Testimony of

Gary Bald

Executive Assistant Director
National Security Branch
September 21, 2005

Statement of
Gary M. Bald
Executive Assistant Director
National Security Branch
Federal Bureau of Investigation

Before the
United States Senate
Committee on the Judiciary

September 21, 2005

Good morning Mr. Chairman, Senator Leahy, and Members of the Committee. Thank you for this opportunity to discuss the FBI's progress in enhancing information sharing with the Department of Defense (DOD), as well as other members of the Intelligence Community (IC) and our partners in law enforcement.

I am testifying today in my new capacity as Executive Assistant Director of the FBI's National Security Branch (NSB), which was established September 12 (pending Administration approval of the new organizational structure). The NSB combines the missions, capabilities, and resources of the counterterrorism, counterintelligence, and intelligence elements of the FBI. It was created in response to a directive by the President to implement the recommendations of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission). While the WMD Commission recognized that the FBI has made substantial progress in building our intelligence program, it wanted to ensure our intelligence elements were responsive to the Director of National Intelligence (DNI) and were fully integrated into the IC. The creation of a unified management structure to oversee the FBI's national security components will help ensure that NSB activities will be coordinated with other IC agencies under the DNI's leadership. We are working with the DNI to assist the Attorney General in preparing a Report to the President from the Attorney General further defining the NSB.

Information Sharing

The FBI has a dual role as both an intelligence agency and a law enforcement agency. Since the terrorist attacks of 9/11, the FBI has made great strides in strengthening our intelligence capabilities and disseminating intelligence throughout the FBI, to other members of the IC, and to our partners in federal, state, local, and tribal law enforcement. We are doing so while

protecting sensitive intelligence and investigative sources and methods, maintaining the integrity of criminal prosecutions, and safeguarding the constitutional and civil rights of the American people.

Changes since 9/11

Prior to 9/11, legal and procedural restrictions, often referred to as the "wall", were created to separate intelligence and criminal investigations. Although intelligence information, including that gathered by DOD, could be passed over the wall and shared with FBI criminal investigators, this process was subject to cumbersome procedures that limited and discouraged information-sharing.

Three significant legal developments after 9/11 affected the FBI's approach to international terrorism investigations and lowered the wall between criminal and intelligence investigations:

1. The Oct. 26, 2001, enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).

2. DOJ's March 6, 2002, issuance of Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI.

3. The Foreign Intelligence Surveillance Court of Review's Nov. 18, 2002, issuance of an opinion regarding the wall between intelligence and law enforcement.

These developments removed real and perceived barriers to coordination among the FBI and the IC, including DOD. This facilitated a fundamental change in the way international terrorism investigations are pursued by the FBI.

Among the changes are that the FBI now places great emphasis on producing Intelligence Information Reports (IIRs), Intelligence Assessments (IAs) and Intelligence Bulletins (IBs) on national security threats to our country. The reports we now produce are disseminated to our partners in the intelligence and law enforcement communities and have enhanced our contributions to the rest of the IC.

Policy

Our policy now is to share by rule and withhold by exception. As part of our efforts to ensure that this policy is implemented, we have created a senior-level "Information Sharing Policy Group" (ISPG). The FBI's Executive Assistant Director (EAD) for Administration and the former EAD for Intelligence co-chaired the ISPG. As the EAD for the NSB, I will now take a leadership role in this group, which brings together the FBI entities that generate and disseminate intelligence. Since its establishment in February 2004, this body has provided authoritative FBI policy guidance for internal and external information-sharing initiatives.
We have just completed the first installment of our new Intelligence Policy Manual. The manual implements the policies on intelligence and information sharing set forth by the President, by Congress in the Intelligence Reform and Terrorism Prevention Act, and by the DNI. One of the

key areas of focus for the manual is how to strike the proper balance between the need to share information versus the need to protect intelligence sources and methods.
Part of this guidance includes a new, comprehensive policy on "write-for-release," which will improve the ease of sharing intelligence with our partners in law enforcement and intelligence. "Write-for-release" techniques include portion marking, the use of "tearlines," and sanitizing sensitive text.
The FBI shares information and ensures collaboration through our National Information Sharing Strategy (NISS), which is part of the Department of Justice (DOJ) Law Enforcement Information Sharing Program (LEISP) that aims to ensure that those charged with protecting the public have the information they need to take action. NISS has three components: the National Data Exchange (N-DEx), which will provide a nationwide capability to exchange data derived from incident and event reports with other agencies; the Regional Data Exchange (R-DEx), which will enable the FBI to join participating federal, state, tribal, and local law enforcement agencies in regional, full-text information-sharing systems under standard technical procedures and policy agreements; and Law Enforcement Online (LEO), which provides a web-based platform for the law enforcement community to exchange information.

