information sharing

INFORMATION SHARING ENVIRONMENT

ISE INFORMATION SHARING ENVIRONMENT

Annual Report to The Congress

Prepared by the
Program Manager, Information Sharing Environment

30 June 2011

Foreword

The threats against the American people and our institutions have compelled us to accelerate responsible information sharing across every level of government. The operators, analysts, and investigators who protect our nation need access to the right information at the right time, shared in a secure manner.

In the six years since the Congress called for the creation of the Information Sharing Environment (ISE), steady progress has been made to build a broad foundation for information sharing across the Federal Government, as well as with our state, local, and tribal partners, the private sector, and the international community. We have met many of our preliminary goals and milestones for sharing terrorism, homeland security, and weapons of mass destruction information – including those prescribed by Section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004, as amended, and those outlined in the 2007 *National Strategy for Information Sharing*. We are now building beyond the foundation to accelerate implementation of the ISE.

Threats do not differentiate between departmental or jurisdictional borders; rather, they are dynamic, often seeking to exploit those boundaries. We must work together, to standardize how we interact, to share best practices and to provide oversight and guidance across every level of government. I am proud to report that the Information Sharing and Access Interagency Policy Committee (ISA IPC) and other governance bodies have made great strides in institutionalizing common standards and solutions. This governance, policy, and strategy structure, which includes broad leadership from across the Federal Government, as well as participation from state, local, and tribal representatives, is a key component of the ISE and has been and will continue to be a driving factor in its success.

Several key initiatives of the ISE continue to mature, providing a more effective operating capability.

- The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) continues to implement standardized processes and policies that provide federal, state, local, and tribal law enforcement with the capability to share timely, relevant SAR information that has a potential nexus to terrorism, while ensuring that the privacy, civil rights, and civil liberties of Americans are protected.
- The PM-ISE, in coordination with federal partners, led the first nationwide Baseline Capabilities Assessment (BCA) of the national network of fusion centers (National Network). The BCA evaluated the maturity of the fusion centers' capabilities and identified gaps in an effort to aid fusion centers in better receiving, analyzing, disseminating, and gathering threat information for state, local, tribal, and territorial agencies. The results of the BCA led our partners to develop a Critical Operational Capabilities Gap Mitigation Strategy, which now guides efforts to build and strengthen capabilities in these critical areas.
- The ISE partners have accelerated the development and adoption of common standards and shared approaches to interoperable architectures through industry engagement and sharing of best practices across all levels of government.

We detail many other areas of progress in this Report, including improving the interoperability of our nation's Sensitive But Unclassified (SBU) and Secret networks; successes by the Interagency Threat Assessment and Coordination Group to strengthen information sharing between the Intelligence Community and state, local, and tribal law enforcement; and the tireless work of the terrorist watchlisting and screening community to streamline and standardize processes for information sharing while protecting the privacy, civil rights, and civil liberties of individuals.

While we have made great progress, we still face significant challenges. The unauthorized disclosure of classified information as a result of the WikiLeaks breach illustrates some fundamental failures to protect sensitive information properly and challenges our government to renew its focus on enhancing the means for the secure and effective use of information. While we cannot eliminate every insider threat, we have taken this opportunity to reassess our posture, our progress toward our goals, and our focus on responsible information sharing and protection.

We are building our mitigation efforts, and numerous corrective actions have been instituted across the Federal Government. We are seizing the momentum of existing efforts to strengthen responsible, trusted, and secure information sharing through efforts like data tagging and managing access to classified information and systems.

We will continue to work closely with our partners to build capacity, strengthen governance, and improve performance. Our roadmap for this will be a new National Strategy for Information Sharing and Protection, which we are currently drafting in close coordination with our ISE mission partners. Our partners have called for holistic solutions, including opening the aperture to the totality of terrorism-related information, focusing on critical capabilities like data aggregation and moving to an enterprise data management approach.

Our partners in public safety organizations are facing significant challenges with fiscal constraints forcing drastic budget cuts. State, local, and tribal public safety executives acknowledge that fundamental changes are required to meet the new realities of policing, including improved operational interoperability through proactive strategies, virtual consolidation, and shared services. We are in a position to support the national public safety and law enforcement community in the development of a common, distributed, decentralized information sharing system that builds upon existing technologies, better aligns and leverages existing efforts, and reinvents the public safety model for the 21st century.

