TESTIMONY TO THE JOINT CONGRESSIONAL INTELLIGENCE COMMITTEE INQUERY
October 1, 2002
by
Ambassador Francis X. Taylor
Coordinator for Counterterrorism
Department of State

Mr. Chairman, Committee members:

I would like to begin by thanking you for this opportunity to discuss an issue of vital importance to America's efforts to combat terrorism, and that is, the way we share terrorist-related information within the U.S. government. Information is a key weapon in the global war on terrorism. Having timely and accurate intelligence is essential to disrupt terrorist activity and dismantle terrorist infrastructure. Information is also one of America's key defenses to deter threats and prevent terrorist acts before they happen. It is in its unique offensive and defensive capacities that having access to intelligence and analysis proves critical to fighting terrorism.

I am accompanied today by a wide range of experts from our department. We share in your interest to improve those systems which are designed to ensure that all levels of our government receive critical information necessary to defend America's interests at home and abroad. We owe it to the thousands of innocent Americans who lost their lives nearly a year ago to better these systems, and we look forward to continuing to work with you to do this.

I have served as the State Department's Coordinator for Counterterrorism since July 2001. I will never forget the chilling call I received at my desk on September 11: two planes had struck the World Trade Center towers. America and the world would never be the same. A call soon after from Deputy Secretary of State Armitage summoned me to the State Department's Operations Center, beginning a non-stop effort to help coordinate the U.S. government's response to the attacks.

Without the constant flow of up-to-the-minute data and analysis from the Intelligence Community, we would not have been able to provide the President, Secretary Powell, and other senior leaders the vital information they needed to formulate a coordinated response. I take my hat off to the

many unsung heroes within the Intelligence Community and our government, who overcame their personal suffering and dedicated themselves to their work, providing the best intelligence and analysis possible given the difficult circumstances. The relationships forged in those harrowing days has not waned between many State Department employees, myself included, and our friends and colleagues in other agencies in the Intelligence Community.

The Office of the Coordinator for Counterterrorism serves as the lead for coordinating international counterterrorism policy within the U.S. government and with foreign governments. The Office of the Coordinator is a major intelligence consumer, rather than an intelligence producer, and our mission depends on the timely and efficient flow of information on terrorism and terrorist threats. One of our objectives therefore is to enhance the sharing of threat and other counterterrorism intelligence between our government and the many other governments around the world that are contributing to the global war on terrorism. We monitor and analyze information, but are not directly involved in the mechanisms and infrastructure through which data is shared within and between agencies. So, I may have to refer to my colleagues here from other bureaus such as Intelligence and Research and Consular Affairs on any detailed questions.

INTERNATIONAL EFFORTS

I would like to emphasize that we at the Department of State are working aggressively with our fellow agencies and international partners to detect, deter, and disrupt terrorist activities around the world. And when terrorist attacks occur, we work cooperatively with intelligence and law enforcement agencies to track down and seek the arrest, extradition, or prosecution of the perpetrators.

A key aspect of these activities is intelligence sharing. For example, since the attacks of September 11, the Department has worked hard to step up U.S. government and international efforts to cut off the funds that terrorist organizations such as al-Qa'ida need to survive. This requires substantial sharing of information and intelligence with many countries.

Again, I would reiterate that as an institution our mission depends on effective and timely information sharing. Consequently, we are very supportive of efforts to improve the processes involved and it is the Department's policy to support and seek expansion of our intelligence sharing capacity.

SHARING INFORMATION

Taking up the questions you raised in your letter of invitation, I would note that in addition to the daily telephone and in-person contacts with our colleagues in other agencies, there are several processes and procedures in place at the State Department to receive terrorism-related information from the intelligence community and law enforcement organizations.

The State Department and its overseas posts are integrated into both classified and unclassified electronic communications networks used by other federal agencies, and the State Department both receives and transmits information on terrorism directly through those channels. Additionally, the Bureau of Intelligence and Research (INR) receives terrorism-related sensitive classified intelligence reports from other intelligence community components through dedicated communications, including INTELINK, a web-based communications medium. This data sharing follows the policies and procedures established by the Director of Central Intelligence for the handling of classified intelligence material.

In 1987, the State Department established the TIPOFF program for the purpose of using biographic information drawn from intelligence products for watchlisting purposes. In 1993, we established the Visas Viper program as a dedicated telegraphic channel for reporting information on known and suspected terrorists directly to the TIPOFF staff. The Viper channel is used both by our posts overseas and by intelligence agency headquarters in Washington, and can accommodate multiple addressees to facilitate information sharing among users.

