

STATEMENT OF
WILLIE T. HULON
DEPUTY ASSISTANT DIRECTOR
COUNTERTERRORISM DIVISION
FEDERAL BUREAU OF INVESTIGATION
BEFORE THE
HOUSE GOVERNMENT REFORM SUBCOMMITTEE ON
TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL
RELATIONS AND THE CENSUS
“Facilitating an Enhanced Information Sharing Network That
Links Law Enforcement and Homeland Security for Federal,
State and Local Governments”

July 13, 2004

Good afternoon Chairman Putnam, Ranking Member Clay and members of the subcommittee. Thank you for inviting me to speak to you today on the information sharing issues that face the Federal Bureau of Investigation and other members of the Intelligence and Law Enforcement communities. The terrorist threat of today poses complex challenges. Today’s terrorists operate seamlessly across borders and continents, aided by sophisticated communications technologies; they finance their operations with elaborate funding schemes; and they patiently and methodically plan and prepare their attacks. To meet and defeat this threat, the FBI must have several critical capabilities:

- First, we must be intelligence-driven. To defeat the terrorists, we must develop intelligence about their plans and use that intelligence to disrupt those plans.
- We must be global. We must continue our efforts to develop our overseas law enforcement operations, our partnerships with foreign law enforcement and intelligence services, and our knowledge and expertise about foreign cultures and our terrorist adversaries overseas.
- We must have networked information technology systems. We need the capacity to manage and share our information effectively.
- Finally, we must remain accountable under the Constitution and the rule of law. We must respect human rights and civil liberties as we protect the American people.

Since September 11th, the FBI has investigated thousands of threats to the U.S., and the number of active FBI investigations into potential terrorist activity has quadrupled. Working with our partners, we have also disrupted terrorist activities on multiple occasions inside the U.S., primarily terrorist financing operations.

To achieve success in this war on terror, we have transformed the FBI's Counterterrorism Division (CTD) and CT program to one that is more collaborative and proactive; we have transformed the Intelligence Program and integrated our investigative and intelligence operations; we have improved information sharing with other federal agencies and state and local law enforcement entities; and enhanced our operational capabilities within FBIHQ and all local Field Offices.

A major element of the Bureau's transformation of our Counterterrorism Program is our increasing integration and coordination with our partners in the U.S. and international law enforcement and intelligence communities. More than any other type of enforcement mission, counterterrorism requires the participation of every level of local, state, national, and international government. A good example is the case of the Lackawanna terrorist cell outside Buffalo, New York. From the police officers who helped to identify and conduct surveillance on the cell members; to the information obtained from sources overseas; to the diplomatic personnel who coordinated our efforts with foreign governments; to the FBI agents and federal prosecutors who conducted the investigation leading to the arrests and indictment, everyone played a significant role.

We recognize that a prerequisite for any operational coordination is the full and free exchange of information. Without procedures and mechanisms that allow information sharing on a regular and timely basis, we and our partners cannot expect to align our operational efforts to best accomplish our shared mission. Accordingly, we have taken steps to establish unified FBI-wide policies for sharing information and intelligence.

Interagency Information Sharing

To ensure a coordinated, enterprise-wide approach, Director Mueller recently designated the Executive Assistant Director of Intelligence (EAD-I) to serve as the principal FBI official for information and intelligence sharing policy. In this capacity, the EAD-I functions as an advisor to the Director and provides policy direction on information and intelligence sharing within and outside the FBI with the law enforcement and intelligence communities, as well as foreign governments.

The FBI shares intelligence with other members of the Intelligence Community, to include the intelligence components of the Department of Homeland Security (DHS), through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include both raw and finished intelligence reports.

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). SCION is currently available to over 1000 users at FBI Headquarters, and the FBI has initiated a pilot deployment project to the following Field Offices: New York, Boston, and Kansas City. The plan is to deliver SCION to all FBI Field Offices, as funding becomes available. Wider access to SCION within the FBI is planned for the future and will enable more extensive on-line collaboration with other intelligence agencies. Limited access to Intelink from other Field Offices is available through the old FBI Intelligence Information System Network (IISNET). Most of the Field Offices have two workstations which have a connection to FBI headquarters.

FBI offices have access to the Secret-level Intelligence Community network SIPRNET, and the FBI website on SIPRNET has been upgraded to provide more information to a wider range of users.

