THE FEDERAL BUREAU OF INVESTIGATION

NATIONAL INFORMATION SHARING STRATEGY

2011

Table of Contents

I. INTRODUCTION

The Federal Bureau of Investigation (FBI) seeks to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners while preserving the privacy and civil liberties of U.S. persons.

Information exchange is an increasingly important component of the FBI's unique and important national security and law enforcement mission. In furtherance of its mission, and consistent with the principles established by the Director of National Intelligence (DNI) in the 2009 National Intelligence Strategy (NIS), the FBI works aggressively to improve information sharing capabilities. The FBI promotes an information-sharing culture, deploys new technologies, and refines its policies and procedures in support of its commitment to share timely, relevant, and actionable intelligence to the widest appropriate audience. The FBI National Information Sharing Strategy (NISS) provides the foundation to shape and implement information sharing initiatives with the FBI's many mission partners, including federal agencies, state, local, and tribal officials, foreign government counterparts, and private sector stakeholders.

II. NATIONAL INFORMATION SHARING STRATEGY

The NISS ensures coordination of FBI initiatives that emphasize the collection and dissemination of intelligence to meet national security and law enforcement needs. The NISS has three goals: 1) reinforce the emerging culture of information sharing by emphasizing the benefits of active information and knowledge exchange, 2) make information sharing easier through the focused use of information technology and policy, and 3) make information sharing more effective. These goals must always be balanced against preservation of privacy and civil liberties.

The NISS is augmented by the Chief Information Sharing Officer (CISO) annual Information Sharing Report, which provides a comprehensive view of the FBI's information sharing activities.

A. Reinforcing a Culture of Sharing

The FBI has accomplished several seminal information sharing initiatives and continues to promote additional sharing and collaboration. The FBI's senior leadership is committed to ensuring information sharing practices are an integral part of the FBI culture. All levels of FBI management emphasize the importance of information sharing while protecting privacy and civil liberties and guarding national security.

Value and Trust

The value of positive outcomes resulting from information or knowledge exchange is easily identified. Information sharing can lead to increased and faster access and acquisition of information, as well as to new sources of information that contribute to investigations and successful prosecutions. Information sharing enhances knowledge of domain or mission areas and of law enforcement and Intelligence Community (IC) operations and procedures. Information sharing also increases an agency's work force through leveraging mission partner activities and by providing more insightful understanding of partner capabilities and limitations. Robust and collaborative partnerships, enhanced lawful sharing of information, and coordinated interactions that increase knowledge will fortify national security.

These positive outcomes derive from trust between the FBI and its mission partners. Relationships are driven by institutional imperatives—public safety and the need to uphold/enforce laws—as well as mutual gain. Organizational relationships are established or broken based upon the level of trust in each member of the relationship and the influence that an individual exerts within his/her respective organization. Trust usually follows from understanding, interaction, and positive personal experiences. Establishing value, therefore, requires not only identification of rewards at the organizational level, but also at the personal level.

Implementation

Various initiatives are underway at the FBI to shape and influence attitudes as well as enhance appreciation of the value of a mutual information exchange. The FBI's efforts are not static activities that can be accomplished once and forgotten. Rather, they are continuing efforts to fully integrate information sharing into the organization's culture, values, internal appraisals, and business processes.

Today's FBI professionals are encouraged to develop professional relationships with their law enforcement and IC counterparts and to contribute to analytical exchanges. Participation in Joint Terrorist Task Forces (JTTFs), other joint task forces, and Fusion Centers is promoted as a positive career growth opportunity. Joint duty assignments, which promote collaboration and establish productive relationships by building rapport and trust, are encouraged; for certain Senior Executive Service (SES) positions, joint duty experience or credit is required. These assignments also benefit the FBI by helping to develop a cadre of certified Intelligence Officers and by enhancing institutional knowledge of intelligence issues. The FBI has established the Intelligence Community Management Liaison Office in the Human Resources Division to facilitate both FBI participation and the placement of external Intelligence Community Officers in FBI assignments. To further institutionalize the value of information sharing, education and training on information sharing which emphasizes understanding and insight is required for all FBI personnel. Additionally, performance appraisals and professional recognition address information sharing behavior.

B. Making Information Sharing Easier

A second goal of the FBI Information Sharing Strategy is to encourage, facilitate, and expand effective information sharing by removing barriers that may impede it, consistent with federal legal requirements, and by easing the means to accomplish it. The FBI will achieve this goal through the insightful application of policy and technology.

