federal, state, local, and international levels. Under SBI, the U.S. has implemented a “catch and remove” policy to ensure detention and removal of all non-Mexican illegal aliens apprehended at the U.S. border; expanded its Expedited Removal (ER) program throughout its southern border as well as the number of countries whose nationals will be subject to ER, which cuts their detention time in half; authorized the completion of a fence near San Diego, California; expanded the use of military-proven technologies like the Unmanned Aerial Vehicles (UAV), Stryker, and sensors; and increased the frequency of deportation flights. This strategy is further supported by the deployment of 1,000 additional U.S. Border Patrol agents and the placement of 2,000 new detention beds.

SBI builds on the Arizona Border Control (ABC) Initiative, which establishes federal, state, and local coordination efforts to achieve operational control of the Arizona border and support the priority mission of anti-terrorism, detection, arrest, and deterrence of all cross-border illicit trafficking. The second phase of the ABC Initiative includes an additional 534 U.S. Customs and Border Protection agents permanently assigned to the Arizona border, a 25 percent increase. These agents were supplemented by 200 agents and 23 aircraft temporarily assigned to the Tucson, Arizona sector. The initiative, coupled with Operation ICE Storm, an anti-human smuggling initiative, has resulted in more than 350 smugglers prosecuted in total, millions in illicit profits seized, and a significant decrease in homicides, according to local authorities.

In order to consolidate terrorist watch lists and provide around-the-clock operational support for Federal and other government law-enforcement personnel across the U.S.

and around the world, the government created the Terrorist Screening Center (TSC). The establishment of the TSC ensures that government investigators, screeners, officers, and agents are working with the same unified, comprehensive set of information about potential terrorist threats. Moreover, the U.S. National Targeting Center (NTC) screens travelers and cargo destined to the United States to identify persons or shipments that may pose high risk for terrorism. The NTC works closely with other federal agencies including the TSC, which produces the National Terrorist Watch List, to ensure that any watch-listed persons are fully identified and processed in coordination with those agencies. Through these means, U.S. border enforcement officials can cross-reference and search information stored in numerous governmental databases for the purposes of confirming the identity of a traveler, determining whether or not the traveler may pose a security risk to the United States and then, as appropriate, assisting in the coordination of an effective response.

Question 1.9

The Committee notes that the United States has taken measures to strengthen its aviation security and would be pleased to have any update in this area.

The United States has taken numerous measures to strengthen aviation security in the U.S. and around the world. Among those measures are improved screening of passengers, crew, and cargo at all levels. For example, the U.S. already complies with the ICAO requirement that 100 percent of hold baggage be screened. We have also moved forward expeditiously with the issuance of machine readable and biometric travel documents and expanded installation of explosive detection equipment at airports. In addition, in coordination with like-minded states, we are working to improve our defense against man-portable air defense systems (MANPADS) and improve exchange of data concerning threats to aviation.

Question 1.10

The International Civil Aviation Organization (ICAO) has recently initiated a Universal Security Audit Programme to audit all Contracting States' compliance with Annex 17 of the Convention on International Civil Aviation. Does the United

States have any difficulties in implementing Annex 17? If so, please explain the difficulties and the standards concerned.

The United States fully supports ICAO's Universal Security Audit Program (USAP). After September 11, the U.S. committed $1 million to ICAO for the establishment of the USAP and continues to give substantial funds to the program. U.S. aviation security experts have been certified by ICAO to conduct audits and we continue to contribute significant numbers of auditors to the program. We have not registered differences with ICAO standards and recommended practices (SARPS) under Annex 17.

United States international air services agreements also contain a commitment by both parties to implement ICAO air security standards.

Question 1.11

Does the United States intend to make contribution to the ICAO Plan of Action for the strengthening of aviation security, including through security audits; the provision of urgent assistance to States, training courses and a range of guidance material; and various other projects?

The United States plans to participate fully in the ICAO Plan of Action to strengthen aviation security. The U.S. Transportation Security Administration already actively participates in ICAO's Aviation Security Panel of Experts and has two individuals seconded to ICAO's Aviation Security Mechanism at no cost to the organization. Additionally, the United States is working closely with ICAO to support aviation security assistance efforts to States by providing subject matter experts for training and other purposes. The United States also provides opportunities for ICAO to train auditors at U.S. training facilities.