The FBI has established a robust channel for sharing information with the Terrorist Threat Integration Center (TTIC) by providing direct electronic access to classified and unclassified internal FBI investigative and operational databases, with narrow exceptions for certain types of sensitive domestic criminal cases unrelated to terrorism. TTIC also has direct electronic access to internal FBI headquarters division websites and e-mail capabilities on the FBI's classified intranet system. Both FBI and non-FBI personnel assigned to TTIC have access to this information.

The FBI has agreed to provide a substantial permanent staff to TTIC. By the end of this year, there will be 65 FBI personnel allocated to the TTIC. TTIC's mission is to enable full integration of terrorist threat-related information and analysis. It creates a structure to institutionalize sharing across appropriate federal agency lines of terrorist threat-related information in order to form the most comprehensive threat picture.

Although the FBI retains authority to approve dissemination of raw FBI information by TTIC to other agencies, the FBI authorizes the TTIC to share FBI intelligence products by posting them on the TTIC Online website on Intelink-TS. The TTIC Online website provides additional security safeguards, and access is granted to Intelligence Community users who have a need-to-know for more sensitive classified intelligence on international terrorism from the FBI and other agencies. The FBI also authorizes the National Counterintelligence Executive (NCIX) to share FBI counterintelligence products on the Intelink-CI(iCI) website with similar safeguards and access by users who have a need-to-know for more sensitive classified counterintelligence products.

The Bureau fully contributes intelligence analysis to the President's Terrorist Threat Report (PTTR). These products are coordinated with the CIA, DHS, and other federal agencies. In addition to the PTTR, the FBI provides Presidential Intelligence

Assessments directly to the President and the White House Executive Staff on subjects other than terrorism.

The FBI is also committed to providing those tools which assist law enforcement in intelligence-led policing -- from the National Crime Information Center, the Integrated Automated Fingerprint Identification System, and the Interstate Identification Index, to Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO users total nearly 30,000 and that number is increasing. That total includes more than 17,000 state and local law enforcement members. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence. Our LEO Intelligence Bulletins are used to disseminate finished intelligence on significant developments or trends. Intelligence Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI has also posted its terrorism intelligence priorities on LEO as well.

In addition, classified intelligence and other sensitive FBI data are shared with federal, state, and local law enforcement officials with appropriate security clearances who participate in the Joint Terrorism Task Forces (JTTFs). The JTTFs partner FBI personnel with hundreds of investigators from various federal, state, and local agencies, and are important force multipliers in the fight against terrorism. Since September 11, 2001, the FBI has increased the number of JTTFs from 35 to 84 nationwide. We also established the National Joint Terrorism Task Force (NJTTF) at FBI Headquarters, staffed by representatives from 38 federal, state, and local agencies. The mission of the NJTTF is to enhance communication, coordination, and cooperation by acting as the hub of support for the JTTFs throughout the United States, providing a point of fusion for intelligence acquired in support of counterterrorism operations. The FBI will continue to create new avenues of communication between law enforcement agencies to better fight the terrorist threat.

With the creation of the Office of Intelligence at the FBI, each FBI field office has established a Field Intelligence Group (FIG). It is the responsibility of these FIGS to manage, execute and maintain the FBI's intelligence functions within the FBI field office. FIG personnel have access to TS and SCI information so they will be able to receive, analyze, review and recommend sharing this information with entities within the FBI as well as our customers and partners within the Intelligence and Law enforcement communities. The FIGs are our field centerpiece in managing the intelligence cycle within field operations. They will complement the JTTFs and other squads and task forces through the management of the intelligence cycle functions of requirements; planning and direction; collection processing and exploitation; analysis and production and dissemination. The FIGs play a major role in ensuring that from now on, "we know what we know" and we tell others in the Intelligence Community and our federal, state, local and tribal law enforcement partners "what we know".

On February 11, 2004 the Attorney General announced the creation of the DOJ Intelligence Coordinating Council. The Council is comprised of the heads of DOJ

agencies with intelligence responsibilities, and is currently chaired by the FBI's EAD-I. The Council will work to improve information sharing within the Department of Justice (DOJ) and to ensure that DOJ meets the intelligence needs of outside customers and acts in accordance with intelligence priorities. It will also identify common challenges (such as electronic connectivity, collaborative analytic tools, and intelligence skills training) and establish policies and programs to address them.

