The Federal Bureau of Investigation

NATIONAL INFORMATION SHARING STRATEGY

August 2008

PURPOSE

The Federal Bureau of Investigation (FBI) National Information Sharing Strategy (NISS) provides the common vision, goals, and framework needed to guide information sharing initiatives with our federal, state, local, and tribal agency partners; foreign government counterparts; and private sector stakeholders. The FBI NISS addresses the cultural and technological changes required to move the FBI to "a responsibility to provide" culture. The FBI will continue its transformation by identifying and adopting the best practices and evolving technology standards of both the intelligence and law enforcement communities in collection, dissemination, analysis, collaboration, and operational efforts.

VISION

The FBI is committed to sharing timely, relevant, and actionable intelligence to the widest appropriate audience. Effective information exchange with federal agencies; state, local, and tribal officials; foreign partners; and the private sector is an increasingly important component to the FBI's unique and important national security and law enforcement mission. The FBI is required to effectively balance the need to effectively and securely share information with its responsibility to protect sources, investigative operations, national security information, and the privacy and civil liberties of US persons.

FRAMING DOCUMENTS

Several documents provide mandates and issue guidance for information sharing:

- The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Section 1016 directed the establishment of the terrorism Information Sharing Environment (ISE) and requested the ISE be "a decentralized, distributed, and coordinated environment." The Implementing Recommendations of the 9/11 Commission Act of 2007, PL 110-53, further refined the ISE mandate.
- Executive Order 13356 and 13388 mandated the establishment of an ISE and the Information Sharing Council (ISC).
- The National Strategy for Information Sharing provided guidelines to advance the development and implementation of the ISE.
- The Director of National Intelligence (DNI) issued the Intelligence Community Information Sharing Strategy and Intelligence Community Policy Memorandum (ICPM) 2007-500-3, "Intelligence Information Sharing," providing guiding principles for creating an information sharing culture and enabling technology framework.
- The Department of Justice (DOJ) established the Law Enforcement Information Sharing Program (LEISP) which created a "One DOJ" information sharing environment at the unclassified level for the law enforcement community.

GUIDING PRINCIPLES

The FBI is both a component of the DOJ as well as a member of the Intelligence Community (IC), and is accountable to both the Attorney General and the DNI for information sharing.

The FBI adheres to both Attorney General and DNI guidelines for information sharing, ensuring that intelligence and law enforcement information is shared with relevant partners while protecting sensitive information and the privacy and civil liberties of US persons.

Consistent with the FBI's strategic execution of major organizational initiatives that emphasize the collection and dissemination of intelligence to meet national security and law enforcement requirements, the FBI NISS is centered on two primary objectives: 1) creating and sustaining a culture of information sharing, and 2) developing and maintaining an information technology (IT) infrastructure that enables a broad spectrum of standards-based information sharing activities. The following guiding principles provide the framework for the FBI NISS:

- Foster a culture of sharing both within the FBI and between the FBI and its federal, state, local, and tribal partners. Encourage information sharing and integration – fusing "all crimes with national security implications" with "all hazards" information.

- Produce documents at the lowest classification level feasible without losing meaning or essential context while protecting sources and vital national security information.

- Share information within the framework of US laws, DOJ LEISP Privacy Policy, and ISE Privacy Guidelines, ensuring the FBI protects privacy rights and civil liberties of US persons.

- Provide information to partners and enable their ability to search, find, and retrieve sharable information.

- Remain flexible to accommodate the various law enforcement entities that operate under different state and local criminal justice laws and policies.

- Ensure that advanced technology for FBI information systems is user-driven so those charged with protecting the public have the information they need with security to protect sensitive investigative techniques and operations as well as personal privacy.

- Leverage existing platforms and develop new technology to enhance our information sharing capabilities. Continue to adopt new technology and invest in IT infrastructure that are compliant with federal standards, meet FBI needs, provide auditable information integrity and quality, provide the appropriate level of security, and allow for strong community user identification and authentication.

IMPLEMENTATION WITHIN THE FBI

Information Sharing Culture. In order to develop a collaborative culture at the FBI, all levels of management within the FBI will emphasize information sharing. Employees will be encouraged to share information within established procedures while protecting privacy and civil liberties. Supervisors will recognize important information sharing work through employee performance appraisals and other incentive awards. Additionally, education and

training on information sharing will be widely available and required by both new and current FBI personnel. Along with internal measures, FBI personnel are also encouraged to develop professional relationships with their IC counterparts and participate in analytical exchanges to further information sharing.

Community joint duty assignments, which will enhance the FBI's knowledge of the IC and develop the future cadre of the Intelligence Community Officer (ICO) ranks, will be encouraged by all levels of FBI management.

As part of information sharing efforts, the FBI will revise relevant policies and procedures to implement the requirements of national policy for Controlled Unclassified Information (CUI).