Question 1.12

The Committee would also be pleased to have further information on the port security measures adopted by the United States and its cooperation with other States on the Container Security Initiative (CSI).

Currently, there are 41 operational Container Security Initiative (CSI) ports in Europe, Asia, Africa, the Middle East, and North and South America. Approximately 75 percent of cargo containers headed to the U.S. originate in or are transshipped from CSI ports.

Under the Container Security Initiative, CBP has entered into bilateral partnerships to identify high-risk cargo containers before they are loaded on vessels destined for the United States. Today, a total of 24 additional administrations have committed to join CSI and are at various stages of implementation.

CSI is an accepted model of international cooperation to protect the global supply chain against terrorism. CBP's goal is to have 50 operational CSI ports by the end of 2006. At that time, approximately 90 percent of all transatlantic and transpacific cargo imported into the United States will be subjected to pre-screening.

The World Customs Organization (WCO), the European Union (EU), and the G8, support CSI expansion and have adopted resolutions implementing CSI security measures introduced at ports throughout the world.

Question 1.13

Pursuant to paragraph 2 (f) of resolution 1373 (2001), States should afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings. The Committee notes the willingness of the United States to provide such assistance, both pursuant to its mutual legal assistance treaties and outside such regimes (first report, pp.17 and 21). The Committee would like to know how many requests for assistance have been received by United States authorities in relation to the prosecution of terrorist offences in other jurisdictions, including requests for access to persons in facilities administered by the United States. In how many cases has assistance been provided? In how many cases has assistance (or portions of a request) been denied? In the latter case, on what basis has assistance been declined?

In the U.S. answer to the FATF mutual evaluation questionnaire, the U.S. Department of Justice's Office of International Affairs provided the following statistics on mutual legal assistance (MLA) in terrorism cases:

Incoming MLA requests related to financial transactions with terrorists or their supporters
Granted – 17
Other – 2 (includes assistance no longer needed)
Pending – 18
Total: 37

Outgoing MLA requests related to financial transactions with a country designated under US law as a sponsor of terrorism or with a person or entity designated as a terrorist or supporter of terrorism under US law
Granted – 44
Denied – 2 (grounds include lack of dual criminality)
Pending – 67
Other – 20 (includes canceled, partially granted and withdrawn)
Total: 133

Incoming extradition requests related to financial transactions with a country designated under US law as a sponsor of terrorism or with a person or entity designated as a terrorist or supporter of terrorism under US law

0

Outgoing extradition requests related to financial transactions with a country designated under US law as a sponsor of terrorism or with a person or entity designated as a terrorist or supporter of terrorism under US law
Granted – 2 (includes deportation)
Denied – 2 (includes double jeopardy)
Pending – 7
Other – 4 (includes deceased person, located/arrested in another country, and withdrawn)

Total – 15

Question 1.14

The Committee notes the stringent restrictions on the right of non-immigrant aliens to own firearms. It notes also the existence of a variety of restriction on the right of United States citizens and aliens to own firearms (third report, pp. 27-28). What procedures have been put in place to ensure that firearms are not transferred from their lawful owners to others?

A U.S. citizen or legal alien must not fall into any of the nine prohibited categories under the Gun Control Act, 18 U.S.C. § 922(g) (discussed in the response to question 1.10 of the third report of the United States to the Counter-Terrorism Committee, dated April 15, 2004). A purchase by a felon, or an individual with a misdemeanor crimes of domestic violence conviction, is prohibited under the GCA. Second, if the individual is purchasing the firearm from a Federal firearms licensee (FFL), the individual must execute Form 4473 of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) of the U.S. Department of Justice, and successfully undergo a National Instant Criminal Background Check System (NICS) check by the Federal Bureau of Investigation (FBI). As discussed above, this background check involves checks of immigration and terrorist databases. Third, Ruling 2004-1 requires that alien purchasers show that they have resided in a State continuously for at least 90 days immediately prior to the FFL conducting the NICS check. If an alien leaves the United States, the 90-day period stops; it restarts when that person renters the United States. The NICS check of the database of U.S. Immigration and Customs Enforcement (ICE) will show whether a non-immigrant alien has entered or exited the United States in the last 90 days. If there is evidence that a non-immigrant alien has entered or exited the country in the last 90 days, NICS will tell the FFL to cancel the transaction.