On February 20, 2004 the FBI formed an information sharing policy group, comprised of Executive Assistant Directors, Assistant Directors and other senior executive managers. Under the Direction of the EAD-I, this group is establishing FBI information and intelligence sharing policies.

Intelligence and Analytical Products and Services

In the past year, the FBI has produced more than 3,000 intelligence products, including "raw" reports, intelligence memoranda, in-depth strategic analysis assessments, special event threat assessments, and focused Presidential briefings. We also conducted numerous intelligence briefings to members of Congress, other government agencies, and the law enforcement and intelligence communities. These efforts mark a new beginning for the FBI's intelligence production capability.

Prior to September 11, 2001, the FBI produced very few raw intelligence reports. In FY 2003, we produced and disseminated 2,425 Intelligence Information Reports (IIRs) containing raw intelligence derived from FBI investigations and intelligence collection. The majority of these IIRs contained intelligence related to international terrorism; the next greatest number contained foreign intelligence and counterintelligence information; and the remainder concerned criminal activities and cyber crime. These IIRs were disseminated to a wide customer set in FBI field offices, the Intelligence Community, Defense Community, other federal law enforcement agencies, and U.S. policy entities.

In addition to these raw intelligence reports, the FBI has begun producing analytic assessments on a par with those of other Intelligence Community agencies. The FBI developed and issued, in January 2003, a classified comprehensive assessment of the terrorist threat to the U.S. This assessment focuses on the threats that the FBI sees developing over the next two years, based on an analysis of information regarding the motivations, objectives, methods, and capabilities of existing terrorist groups and the potential for the emergence of new terrorist groups and threats throughout the world. This threat assessment is used as a guide in the allocation of investigative resources, as a useful compilation of threat information for investigators and intelligence personnel within and without the FBI, and as a resource for decision-makers elsewhere in the government. The 2004 threat assessment was released in April 2004. FBI analysts have produced over 100 in-depth analyses and several hundred current intelligence articles in addition to the work they do supporting FBI investigations.

We are preparing to produce, in the near future, the *FBI Daily Report* and the *FBI National Report* to provide daily intelligence briefings to personnel in the field and

external customers. One will be produced at the classified level and limited in distribution to upper-level field managers. The other will be unclassified and widely distributed to field office personnel and our partners in the law enforcement community.

A good example of our ability to exploit evidence for its intelligence value and share that intelligence with appropriate members of the law enforcement and Intelligence Communities, is our use of the al-Qa'ida terrorism handbook. A terrorism handbook seized from an al-Qa'ida location overseas in the mid-1990's was declassified and released by DOJ shortly after the events of September 11, 2001. We determined that intelligence gleaned from the handbook could provide useful guidance about al-Qa'ida's interests and capabilities. Accordingly, we produced and disseminated a series of intelligence products to share this intelligence with our personnel in the field and with our law enforcement partners. Nine Intelligence Bulletins were based in whole or in part on this intelligence. In addition, we used information derived from the al-Qa'ida Handbook to update our counterterrorism training, including the Intelligence Analyst Basic Course at the College of Analytical Studies, the Introduction to Counterterrorism Course at the National Academy, and sessions on Terrorism Indicators and Officer Safety in our State/Local Anti-Terrorism Training (SLATT). The unclassified version of the handbook is now maintained as a reference in the FBI Library and is accessible to all the students at the Academy. It also is included in the reference manual CD-Rom distributed as part of SLATT training.

One telling measure of our improved counterterrorism operations is the development of our capability to brief the daily terrorist threat information. The development of this capability reflects the maturing of our centralized Counterterrorism Program.

Prior to September 11th, the FBI lacked the capacity to provide a comprehensive daily terrorism briefing – to assemble the current threat information, to determine what steps were being taken to address each threat, and to present a clear picture of each threat and the Bureau's response to that threat to the Director, senior managers, the Attorney General, and others in the Administration who make operational and policy decisions. With a decentralized program in which investigations were run by individual field offices, the Bureau never had to develop this specialized skill. With the need for centralized management, however, it became an imperative.

In the aftermath of the September 11th terrorist attacks, we were asked to begin sending to the White House each morning daily reports on counterterrorism-related events. We had no mechanism in place for collecting that information, so preparation of the reports was initially haphazard. During the past 34 months, with the assistance of veterans from the Intelligence Community, we have established the infrastructure and the cadre of professionals to produce effective daily briefings and to share briefing materials more widely within the Bureau and with our partners.