We are continuing to work together, at every level of government, to accelerate the delivery of the ISE in a strategic and focused way.

Kshemendra Paul
Program Manager,
Information Sharing Environment

Table of Contents

Executive Summary

This Fifth Annual Report to the Congress on the state of the Information Sharing Environment (ISE) is submitted in accordance with requirements in Section 1016(h) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, and Section 210D(c) of the Homeland Security Act of 2002, as amended. This Report builds upon the mission partner accomplishments highlighted in the 2010 Report and reflects:

- Progress on ISE implementation by the bureaus and agencies of federal, state, local, and tribal governments and our private-sector and international partners;
- Collective accomplishments of the terrorism and homeland security information sharing and access community;
- Individual agency initiatives that stand out as best practices in information sharing and help form the fabric of the ISE; and
- Successful partnerships between the PM-ISE and federal and non-federal mission partners, involving terrorism, homeland security, and weapons of mass destruction (WMD) information sharing.

The Program Manager, Information Sharing Environment (PM-ISE) facilitates the development of the ISE by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices. Consistent with the direction and policies issued by the President and the Office of Management and Budget (OMB), the PM-ISE issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE. The ISE is realized by the investment of mission partners—the bureaus and agencies of federal, state, local, and tribal governments and our partners in the private sector and internationally—and is used by front line law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel.

This Report describes information sharing progress since July 2010. The Report is organized into five central themes:

1. Strengthening Management and Oversight
2. Improving Information Sharing Activities
3. Establishing Standards for Responsible Information Sharing and Protection
4. Enabling Assured Interoperability Across Networks
5. Enhancing Privacy, Civil Rights, and Civil Liberties Protections

Strengthening Management and Oversight

In strengthening the management and oversight of the ISE, the PM-ISE actively governs, integrates performance and investment, engages stakeholders, and encourages a culture of information sharing.

Governance: The Information Sharing and Access Interagency Policy Committee (ISA IPC) is the interagency forum for overseeing the planning and implementation of the ISE. The ISA IPC formally charters Sub-Committees to provide advice and support to the IPC on a range of related issues within their designated portfolios, and inform ISE planning and implementation. ISA IPC Sub-Committees have formed a number of Working Groups to address discrete issues or topics within the Sub-Committees portfolio.

Since January 2011, ISA IPC Sub-Committees and Working Groups have organized and managed their efforts, and are reporting their accomplishments on a quarterly basis in line with annual and longer-term objectives and goals for the ISE. In accordance with IRTPA Section 1016, several of the ISA IPC Sub-Committees and Working Groups include participation by representatives of non-federal organizations in order to ensure adequate consultation and representation from all ISE stakeholders.

More than half of the ISE departments and agencies have dedicated information sharing offices, directorates, divisions or executives. The establishment of a single office to ensure full cooperation in the development of the ISE is considered a best practice and is encouraged across the ISE.

- In October 2010, the Director of National Intelligence (DNI) strengthened the responsibilities and title of the Intelligence Community (IC) Information Sharing Executive.
- The Federal Bureau of Investigation (FBI) established an ISE and a Chief Information Sharing Officer position in 2008 to coordinate internal and external information sharing policy issues. In February 2011, the Directorate of Intelligence (DI) created a new DI Branch, the Intelligence Integration Branch (IIB), to enhance sharing and outreach efforts. The IIB is specifically charged with engaging federal, state, local, tribal, and IC partners to increase the effectiveness of information sharing and also to coordinate efforts to combat violent extremism.

Performance and Investment Integration: Each year, OMB and the National Security Staff issue programmatic guidance for the federal budget describing ISE priority areas. The implementation of this guidance moves each of the agencies closer to collaborative endeavors—eliminating redundancies, identifying reuse options, leveraging best practices, and consolidating similar projects across organizational boundaries. Partner agencies continue to strategically invest in the ISE and to indicate alignment of their information technology investments to the ISE priorities. Initial use of enhanced Exhibit 53 reporting allowed analysis of federal agency information technology spending aligned to ISE priorities.

The ISE continues to employ a performance management process to report on results. The PM-ISE monitors performance across strategic investments, mapping the ISE strategic vision to initiatives and outlining clear measures.