Interagency Efforts

The FBI also participates in a variety of interagency centers, working groups, and committees that were established to improve information sharing. For example, the FBI participates in and chairs the Justice Intelligence Coordinating Council (JICC), which was established by the Attorney General (AG) in 2004 to increase coordination among the DOJ's intelligence activities, communicate with the IC, and coordinate with law enforcement. The JICC will soon submit a report to the Attorney General on its progress toward implementing the following goals: document DOJ intelligence capabilities and resources to drive an analysis of capability strengths, weaknesses and gaps; engage in a threat-based planning process to identify common threats and prioritized intelligence needs for FY07; recommend the inclusion of Law Enforcement intelligence priorities in the National Intelligence Priorities Framework (NIPF); create new avenues for electronic data sharing with Law Enforcement and Homeland Security agencies; and introduce security, coordination, and user flexibility measures to enhance the LEISP.

The FBI also participates in the GLOBAL Intelligence Working Group and the GLOBAL Criminal Intelligence Coordinating Council (CICC), which were established in 2004 to set national-level policies to improve the flow of intelligence information among U.S. law enforcement agencies. The CICC has developed standards for the law enforcement intelligence component of Fusion Centers and Regional Intelligence Centers (RICs), which are collaborative efforts sponsored by state, local, or federal agencies. The FBI currently sponsors nine RICs, has contributed personnel to 25, and is co-located with 18 of them. The FBI is committed to developing relationships with all active RICs.

In each of the FBI's 56 field offices and in most major U.S. cities, the FBI has created Joint Terrorism Task Forces (JTTFs) to combine the resources of the FBI and other federal agencies with the expertise of state and local law enforcement agencies to prevent acts of terrorism and investigate the activities of terrorists in the United States. Nearly 150 personnel representing five DOD agencies - Defense Intelligence Agency (DIA), U.S. Army Intelligence and Security

Command (INSCOM), Air Force Office of Special Investigations (AFOSI), Defense Criminal Investigative Service (DCIS), Naval Criminal Investigative Service (NCIS), and the Coast Guard Intelligence and Criminal Investigative Program - are assigned to the 103 JTTFs that are currently in operation.

At FBI Headquarters, the FBI created the National Joint Terrorism Task Force (NJTTF), to enhance communications, coordination, and cooperation between federal, state, and local government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety and homeland security communities. Through the NJTTF, we provide a point of fusion for terrorism intelligence and support the JTTFs throughout the United States. Nine different DOD agencies are represented on the NJTTF by 10 full-time and seven part-time representatives. The NJTTF holds a daily counterterrorism intelligence briefing for all members. All JTTF and NJTTF members have access to FBI information systems (Automated Case File and Guardian), and a memorandum of understanding guides the use of material outside the JTTF and the NJTTF.

In addition, the FBI participates in the National Counterterrorism Center (NCTC) and the National Virtual Translation Center (NVTC), and intends to participate in the National Counter Proliferation Center (NCPC). NCPC was established to coordinate and oversee the Intelligence Community's efforts against proliferation of weapons of mass destruction. NCTC serves as the primary organization in the United States Government for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the United States Government. The FBI currently has 67 personnel at NCTC. NVTC serves as a clearinghouse to facilitate timely and accurate translation of foreign intelligence for all elements of the IC. The FBI is the executive agent for this interagency center.

The FBI is proud of its efforts and partnership with DOD. In an effort to support the Global War on Terrorism and information sharing initiatives, the FBI's Criminal Justice Information Services Division (CJIS), in conjunction with DOD's Biometric Fusion Center (BFC), has been working to share data collected by military troops deployed internationally. The data consists of fingerprints, photographs, and biographical data of military detainees, enemy prisoners of war, or individuals of interest as national security threats to the United States. Together, CJIS and DOD have researched and developed an Automated Biometric Identification System (ABIS). The DOD ABIS consolidates, formats, and exchanges data equivalent and consistent to the FBI's current State/County/Local law enforcement model. The ABIS provides the DOD the ability to gather, store, share, and enter the information into the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which allows the FBI to disseminate the information to other government and law enforcement agencies.

The FBI currently has Special Agents assigned as liaison officers to several DOD Combatant Commands, including Central Command (CENTCOM), European Command (EUCOM), Northern Command (NORTHCOM), Special Operations Command (SOCOM), and Joint Special Operations Command (JSOC). JSOC currently has a detailee assigned to the FBI's Counterterrorism Division (CTD) and NORTHCOM and SOCOM have detailees to the National JTTF. The FBI and the National Security Agency also have detailees assigned to each other's headquarters.

DOD and the FBI are also collaborating on the Foreign Terrorist Tracking Task Force (FTTTF), which uses analytical techniques and technologies to enable and enhance terrorist identification and tracking. The Deputy Director of FTTTF is a DOD Counterintelligence Field Activity (CIFA) employee and CIFA provides three contract analysts assigned to the FTTF. The director of FTTTF meets with the director of CIFA on a bi-weekly basis. The two agencies share data and collaborate on the development of analytical tools.