In 2002 we established the Presidential Support Group within the Counterterrorism Division to prepare daily briefing materials. In the summer of 2003, this

group was renamed the Strategic Analysis Unit and moved to the Office of Intelligence. Beginning in August 2003, the Strategic Analysis Unit began producing the Director's Daily Report (DDR), a daily intelligence briefing that includes information on counterterrorism operations, terrorism threats, and information related to all areas of FBI investigative activity.

To produce the DDR, the Strategic Analysis Unit consolidates and refines information provided in a standardized format by intelligence personnel in each division. Each morning, information about new threats is added, and information about threats that have been thoroughly vetted during the night is removed. The DDR is distributed to executives in all FBI operational divisions. The Director uses the DDR to brief the President nearly every weekday morning. The FBI also produces the *Presidential Intelligence Assessment*, a finished FBI intelligence product covering topics of particular interest to the President, and as noted earlier, our personnel at TTIC and at FBI Headquarters contribute to the formulation of the daily *President's Terrorist Threat Report*.

Beyond these information sharing initiatives, we are increasing our operational coordination with our state, federal, and international partners on a number of fronts.

We have established much stronger working relationships with the CIA and other members of the Intelligence Community. From the Director's daily meetings with the Director of Central Intelligence and CIA briefers, to our regular exchange of personnel among agencies, to our joint efforts in specific investigations and in the Terrorist Threat Integration Center, the Terrorist Screening Center, and other multiagency entities, the FBI and its partners in the Intelligence Community are now integrated at virtually every level of our operations. In addition, the FBI is a participant in the Gang of Eight meetings.

The FBI currently has Agents and Analysts detailed to CIA entities, including the DCI's Counter Terrorist Center (CTC). We also have FBI agents and intelligence analysts detailed to the NSA, the National Security Council, DIA, the Defense Logistics Agency, DOD's Regional Commands, the Department of Energy, and other federal and state agencies.

The Terrorist Threat Integration Center is a good example of our collaborative relationship with our federal partners. Established on May 1, 2003 at the direction of President Bush, TTIC has the primary responsibility in the USG for terrorism analysis (except information relating solely to domestic terrorism, which is the responsibility of the FBI). Analysts from the FBI, CIA, DHS and DOD work side-by-side at TTIC to piece together the big picture of threats to the U.S. and our interests. TTIC analysts synthesize government-wide information regarding current terrorist threats and produce the Presidential Terrorism Threat Report for the President, the Threat Matrix and other analytic products. The FBI personnel at TTIC are part of the Office of Intelligence and work closely with analysts at FBI Headquarters in combining domestic and international terrorism developments into a comprehensive analysis of terrorist threats. In addition to

the analysis developed by FBI analysts detailed to TTIC, FBI analysts at Headquarters regularly contribute articles to the President's Terrorist Threat Report.

At the same time, we have intelligence analysts from other agencies working in key positions throughout the Bureau. The Associate Deputy Assistant Director for Operations in the Counterterrorism Division is a CIA detailee. CIA officers are detailed to the Security Division, including the Assistant Director, the Chief of the Personnel Security Section, and managers working with the SCI program and the FBI Police. An experienced manager from the CIA's Directorate of Science and Technology now heads the Investigative Technologies Division and a Section Chief in that division is on rotation from CIA. This exchange of personnel is taking place in our field offices as well.

We have also worked closely with DHS to ensure that we have the integration and comprehensive information sharing between our agencies that are vital to the success of our missions. The FBI and DHS share database access at TTIC, in the National JTTF at FBI Headquarters, in the Foreign Terrorist Tracking Task Force (FTTTF) and the Terrorist Screening Center (TSC), and in local JTTFs in our field offices around the country. We worked closely together to get the new Terrorist Screening Center up and running. We hold weekly briefings in which our CTD analysts brief their DHS counterparts on current terrorism developments. The FBI and DHS now coordinate all joint warnings through the Homeland Security Advisory System to address our customers' concerns about multiple and duplicative warnings. We designated an experienced executive from the Transportation Security Administration to run the TSC and a senior DHS executive was detailed to the FBI's Office of Intelligence to ensure coordination and transparency between the agencies.