Nonimmigrant aliens generally are prohibited from possessing or receiving (purchasing) firearms and ammunition in the United States or from taking possession of a firearm in the United States. There are exceptions to this general prohibition as follows:

> If a person is an official of a foreign government or a distinguished foreign visitor who has been so designated by the Department of State and will possess the firearm in his or her official capacity; or

If a person is a foreign law enforcement officer of a friendly foreign government entering the United States on official law enforcement business; or

If a person is admitted to the United States for lawful hunting or sporting purposes and is in possession of a valid hunting license or permit lawfully issued in the United States; or

If a person who has received a waiver from the prohibition from the U.S. Attorney General.

Significantly, even if a nonimmigrant alien falls within one of these exceptions, the nonimmigrant alien cannot purchase a firearm from an FFL unless he or she can provide the FFL with documentation showing that he or she has resided in a State within the United States for 90 days prior to the firearms transaction. (For handguns it must be the State where the alien buys the handgun.)

If a person is not eligible to purchase a firearm from an FFL to possess in the United States, they may not have someone who is eligible purchase one for them.

If any of the preceding prohibitions are violated the violator can receive a maximum of five or ten years of imprisonment, depending on the violation.

Importers of handguns, rifles, and shotguns are required to declare the weapons and to have a permit (ATF-6 form) from ATF prior to their import, export or transit. The transit and export of handguns and rifles requires either a Department of State license or license exemption for each shipment, and the Shipper’s Export Declaration must be presented to CBP citing the license or license exemption. Violations of the regulations may result in the seizure of the weapons or further legal action.

With respect to importation of firearms by aliens, on February 5, 2002, ATF published a rule requiring non-immigrant aliens bringing firearms and ammunition into the United States for hunting or sporting purposes to obtain an import permit from ATF. In the interest of national security and public safety, ATF now requires non-immigrant aliens to obtain import permits for all importations of firearms and ammunition into the United States. Non-immigrant aliens who wish to import firearms and ammunition must submit to ATF an ATF Form 6NIA, Application and Permit for Temporary Importation of Firearms and Ammunition by Non-immigrant Aliens. The Form 6NIA

requires alien applicants to list identifying information, including their ICE alien or admission number.

The original ATF-6 form must be presented to CBP at time of import and the exporter must present an original license and file the Shipper's Export Declaration for the export against that license. Additionally, CBP receives a download nightly of all licenses issued by the Department of State.

The United States continues to strengthen security measures concerning the import, export, and transit of firearms. Persons engaged in the business of importing firearms must first apply and be granted a license as an importer of firearms under the GCA. Any person, including a licensed importer, who wishes to import firearms must also obtain an approved import permit (Form 6) from ATF as discussed above. The Form 6 requires the applicant to list their name and address, as well as that of the broker, the foreign seller and any foreign shipper. The Form 6 requires specific information about the firearms to be imported, including serial number. Importers must also be registered pursuant to the Arms Export Control Act, 22 U.S.C. § 2778 (AECA). The export provisions of the AECA are administered by the United States Department of State. To export firearms, persons must first obtain a valid export license from the State Department under the AECA.

Question 2.2

The Committee's Directory of Assistance (www.un.org/sc/ctc) is frequently updated to include new relevant information on available assistance. The Committee takes note of the fields of technical assistance in which the United States has provided training to other States and would welcome an update concerning the United States capacity to provide ongoing assistance.

Since the United States last provided updated information for the Committee's Directory of Assistance, the United States has developed a number of important training initiatives. For example, in the area of Counterterrorist Finance Training, the United States has recently developed training programs addressing bulk cash smuggling and terrorist abuse of charities. These new training programs are designed to assist foreign partners in enhancing their ability to implement FATF Special Recommendations 8 and 9 and to meet other relevant international standards.

The United States government is currently undertaking a government-wide review and compilation of CT training initiatives currently underway. The United States will provide this updated information to the Committee as soon as its review is complete. The United States remains committed to providing CT training and working with foreign partners to increase global capacity to combat terrorism. Unfortunately, due to limited resources and training personnel, it is sometimes prevented or delayed from providing training requested by foreign partners.