In addition to receiving information through the Viper channel, TIPOFF draws from all sources the information it uses to watchlist terrorists. Independently from TIPOFF, the Bureau of Consular Affairs also receives basic biographic data directly from the FBI criminal databases -- some of which might include information about terrorists -- and feeds that information into the Consular Lookout and Support System (CLASS). All consular officers adjudicating visa applications overseas run checks against that system before issuing a visa.

The Bureau of Diplomatic Security receives information from a variety of sources. Domestically, DS receives information from other federal and local law enforcement

agencies directly at the headquarters level and through field offices. Overseas, information is acquired from host governments or other USG sources at our Missions abroad. Data arrives via correspondence, reports, reliable sources, and even untested "walk-ins." The process by which the information is received is often diverse. Once received, DS may forward its information for inclusion in TIPOFF or the CLASS system.

INTERAGENCY GROUPS

Since ramping-up our counterterrorism activities over the last year, State Department personnel have participated in -- and continue to participate in -- a number of interagency organizations and task forces. Consular Affairs is represented at the FBI's Foreign Terrorist Tracking Task Force, the Secret Service's Document Security Alliance Group, and the interagency Migrant Smuggling and Trafficking in Persons Coordination Center. The Bureau of Intelligence and Research (INR) represents the Department on the Interagency Intelligence Committee on Terrorism and the Bureau of Diplomatic Security and the Office of the Coordinator for Counterterrorism also participate in selected committee activities. The Bureau of Diplomatic Security is a member of the FBI's 19 Regional Joint Terrorism Task Forces, the National Joint Terrorism Task Force, and the Alien Smuggling Task Force.

Individual employees of the Department have also been integrated into a number of intelligence and law enforcement organizations, including INTERPOL, the Director of Central Intelligence's Interagency Intelligence Committee on Terrorism and the DCI's Counterterrorism Center, the FBI's Foreign Terrorist Tracking Task Force, the Data Management Improvement Act Task Force, and the Office of Homeland Security.

Employees from the Bureau of Consular Affairs participate in several groups working to upgrade border security through improved identification and travel documentation. These include the Federal Smart Card Working Group, the GSA Smart Card and Biometrics Group, the Interagency Working Group on Birth Certificate Standardization, and the INS Entry/Exit Working Group. Moreover, the State Department's Visa Office participates in frequent meetings and teleconferences with INS, FBI, CIA, the Social Security Administration, and other agencies to share lookout information and visa data.

State also chairs the Data Share Working Group of the Border Agency Partnership, and Visas Viper committees composed of the many agencies represented at our posts abroad work to coordinate the reporting of terrorism information to Washington and its entry into the TIPOFF system. In addition, my office hosts liaison officers from CIA's Counterterrorism Center and FBI's International Terrorist Operations Section.

These partnerships have been very effective in pursuing the United States' counterterrorism goals, and the sharing of information as it relates to these activities generally has been excellent, though there remains room for improvement. State Department personnel participating in these groups and task forces generally enjoy broad access to terrorism-related information. We offer the same access to CIA and FBI personnel in the State Department.

INFORMATION TECHNOLOGY

Terrorism-related information, especially that used for watchlisting terrorists, is shared within and outside the State Department through a variety of electronic media, in hardcopy, and by oral briefings. For example, the Department's TIPOFF watchlist program receives information electronically and feeds it directly into the Consular Lookout and Support System (CLASS), which is checked by consular officers worldwide as a mandatory step in the visa adjudication process. Under the terms of a 1991 MOU approved by the intelligence and law enforcement communities, that information is also entered into the Interagency Border Inspection System (IBIS) for use by U.S. Immigration and Customs officers at ports-of-entry. In August 2002, the entire TIPOFF database, including full biographic records on nearly 85,000 terrorist names, photos, fingerprints, and on-line source documentation, was made available on CT-LINK to authorized users from five Intelligence Community and law enforcement agencies. That information is now instantly available to those users for analytical and law enforcement purposes.

The State Department Bureau of Intelligence and Research (INR) manages web pages available to other members of the Intelligence Community on two web sites - one classified at the SECRET level, and one at the TOP SECRET level. Every day, INR loads intelligence reports known as "INR Assessments" and other finished intelligence publications onto those sites. Most Assessments are published on INTELINK within 24 hours of production and

approval. All INR products on counterterrorism loaded onto the TOP SECRET site appear on a dedicated page called "September 11 and Aftermath - The War on Terrorism." INR does not maintain a similar page on the SECRET website because of resource constraints. INR web pages on both systems are indexed by date, country of interest, and product series for user convenience.