The FBI is committed to participating in the Attorney General's 94 Antiterrorism Advisory Councils that bring together federal, state and local law enforcement, first responders and other federal, state, and local homeland security entities with an interest in preventing and responding to terrorist threats.

Improving the compatibility of information technology systems throughout the Intelligence Community, meanwhile, will increase the speed and ease of information sharing and collaboration. Accordingly, the FBI's information technology team has worked closely with the Chief Information Officers (CIOs) of DHS and other Intelligence Community agencies, to develop our recent and ongoing technology upgrades. This coordination has affected our decisions on several key technology upgrades.

To facilitate further coordination, the FBI CIO sits on the Intelligence Community CIO Executive Council. The Council develops and recommends technical requirements, policies and procedures, and coordinates initiatives to improve the interoperability of information technology systems within the Intelligence Community. It was established by Director of Central Intelligence directive and is chaired by the CIA's CIO.

On March 4, 2003, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence signed a comprehensive Memorandum of

Understanding (MOU) establishing policies and procedures for information sharing, handling, and use. Pursuant to that MOU, information related to terrorist threats and vulnerabilities is provided to DHS automatically without DHS having to request it. Consistent with the protection of sensitive sources and methods and the protection of privacy rights, we now share as a rule, and withhold by exception.

With terrorists traveling, communicating, and planning attacks all around the world, coordination has become more critical than ever before. We have steadily increased our overseas presence and now routinely deploy agents and crime scene experts to assist in the investigation of overseas attacks, such as the May 2003 bombings in Saudi Arabia and Morocco. As of January 7, 2004, 413 FBI personnel were assigned overseas, over 200 of whom are permanently assigned. Their efforts have played a critical role in the successful international operations we have conducted over the past 34 months.

Bureau personnel have participated in numerous investigations of terrorist attacks in foreign countries over the past 34 months. Our approach to those investigations differs from the approach we traditionally have taken. Prior to September 11th, our overseas investigations primarily focused on building cases for prosecution in the U.S. Today, our focus has broadened to providing investigative, forensic, and other types of support. This is paying dividends with greater reciprocal cooperation and more effective joint investigations.

Information Sharing Systems

The FBI has a responsibility to the nation, Intelligence Community, and federal, state and local law enforcement to disseminate information, and to do so is an inherent part of our mission. Sharing FBI information will be the rule; filtering the information will be the exception, where sharing is legally or procedurally unacceptable. The FBI will deliver its information through the systems the FBI and its customers and partners use.

In the area of organizational message traffic for dissemination of official information and taskings to other agencies, the FBI has just implemented its new FBI Automated Messaging System (FAMS) which is based on the Defense Messaging System (DMS). FAMS will provide on-line message creation, review, and search capabilities to everyone connected to FBINET. FAMS gives us the capability to send and receive critical organizational message traffic to any of the 40,000+ addresses on DMS or Automated Digital Network (AUTODIN). The TS/SCI version of FAMS is currently in testing and will provide the same capability to everyone on SCION or IISNET in the near future. The FBI's implementation of the DMS will provide writer-to-reader secure e-mail to internal and external users. Within the government, DMS will replace AUTODIN and a diverse array of e-mail systems currently in use throughout the Department of Defense and Intelligence Agencies. In its final form, DMS could become the government's global secure e-mail system. It will provide certified interoperability of various commercially off-the-shelf software products and connect over 2 million civilian

and military users. The system will permit multi-media attachments to messages and provide end-to-end security.

The FBI Chief Information Officer is also working with the Department of Justice on interfaces between the Intelligence Community System for Information Sharing (ICSIS) and the Law Enforcement Information Sharing initiative, and with the FBI Criminal Justice Information Services (CJIS) Division to increase the sharing of intelligence related information to and from state and local officials.

The FBI is currently deploying the SECRET versions of FAMS, which uses DMS and secure Outlook-like e-mail for organizational messages, so that our analysts and reports officers can send and receive timely intelligence with other agencies in near real time. The FBI is also working on a digital production capability for IIRs using extended markup language (XML) that will interface with FAMS and support on-line digital production of intelligence reports. The FBI is applying XML data standards and meta-data tagging to facilitate the exchange of information with the intelligence community. The FBI is also applying new security technology to deploy a Protection Level 3 Data Mart capability with discretionary access controls and Public Key Infrastructure certificates in support of closed Community of Interests, which will permit secure sharing of our most sensitive data with trusted members of other agencies. The FBI is also investigating the use of secure one-way transfers to move information between security domains and to permit all-source intelligence analysis. The use of next-generation, community High Assurance Guards is being planned to provide for the two-way transfer of critical intelligence between security domains. Secure wireless connectivity and Virtual Private Networks are also being looked at to provide increased access to intelligence to deployed personnel. The FBI is also starting to use On-line, desktop collaboration tools such as Info Work Space which is the foundation for the Intelligence Community Collaboration Portal to increase intelligence collaboration.