The Use of Policy

Impediments to sharing information may result from narrowly crafted policy. The FBI endeavors to make policy that encourages information sharing through cross-division consideration and review at the enterprise level. The Information Sharing Policy Board (ISPB) supports corporate policy development to promote broader perspectives. At the same time, it tracks individual projects and programs for impact on enterprise philosophy and equities.

As a component of the Department of Justice (DOJ) and a member of the IC, the FBI is accountable to both the Attorney General (AG) and the DNI for information sharing. FBI policies govern information sharing in accordance with U.S. laws and regulations, Executive Orders, DOJ policy, IC policy, and guidelines.[1] The policies outline authorities and procedures for sharing FBI information with other government agencies and establish responsibilities to ensure compliance with privacy protection requirements for sharing information. All information sharing activities subject to Corporate Policy Directive 0012D, FBI Information Sharing Activities with Other Government Agencies, undergo an information sharing risk assessment and are controlled by a written governing document. The governing document must address the duty to protect privacy, civil liberties, and other legal rights of U.S. persons. Each new initiative is carefully reviewed to safeguard privacy, civil liberties, and other legal rights of U.S. persons to ensure they are not compromised, and written analyses are performed as required to verify privacy and civil liberties are vigorously protected.

Other principles also guide the formal structure that enables information sharing. National security considerations require a full-spectrum defense using all the capabilities of the law enforcement and intelligence communities. The refinement of policy language to broaden interpretations and facilitate the use of lawfully-collected information is an important means of enhancing the ability of mission partners to search, find, and retrieve sharable information. Production of assessments and reports at the lowest, feasible classification level, while preserving meaning and protecting vital source information, is a challenging, but necessary part of standard operating procedures. All policies must include an understanding of the authorities under which our mission partners operate.

The Use of Technology

The FBI continues to develop an information technology (IT) infrastructure that facilitates information sharing activities. The IT strategy is to leverage existing platforms and to adopt or develop new technologies to enhance information sharing capabilities, while also ensuring that

[1] The organizational elements with information sharing roles are described in Appendix A, Information Sharing Elements.

FBI information systems are sufficiently secure to protect sensitive investigative sources, techniques, and operations, as well as personal privacy.

To facilitate and encourage more extensive information sharing the FBI has undertaken a broad range of IT-related initiatives:

- Employment of IT standards and protocols that are consistent and compatible with the IC and DOJ;
- Development/adoption of cross-domain solutions that provide multi-level browse and transfer capabilities while retaining access controls across security enclaves;
- Adoption of enterprise standards and protocols to enable common services, information discovery, and seamless communication across the information sharing (or mission) environment; and
- Establishment of appropriate network connectivity to information sharing partners.

Implementation

The FBI strategy is to employ technology initiatives to identify and resolve impediments to information sharing, and to recognize and exploit opportunities to make information sharing easier. Working from the initiative level up (rather than by adopting a top-down architecture) is necessary to protect from disruption the daily execution of the FBI law enforcement and national security missions.

There are many ongoing initiatives that embody the FBI's use of policy and technology to make information sharing easier. The FBI Strategy for Engagement with State and Local Fusion Centers reinforces the importance of interaction with fusion centers, using policy as well as technology to enhance sharing with mission partners. The FBI is also expanding efforts to develop and share criminal information through programs such as the Law Enforcement National Data Exchange (N-DEx). In addition, the FBI is an active participant in development of the Controlled Unclassified Information (CUI) concept and guidelines for its implementation. The CUI marking replaces multiple Sensitive But Unclassified (SBU) categories with a uniform designation, while the framework specifies the requirements for designating, marking, safeguarding, and disseminating information designated as CUI. The CUI marking and framework will standardize the manner in which the intelligence and law enforcement communities store, manage, and share sensitive but unclassified information.

C. Making Information Sharing More Effective

The ultimate purpose of improving information sharing is to enhance the security posture of our nation by defeating national security threats and criminal activity. The impact of improved information sharing at all levels was demonstrated in the close collaboration among mission partners during the terrorist threat investigations of 2009 and 2010. Increased effectiveness is largely an outcome of other facets of this strategy – reinforcing the information sharing culture to motivate sharing, and facilitating sharing through the skillful use of policy imperatives and technological capabilities. Advances in technology and policy refinements make more effective action possible. Stronger relationships resulting from enhanced trust and confidence enable

improved communications, increased cooperation, and more effective exchanges. The net effect enables more informed decisions and more effective action.