The State Department's Bureau of Consular Affairs (CA) is an innovator in the use of information technology to facilitate information sharing, and uses advanced information technology to make visa lookout information, including terrorist lookouts, available to consular officers around the world on a real time basis. The Consular Lookout and Support System (CLASS) uses sophisticated search algorithms to match lookout information to individual visa applicants. CLASS check is mandatory, and the system will not print a visa until the consular officer has checked and resolved "hits" of the applicant's bio-data against the lookout system data. CLASS records doubled after 9/11. Consistent with the requirements of the USA Patriot Act, more than 7 million names of persons with FBI criminal and other name-retrievable records were added to CLASS by August 2002, augmenting 5.8 million name records from State, INS, DEA, and intelligence sources.

In addition to the watchlist information contained in CLASS, the State Department greatly expanded the types of non-lookout data shared with INS following 9/11. Much of the bio-data and photos concerning individual visa cases are replicated in CA's Consolidated Consular Database (CCD) and are shared with INS. The CCD contains records of the past five years' nonimmigrant visa issuances and denials, most including photos. CCD is accessible at all consular posts and is updated from around the world every 5 minutes. Records of all immigrant visa and nonimmigrant visa issuances have been available to INS on-line since January 2002, and can be accessed at most ports of entry. U.S. passport application and issuance information is captured in our Passport Files Miniaturization (PFM) system. Scanned images of passport applications are also included in a separate database connected to this system.

The Department's Bureau of Consular Affairs is working with other agencies to establish better means to share data, as well as working to establish a connection to the Open Source Information System (OSIS), an unclassified network widely used by a large number of government agencies. In connection with this latter effort, we are cooperating with other law enforcement and intelligence agencies on the best

ways to use the planned connection to provide direct access to data from the CCD. In addition, we have begun to scan visa applications in order to make images of these documents electronically retrievable. We are modifying our software to add over two dozen data fields to the NIV processing system so that this data may be more easily shared with the intelligence and law enforcement communities.

STATE AND LOCAL COOPERATION

In addition to working closely with its federal counterparts, The Department of State understands the benefits of integrating state and local law enforcement agencies into its counterterrorism activities, in accordance with applicable law and regulations. The Bureau of Diplomatic Security has 21 offices in the United States, each having liaison responsibility with state and local law enforcement on a variety of law enforcement issues, including counterterrorism. DS exchanges information among these entities on a regular basis. Domestically, DS focuses investigating passport and visa fraud and its mission to protect Department of State and international persons and facilities.

The extent to which counterterrorism information is shared by or with us is, generally speaking, is predicated on those missions and the methods vary by jurisdiction. Task forces, such as the regional Joint Terrorism Task Forces or ad-hoc task forces, may participate. DS, through its Protective Intelligence and its Protective Liaison Divisions, works with state and local law enforcement on a variety of threats against those we protect. DS participates in a variety of local law enforcement forums -- each designed to enhance communication and networking. The critical component in achieving success is that both federal and local law enforcement have a user-friendly, real time method for communicating threats and responses to terrorist related incidents.

In addition to DS, other parts of the Department are involved in efforts to share information with local and state law enforcement authorities. The INR TIPOFF program currently does not share information directly with state and local law enforcement agencies due to restrictions on disclosure of sensitive intelligence information to persons not authorized to receive it. However, an agreement was written after 9/11 that permits TIPOFF to periodically export certain declassified biographic data elements from its database under strictly controlled conditions to the

Foreign Terrorist Tracking Task Force.

Under procedures established by the DCI, classified background information may be provided to authorized FTTTF personnel for law enforcement purposes. The Foreign Terrorist Tracking Task Force has the ability to share certain declassified biographic data with authorized state and local law enforcement officers by means of the FBI's Joint Terrorist Task Forces.

The INR TIPOFF initiative is another example of the Department's efforts to responsibly maximize information sharing. Discussions with the FBI are underway which will permit a portion of the TIPOFF database to be placed in the National Crime Information Center's Violent Gangs and Terrorist Organizations File. Local law enforcement has access to that database.

OVERSEAS ACTIVITIES

Overseas, the Department also facilitates information sharing with foreign law enforcement authorities. Regional Security Officers, the Department's law enforcement officers at overseas Missions, are responsible for initiating and maintaining an open line of communication with host country law enforcement on a variety of security issues, including terrorism. Of course, the security environment and other factors dictate what method and level of information sharing is appropriate. For example, the Antiterrorism Assistance (ATA) Program may help educate foreign counterparts on the benefits and methodology of information sharing.