The FBI plans to use additional systems as the foundation for additional information sharing with the Intelligence Community, Federal, State and Local entities.

The CJIS National Data Exchange (NDEx) has plans for developing a systems approach to the operation, and maintenance of several interconnected IT and supporting telecommunications systems including Law Enforcement On-line (LEO) and CJIS Wide Area Network (WAN). The NDEx is to be a repository of national indices and a pointer system for state/local/federal and inter-governmental law enforcement entities. The NDEx will also be a fusion point for the correlation of nationally-based criminal justice information with certain national security data.

Law Enforcement On-Line provides web-based communications to the law enforcement community to exchange information, conduct on-line education programs, and participate in professional special interest and topically focused dialog. The system has been operational since 1995 and presently serves about 30,000 users. LEO has secure connectivity to the Regional Information Sharing Systems network (riss.net). The FBI Intelligence products are disseminated weekly via LEO to over 17,000 law enforcement agencies and to

60 federal agencies, 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 plans to enhance LEO for robust, high-availability operation. The FBI will use the enhanced LEO as the primary channel for sensitive but unclassified communications with other federal, state and local agencies. LEO and the Department of Homeland Security's Joint Regional Information Exchange System (JRIES) will be interoperable.

The Investigative Data Warehouse (IDW) is following a multiple-phased approach to quickly provide support to FBI investigators, and JTTF members in the form of a spirally-developed operational prototype system, the *Secure Counterterrorism Operational Prototype Environment* (SCOPE). The IDW provides the Bureau with a single access point to several data sources that were previously available only through separate, stove-piped systems. By providing consolidated access to the data, for the first time analytical tools can be used across data sources to provide a more complete view of the information possessed by the Bureau.

The IDW, delivered in its first phase in January 2004, now provides analysts with full access to investigative information within FBI files, including ACS and VGTOF data, open source news feeds, and the files of other federal agencies such as DHS. The IDW provides physical storage for data and allows users to access that data without needing to know its physical location or format. The data in the IDW is at the Secret level, and the addition of TS/SCI level data is in the planning stages.

Later this year, we plan to enhance the IDW by adding additional data sources, such as Suspicious Activity Reports, and by making it easier to search. When the IDW is complete, Agents, JTTF members and analysts, using new analytical tools, will be able to search rapidly for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days. They will be able to extract subjects' addresses, phone numbers, and other data in seconds, rather than searching for it manually. They will have the ability to identify relationships across cases. They will be able to search up to 100 million pages of international terrorism-related documents in seconds. The IDW will help meet the law enforcement and the IC need for rapid, secure, dependable indexed data and will provide data mining access to FBI investigative files.

We are introducing advanced analytical tools to help us make the most of the data stored in the IDW. These tools allow FBI agents and analysts to look across multiple cases and multiple data sources to identify relationships and other pieces of information that were not readily available using older FBI systems. These tools 1) make database searches simple and effective; 2) give analysts new visualization, geo-mapping, link-chart capabilities and reporting capabilities; and 3) allow analysts to request automatic updates to their query results whenever new, relevant data is downloaded into the database.

Another information sharing project, the Multi-agency Information Sharing Initiative (MIS), is intended to enable Federal, state, and local law enforcement agencies to share regional investigative files and provide powerful tools for cross-file analyses. A proof-of-concept effort is underway in St. Louis; additional demonstration sites are being planned.

The goal of the demonstrations is to (1) show the value of sharing investigative data which can be analyzed by modern software tools; and (2) help define technical and organizational approaches for regional shared systems. Final decisions about deployment of the MIS will be based on the results of the demonstrations and the department wide plan for law enforcement information sharing being developed by the Department of Justice.

Thank you for allowing me the opportunity to testify before you today and I will be happy to entertain any questions you may have.