Since September 11th, intelligence operations have been transformed, with most efforts focused at the federal level. Less publicized are corresponding enhancements to state and local law enforcement intelligence operations, which enable state and local law enforcement agencies to play a role in homeland security and facilitate more effective response by local law enforcement to traditional crimes. The FBI Strategy for Engagement with State and Local Fusion Centers reinforces interaction and collaboration at the state and local levels. This is being extended to an enterprise strategy by incorporating several initiatives for improved engagement with the broader law enforcement community, including the Criminal Intelligence Coordinating Council. These changes in law enforcement intelligence relationships have improved not only crime response, but also the mutual exchange of information between federal and local partners.

An emerging effort at the FBI that will have a positive impact on internal information sharing is domain awareness. Domain awareness describes the landscape in which the FBI carries out its daily mission while providing context and a more-informed sense of the environment in which the threat conducts its activities. The purpose of the Domain Management / Domain Awareness initiative is to provide managers in the field with improved information for better resource alignment with threat priorities. Expanding domain awareness will improve the breadth, understanding, and scope of national security or criminal threats, and the FBI's ability to anticipate and neutralize them. This improved understanding and insight will position FBI professionals to more effectively share information and should have a positive impact on national security.

Trusted information sharing decreases information gaps by providing pertinent national or regional intelligence that gives context to identified threat activity in respective domains; facilitates responses to threats that transcend organizational boundaries; strengthens collaborative assessments of risk through improved access to data and analysis; fosters increased knowledge and domain awareness through improved access to data and analysis; and helps organizations standardize processes and align their respective goals with common purpose. Each party—law enforcement agencies and IC members; federal, state, local and tribal organizations, domestic and foreign partners—can better execute their respective missions while contributing to the safety of the U.S. as a whole.

Deeper understanding of the threat will enable wiser decisions and more effective action. Robust and collaborative partnerships, enhanced lawful sharing of information, and coordinated interactions that increase domain awareness will fortify national security.

III. CONCLUSIONS

Effective information exchange is an important component of the FBI's unique national security and law enforcement mission. The FBI is committed to sharing timely, relevant, and actionable intelligence with the widest appropriate audience. It is also committed to making the best possible use of information these partners share with the FBI.

In accordance with the principles of the National Intelligence Strategy, the FBI will continue to work to establish a more integrated national information sharing capability to ensure that those who need information to protect our nation from national security threats receive it and those who have that information share it. Further, information sharing activities at the FBI embody the commitment to operate at all times under the rule of law, respectful of privacy, civil liberties, and human rights, and in a manner that retains the trust of the American people.

The FBI NISS provides the goals and structure to initiate and implement information sharing activities and capabilities. This Strategy is multi-faceted and emphasizes reinforcement of a culture that encourages information sharing, makes information sharing easier through the focused use of information technology and policy, and makes information sharing more effective. By promoting an information sharing culture and by instituting policies, procedures and technical capabilities to empower it, the FBI is creating the climate necessary for its professionals to fully embrace their information sharing role and deepen their understanding of both threats and opportunities which will enable informed decisions and effective action to strengthen the national security of the United States.

APPENDIX A: INFORMATION SHARING ELEMENTS

The FBI is committed to sharing timely, relevant, and actionable intelligence with federal agencies; state, local, and tribal officials; foreign partners; and the private sector as part of its national security and law enforcement missions. The FBI's efforts to meet its information sharing mandates are an enterprise-wide activity.[2]

The National Security Council (NSC) and its Information Sharing and Access Interagency Policy Committee (ISA IPC) oversee collaboration among the major Executive Departments to enhance information sharing on all issues which impact national security. The Office of the Director of National Intelligence (ODNI) sets ground rules for the sharing of sensitive intelligence among the members of the IC, including the FBI. In particular, the ODNI Intelligence Community Information Sharing Steering Committee (IC ISSC) and the PM-ISE develop a coordinated position for information sharing activities within the IC and the information sharing environment.

Established by the Deputy Attorney General and sponsored by DOJ, the LEISP Coordinating Committee (LCC) promotes information sharing among law enforcement communities. DOJ's Global Justice Program sponsors a variety of initiatives that enhance FBI information sharing, ranging from the establishment of common data models to the establishment of the Criminal Intelligence Coordinating Council, a council of intelligence experts from state and local law enforcement.