The information shared is based on a variety of sources, both USG and others. Its substance may have direct impact on the safety of our employees and Americans overseas. As importantly, it may impact our security at home. What remains critical in the process is that the sharing of the information cannot be considered the end use. Rather, it must be quickly and accurately vetted and applied to have any value.

LEGAL QUESTIONS

In general, the Department of State is more a recipient than a producer of information relevant to terrorist suspects. Department of State-generated information is typically derived from diplomatic sources and thus is not subject to the constraints on dissemination of law enforcement or intelligence information. In the past, the Department has not encountered significant legal barriers to sharing its own information related to terrorist suspects with other agencies. The Department of State did, however,

encounter legal barriers that precluded receiving information from other agencies. The USA PATRIOT Act made significant improvements in this area.

Executive Order 12958 (concerning classified national security information), the Privacy Act, and the Immigration and Nationality Act provide the primary legal framework relevant to the Department's sharing terrorism-related information with other agencies. The procedures most relevant to sharing information relating to terrorism concern the handling of classified information, and the restrictions on dissemination of classified information under E.O. 12958. Since the relevant persons at other federal agencies typically have security clearances, these procedures and restrictions have not generally been an impediment to providing terrorism-related information to other U.S. agencies on a need-to-know basis. Restrictions on dissemination of classified information, however, could be an issue with respect to sharing information with state and local law enforcement authorities.

In some cases, restrictions that third parties place on information they provide to the Department will affect our ability to share that information with other agencies. As E.O. 12958 requires, the Department of State cannot disclose information originally classified by another agency without obtaining authorization from that agency. Some highly sensitive information the Department receives from other U.S. agencies or that the Department generates itself cannot be distributed beyond the original addressees without the prior approval of the office that originated the information or another appropriate office. While the need to obtain approval before distributing such highly sensitive information does not, as a practical matter, preclude the Department from sharing sensitive information relating to terrorism, it does impose certain procedural hurdles that must be overcome before such sharing can take place.

The Privacy Act generally restricts disclosure of personal information about U.S. citizens and lawful permanent residents. It has not, in our experience, been an obstacle to sharing information related to terrorist suspects, at least for law enforcement purposes. It is possible in theory, however, that it could restrict disclosure in a particular case, where the information concerned a U.S. citizen or lawful permanent resident, and the disclosure was not consistent with the purpose for which the information was kept. Generally speaking, information-sharing should not be a problem in the context of a law enforcement investigation, but in the context of pure

information-gathering for intelligence purposes, the Privacy Act could present an obstacle to the sharing of such information between U.S. agencies about U.S. citizens and lawful permanent residents.

Visa records and visa record information are considered confidential and protected from disclosure under section 222(f) of the Immigration and Nationality Act (INA). Because the statute permits the Department to share such information with other USG agencies if it will be used for the enforcement of the laws of the United States, section 222(f) does not restrain our ability to share information on terrorism with other USG agencies for law enforcement purposes. Theoretically, there could be a problem if there were no link whatsoever to enforcement of the laws, but in the context of immigration that seems unlikely. In addition, section 222(f) would not prevent the Department from sharing any information relating to terrorism that the Department had received that might underlie a visa decision but be independent of the visa record itself. Further, Congress recently expanded our ability to share information protected by section 222(f) with foreign governments, and we can always share such information in discretion when a court certifies that the information is needed in the interests of justice.

Similarly, although alien registration and fingerprint records are confidential by law, such information may be made available to federal, state, and local law enforcement agencies, upon request, and to persons or agencies designated by the Attorney General.

FLOW OF INFORMATION

Finally, Mr. Chairman, we believe that the free flow of terrorism-related information within the Department of State and between the Department and other agencies is important. While the flow has not always been unfettered, we see no institutional or organization culture impediments to information sharing that cannot be successfully resolved.

Bureaus have provided a few examples of areas that need further work. Consular Affairs notes that its Fraud Prevention office has responded to an increased demand from the intelligence community since 9/11 for its information, but so far has received little data in return. There seems to be a lack of understanding within the community of what information would be useful to fraud program managers. We are working on this issue.

As noted earlier, the consular lookout system has been significantly enhanced with biodata from FBI NCIC records. Consular affairs continues to work on two related issues - getting a more comprehensive extract of specific records and obtaining access to the FBI's non-name retrievable information that may pertain to an individual visa applicant's eligibility.

Mr. Chairman, this overview ends my formal testimony. I hope this overview has been useful. If you have any questions, my colleagues and I will do our best to answer them. Thank you.