IMPLEMENTATION WITH EXTERNAL ENTITIES

As the FBI interfaces with a variety of customers, different types of information and sharing mechanisms are essential. Although many processes apply universally to information sharing, some unique aspects apply to specific customers.

The FBI NISS divides FBI's information sharing customers/partners into five categories: 1) Presidential Offices; 2) Department of Justice and other federal departments and agencies; 3) state, local, and tribal authorities; 4) private sector entities; and 5) foreign partners.

Executive Office of the President

The FBI coordinates information sharing within the Executive branch through several mechanisms. The FBI is a member of the National Security Council / Homeland Security Council Policy Coordination Committee on Information Sharing. Additionally, the FBI works closely with the Office of Management and Budget to program financial resources needed for information sharing initiatives and technology. The IRPTA required the President designate a Program Manager for the ISE (PM-ISE), which the President placed under the DNI. The FBI works closely with the PM-ISE.

Information Sharing with Federal Departments and Agencies

The Intelligence Community Information Sharing Strategy calls for increased collaboration and enhanced intelligence information sharing policies, processes, and procedures, including a shift from the "need-to-know" to "responsibility to provide" culture. To promote an effective exchange and coordination among federal departments and agencies, the FBI will share terrorism information in a manner consistent with applicable legal and policy standards.

Director of National Intelligence. Under the DNI, several important information sharing entities exist.

DNI/Chief Information Officer. The DNI/Chief Information Officer (CIO) has developed several ICPMs regarding information sharing. ICPM 2007-500-3, Intelligence Information Sharing," requires IC agencies to provide maximum access to and

dissemination of intelligence information while protecting intelligence sources and methods; apply DNI metadata tagging standards for all intelligence information to enable retrieval; and implement DNI-approved attribute-based identify management capability to enable attribute-based access, user authorization, and use auditing services.

DNI/Analysis. The Deputy DNI for Analysis (DDNA/A) has developed ICPM 2007-200-2, "Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide," requires IC agencies to more effectively balance the "need to share" intelligence with the requisite "need to protect" intelligence sources and methods. FBI will support DDNI/A initiatives, including a Library of National Intelligence and A-Space, for sharing intelligence reports and other products among analysts from across the IC.

National Counterterrorism Center. The National Counterterrorism Center (NCTC) has the primary responsibility within the US Government for analysis of all intelligence and information pertaining to terrorism. FBI will support NCTC by:

- Providing terrorism-related intelligence and information to NCTC for analysis and integration unless prohibited by law or otherwise directed by the President;
- Assigning personnel to NCTC to assist in developing coordinated and integrated assessments of terrorist threats, plans, intentions, and capabilities;
- Allowing direct access to FBI raw operational electronic files and databases on international terrorism cases, as appropriate to support the national counterterrorism analysis efforts of NCTC; and
- Participating in pilot projects to evaluate the utility of matching data on international terrorist suspects and activities with other relevant government databases.

Interagency Centers and Initiatives. The FBI leads and participates in several interagency centers and initiatives in order to share and exchange information.

Terrorist Screening Center. The Terrorist Screening Center (TSC) manages the single, consolidated terrorist watchlist providing key resources for screeners and law enforcement personnel. These include a single coordination point for terrorist screening data; a 24/7 call center for encounter identification assistance; access to a coordinated law enforcement response center; a formal process for tracking encounters; feedback to the appropriate entities; and a redress process. TSC provides unclassified identifying information to the Department of Homeland Security (DHS) and the Department of State (DOS), as well as to other federal, state, local, and tribal law enforcement agencies through the FBI's National Crime Information Center (NCIC).

Terrorist Explosive Device Analytical Center. At Terrorist Explosive Device Analytical Center (TEDAC), US military, intelligence, and law enforcement agencies consolidate their information and integrate their efforts to exploit all information about terrorist improvised explosive devices (IEDs) of interest to the US Government. TEDAC provides an opportunity to liaise with the Bureau of Alcohol, Tobacco, and Firearms (ATF) and the Department of Defense (DOD).

Biometrics. The Next Generation Identification (NGI) project and the Combined DNA Index System (CODIS) will be integral to a national biometrics initiative under the National Counterterrorism Strategy. The FBI will participate actively in interagency efforts to reach agreement on data standards, including standards for biometric data required by TSC.

National Gang Intelligence Center. The FBI hosts the National Gang Intelligence Center (NGIC) at headquarters to support law enforcement partners. The NGIC shares information and analysis products concerning the growth, migration, criminal activity, and association of gangs that pose a significant threat to US communities. The NGIC is co-located with the National Gang Targeting, Enforcement, and Coordination Center (GangTECC).

National Crime Information Center. The National Crime Information Center (NCIC), established in 1967, is a computerized index of documented criminal justice information available to criminal justice agencies nationwide. The information in NCIC assists authorized users in identifying terrorists, apprehending fugitives, locating missing persons, and recovering stolen property.