Within the FBI, the Information Sharing Policy Board (ISPB) is chaired by the Executive Assistant Director (EAD) National Security Branch (NSB) and provides senior-level policy coordination, while the CISO serves as the principal advisor to FBI Executives for information sharing and coordinates Bureau information sharing activities, internally and externally.

The FBI Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) is a federal advisory committee established in accordance with the Federal Advisory Committee Act. The CJIS APB is responsible for reviewing policy issues and appropriate technical and operational issues related to the programs administered by the FBI's CJIS Division, and thereafter, making appropriate recommendations to the FBI Director.

[2] The CISO annual Information Sharing Report provides additional information regarding the important Information Sharing Elements.

APPENDIX B: REFERENCES

The Attorney General's Guidelines for Domestic FBI Operations, September 29, 2008.

Attorney General Memorandum, "The Attorney General's Guidelines for FBI Domestic Operations," September 29, 2008.

Bureau of Justice Assistance, Office of Justice Programs, Department of Justice, *Intelligence-Led Policing: The New Intelligence Architecture*; September, 2005.

Chief Information Sharing Officer, Federal Bureau of Investigation, *Information Sharing Report, 2009*.

Department of Justice, *Law Enforcement Information Sharing Program (LEISP)*, October, 2005.

Deputy Attorney General, Paul J. McNulty, Memorandum, "Law Enforcement Information Sharing Policy Statement and Directives" December 21, 2006.

Director of National Intelligence, Intelligence Community Directive Number 500, "Director of National Intelligence, Chief Information Office," Effective August 7, 2008.

Director of National Intelligence, Intelligence Community Directive Number 501, "Discovery and Dissemination or Retrieval of Information Within the Intelligence Community," Effective January 21, 2009.

Director of National Intelligence, Intelligence Community Policy Memorandum 2007-200-2, "Preparing Intelligence to Meet the Intelligence Community's Responsibility to Provide," December 11, 2007.

Director of National Intelligence, Intelligence Community Policy Memorandum 2007-500-3, "Intelligence Information Sharing," December 22, 2007.

Director of National Intelligence, *National Intelligence Strategy of the United States of America, August, 2009*.

Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy*, February 22, 2008.

Executive Order 13356, "Strengthening the Sharing of Terrorism Information to Protect Americans," August 27, 2004.

Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005.

FBI Corporate Policy Directive 0012D, "FBI Information Sharing Activities with Other Government Agencies," April 2, 2008.

FBI Corporate Policy Directive 0095D, "Protecting Privacy in the Information Sharing Environment," July 14, 2008.

Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law No. 110-53, August 3, 2007.

Information Sharing Environment Implementation Guide, November, 2006.

Information Sharing Environment Privacy Guidelines, December 4, 2006.

Information Sharing Executive, Office of the Chief Information Sharing Officer, Department of Defense, *Information Sharing Strategy*, May 4, 2007.

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law No. 108-458, December 17, 2004.

National Security Presidential Directive - 59 / Homeland Security Presidential Directive -24, "Biometrics for Identification and Screening to Enhance National Security," June 5, 2008.

National Strategy for Information Sharing, October, 2007.

Presidential Memorandum, "Designation and Sharing of Controlled Unclassified Information (CUI)," May 9, 2008.

Presidential Memorandum, "Strengthening Information Sharing with the Establishment of Two Program Management Offices," December 17, 2009.

APPENDIX C: ACRONYMS

AG	Attorney General
APB	Advisory Policy Board
CICC	Criminal Intelligence Coordinating Council
CISO	Chief Information Sharing Officer
CJIS	Criminal Justice Information Services
COI	Community of Interest
CUI	Controlled Unclassified Information
DNI	Director of National Intelligence
DOJ	Department of Justice
EAD	Executive Assistant Director
FBI	Federal Bureau of Investigation
IC	Intelligence Community
IC ISSC	Intelligence Community Information Sharing Steering Committee
ICO	Intelligence Community Officer
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISE	Information Sharing Environment
ISPB	Information Sharing Policy Board
ISSC	Information Sharing Steering Committee
IT	Information Technology
JTTF	Joint Terrorism Task Force
LCC	LEISP Coordinating Committee
LEISP	Law Enforcement Information Sharing Program
LES	Law Enforcement Sensitive
CISP	National Criminal Intelligence Sharing Plan
NIS	National Intelligence Strategy
NISS	National Information Sharing Strategy
NSB	National Security Branch
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
PIA	Privacy Impact Assessments