In addition, the two agencies share information as participants in the Terrorist Explosive Device Analytical Center (TEDAC), which coordinates and manages a unified national effort to gather and technically and forensically exploit terrorist improvised explosive devices (IEDs) worldwide. The FBI supports DOD's Combined Explosive Exploitation Cell (CEXC) mission with Special Agent Bomb Technician (SABT) rotations through both Iraq and Afghanistan.

Additional FBI personnel are embedded with DOD in military operations in Iraq, Afghanistan, and Guantanamo Bay, Cuba (GTMO).

In support of those operations and others, the FBI has developed the Intelligence and Terrorist Photograph Identification Database (INTREPID), a web-based repository of images and videos of individuals affiliated with terrorist organizations. More than 12,000 photos collected by the FBI and DOD in GTMO, Iraq and Afghanistan are being included in the database, which allows investigators to link vital information captured world wide, as well as create photo lineups, produce individual information photo cards, and store video clips for online retrieval. All photos of FBI's terrorism subjects are accessible to DOD through NCTC's Terrorist Identities Datamart Environment (TIDE). The entire INTREPID database is also accessible to JTTF members through the FBI's Sensitive Compartmented Information Operational Network (SCION).

Dissemination

The FBI has a responsibility to the nation, the IC, and federal, state, and local, and tribal law enforcement to disseminate relevant information. Doing so is an inherent part of our mission. Sharing FBI information will be the rule, unless sharing is legally or procedurally unacceptable.

The FBI primarily uses six information-sharing tools to disseminate its intelligence products: the FBI Intranet, INTELINK-TS, INTELINK-S, Law Enforcement Online (LEO), Homeland Security Information Network (HSIN), and Secure Automated Message Network (SAMNET).

Products up to and including the Secret level are disseminated throughout the FBI via the FBI Intranet.

The FBI uses the Intelligence Community's INTELINK-TS to facilitate sharing intelligence products up to the Top Secret /Sensitive Compartmented Information (SCI) level. INTELINK-TS is carried on the Defense Department's Joint Worldwide Intelligence Communications System (JWICS) and is known in the FBI as the SCI Operational Network (SCION). The SCION project was initiated in September 2001 and has met all schedule, budget, and performance requirements.

Information sharing with other government agencies at the SECRET level requires access to the DOD Secret Internet Protocol Router Network (SIPRNET). SIPRNET provides the communications backbone for INTELINK-S, the Secret intelligence Intranet. INTELINK-S contains classified information from more than 200 Web servers supporting the intelligence, homeland security, military, counterintelligence, and law enforcement communities.

The FBI's LEO network is a core capability for information sharing. LEO provides Web-based communications to the law enforcement community to exchange information, conduct online education programs, and participate in professional special interest and topically focused dialogue. The FBI intelligence products are disseminated weekly via LEO to its more than 40,000 users, providing information about terrorism, criminal, and cyber threats to patrol officers and other local law enforcement personnel who have direct daily contacts with the general public.

The FBI shares intelligence products posted on LEO with HSIN users as well. HSIN provides states and major urban areas real-time interactive connectivity with the Homeland Security Operations Center through a secure system carrying information on a Sensitive But Unclassified level to all users.

The FBI's SAMNET provides the capability to share Intelligence Information Reports (IIRs) within the FBI and with IC members. To convert IIRs to the proper teletype format for dissemination, the FBI uses the FBI IIR Dissemination System (FIDS) - a web-based form to create and track draft IIRs through an approval process. Eventually, the FBI Automated Messaging System (FAMS), which enables users to exchange information with more than 40,000 addresses on the Defense Messaging System, will replace SAMNET.

So far in calendar year 2005 (as of August 31, 2005), the FBI has issued 254 finished intelligence products (Intelligence Assessments and Intelligence Bulletins) on SIPRNET, 333 on INTELINK, and 149 on LEO. During the same time period, the FBI has posted 202 IIRs on INTELINK, 330 on SIPRNET, and 698 on LEO. This is a significant increase over previous years.

The primary route for DOD components to receive FBI intelligence products is through DIA, which is on the primary distribution list for all FBI intelligence products, and is responsible for forwarding them to all DOD customers that have a counterterrorism reporting requirement. The FBI also sends appropriate messages to specific DOD elements, such as NORTHCOM, and provides tearlines for sharing with partner nations. A secondary route for DOD commands to access FBI intelligence products is via the FBI SIPRNET website.

Conclusion

The FBI has made significant progress in its efforts to share information with partners in the intelligence and law enforcement communities. We have established policies and created the necessary organizational structures to make it easier for us to disseminate our intelligence and provide access to those who need it. We are collaborating on many fronts with DOD and other members of the Intelligence Community. As Director Mueller stated in recent testimony, in this era of globalization, working side-by-side is not just the best option, it is the only option.

By building our intelligence capabilities, improving our technology, and working together, we can and we will develop the capabilities we need to succeed against the threats of the future.

Thank you for your continued support and interest in the FBI.