Information Sharing with State, Local, and Tribal Entities

Information Sharing Environment. The National Strategy for Information Sharing mandated the Information Sharing Environment. Efforts within the ISE include:

State and Major Urban Area Fusion Centers. Where security and resources permit, FBI personnel will provide Fusion Center access to classified FBI information systems.

e-Guardian. The e-Guardian system is designed as a tool where unclassified counterterrorism threat data and suspicious activity incidents can be routinely shared with state and local law enforcement officials to view and search this threat data, and to create useful reports.

Interagency Threat Assessment Coordination Group. The Interagency Threat Assessment Coordination Group (ITACG) was established to develop coordinated intelligence reports and analytical products regarding terrorist threats and related issues that address the needs of state, local, tribal, and as appropriate, private sector entities.

Law Enforcement Information Sharing Program. In October 2005, the DOJ released the LEISP, and in a December 21, 2006 memorandum, the Deputy Attorney General directed the FBI and other DOJ components to participate in regional and national law enforcement information sharing initiatives. The LEISP is a program that addresses barriers to information sharing and creates a forum for collaboration on how existing and planned systems will be coordinated and unified for information sharing purposes. The LEISP delineates guiding principles, a policy framework, and functional requirements that are necessary to facilitate multi-jurisdictional law enforcement sharing. The LEISP established DOJ's commitment to move from a culture of "need to know" toward a culture of "need to

share." The LEISP Coordinating Committee provides oversight and adjudicates concerns for these initiatives.

The Information Sharing technology components of LEISP are:

The **OneDOJ** system is a federation of regional systems that allows information sharing among the FBI, ATF, Drug Enforcement Agency (DEA), Bureau of Prisons, US Marshals Service, and regional law enforcement agency partners.

The **Law Enforcement National Data Exchange (N-DEx)** program is designed for use by all federal, state, local, and tribal law enforcement agencies and will eventually incorporate OneDOJ functions as a one-stop information sharing service.

The FBI's **Law Enforcement On-Line (LEO)** network will provide the web-based platform to support N-DEx, OneDOJ, and access to an extensive array of FBI and other law enforcement agencies' databases and services at the sensitive but unclassified level.

State, local, and tribal law enforcement user needs and concerns are identified through the FBI Criminal Justice Information Services Advisory Policy Board (CJIS/APB) and the DOJ Global Criminal Intelligence Coordinating Council (CICC).

Information Sharing with Private Sector Stakeholders

The FBI is committed to developing effective and efficient information sharing partnerships with private sector entities. To this end, the FBI will share terrorism-related information on incidents, threats, consequences, and vulnerabilities, as appropriate, to private sector entities while ensuring that all proprietary information is protected.

InfraGard is a partnership between the Federal Government, an association of businesses, academic institutions, state and local law enforcement, agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard members communicate with each other and the FBI via public and secure Internet websites. InfraGard began in 1996 with cyber threats and has expanded to cover thirteen critical infrastructure sectors. The FBI's Counterintelligence Division partnered with InfraGard to help protect national and economic security.

The **Cyber Initiative Resource Fusion Unit** is a fusion center combining the resources and the expertise of law enforcement and the private sector. Experts from federal agencies, software companies, Internet Service Providers, and the financial sector share information and collaborate about cyber threats and security breaches.

The **Domestic Security Alliance Council (DSAC)**, a strategic partnership between the FBI and the US private sector, was established to promote the timely and effective exchange of information. DSAC advances the FBI mission of preventing, detecting, and investigating criminal acts, particularly those affecting interstate commerce, while advancing the ability of the US private sector to protect its employees, assets, and

proprietary information. Following the model built by the DOS Overseas Security Alliance Council (OSAC), the FBI stood up DSAC within the Criminal Investigative Division in 2007.

Information Sharing with Foreign Partners

Sharing with foreign partners, including exchange of biographic and biometric information of known or suspected terrorists, requires both flexibility and adequate security precautions. The FBI will adhere to strict handling restrictions and ensure the protection of US person data. The FBI has established Memorandum of Understanding (MOUs) with many foreign governments. The Office of International Operations and Legal Attaches will serve as the primary mechanism to establish MOUs with foreign governments.

DEPLOYING INFORMATION SHARING TECHNOLOGIES AND STANDARDS

Technological Infrastructure: FBI IT initiatives and investments will provide an IT infrastructure that will enable the FBI to share information with the law enforcement and intelligence communities in the most secure and cost efficient manner possible consistent with current law, policy, and program guidance.

Technological Standards: Compliance with intelligence and law enforcement standards will provide an IT infrastructure that will enable the FBI to share information with the law enforcement and intelligence communities in the most secure and cost efficient manner possible consistent with current law, policy, and program guidance.

SUMMARY

The FBI has taken substantial steps to improve intelligence and information sharing both internally and externally. By continuing to refine internal processes and procedures and with the implementation of new information technology and standards, the FBI will increase its ability to share investigative and intelligence information within the law enforcement and intelligence communities in a manner that protects the privacy and civil liberties of US persons.