Stakeholder Engagement: The PM-ISE engages ISE mission partners through live events across the country, roundtables, the ISE website (www.ISE.gov), and the use of social media. This year, PM-ISE placed a special emphasis on engagement with industry. Standards organizations and industry consortia

assist mission partners in developing, coordinating and maintaining technical standards, and provide a means to communicate ISE requirements to industry while providing industry with a means to communicate potential solutions to ISE mission partners.

Refreshing the Strategy: In 2010, the Executive Office of the President asked the PM-ISE to refresh the 2007 *National Strategy for Information Sharing* in order to outline an updated vision and strategy for responsible information sharing and protection. Input from our ISE mission partners is critical to ensure that this refreshed strategy supports the counterterrorism mission and provides complete solutions for ISE mission partners. To accomplish this, the PM-ISE invited partners to provide their vision for the ISE, as well as input on various topics for incorporation into the new Strategy.

Culture: Achieving a culture in which responsible information sharing is the norm rather than the exception is a major goal of IRTPA. Federal agencies continue to expand their programs to include information sharing and collaboration as part of the recruitment, orientation, and performance evaluation of all employees; to increase and improve mission specific training programs; to encourage the use of incentive awards for collaborative efforts; to encourage joint duty-like assignments to foster knowledge sharing; and to create communities of interest around particular topics.

Improving Information Sharing Activities

The PM-ISE's responsibilities extend to addressing and facilitating improved information sharing between and among the intelligence, defense, homeland security and law enforcement communities. Significant progress has been made toward building a broad foundation for information sharing across the Federal Government, as well as with state, local, tribal, private sector, and international partners.

Suspicious Activity Reporting: The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) provides analysts, operators and investigators with another tool to "connect the dots" in the course of combating crime and terrorism by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR in a manner that rigorously protects the privacy, civil rights, and civil liberties of Americans. The NSI has made substantial progress toward standardizing ad hoc methods of reporting and analysis, and implementing these standards, policies, and processes within fusion centers. It has also developed training for front line officers, analysts, and chief executives regarding the behaviors and indicators of terrorism related criminal activity. To date, nearly 50,000 officers have received line officer training.

Over the past year the NSI Program Management Office (PMO) has also been coordinating closely with the Department of Homeland Security (DHS) on the "If You See Something, Say Something™" campaign—a simple and effective program to raise public awareness about indicators of terrorism, crime, and other threats, and to emphasize the importance of reporting suspicious activity to the proper authorities.

The FBI and the NSI PMO are integrating the FBI's eGuardian system to enhance information sharing among all mission partners in order to protect the security of the homeland. This initiative helps formalize the sharing of information currently taking place between state, local, and tribal partners, and leverages the already successful relationships between SLT partners and the FBI's Joint Terrorism Task Forces.

National Network of Fusion Centers: Located in state and major urban areas throughout the country, fusion centers are uniquely situated to empower front line law enforcement, public safety, fire service, emergency response, public health, Critical Infrastructure and Key Resources (CIKR) protection, and private-sector security personnel to understand local implications of national intelligence, enabling local officials to better protect their communities. In September 2010, federal, state, and local officials completed a Baseline Capabilities Assessment (BCA)–the first nationwide, in-depth assessment of fusion centers to evaluate fusion center capabilities and to establish strategic priorities for Federal Government support. Based on the results, fusion centers made progress in building their capabilities and in addressing identified gaps.

In 2010, all 56 FBI field offices conducted self-assessments on their relationship with fusion centers, providing a comprehensive understanding of how the FBI is currently engaging with fusion centers. The FBI plans to continue close collaboration at both the field office and headquarters levels to standardize processes; clarify procedures; and facilitate more effective engagement with fusion centers.

One of the Federal Government's priorities for coordinating support to fusion centers was to clearly define the parameters for the allocation of federal resources to fusion centers. The Fusion Center Sub-Committee of the ISA IPC developed the Federal Resource Allocation Criteria policy, which defines objective criteria and a coordinated approach for prioritizing the allocation of federal resources to fusion centers.

Representatives from federal, state and local agencies—including High Intensity Drug Trafficking Areas (HIDTAs), fusion centers, the DHS, the White House Office of National Drug Control Policy (ONDCP), the Department of Justice (DOJ), the FBI, the National Drug Intelligence Center (NDIC), and the PM-ISE—met in February to explore how best to leverage fusion centers and HIDTAs as uniquely valuable resources and partners. As a result of their discussions, these partners are continuing to build and formalize relationships within their states through business plans and concepts of operation to enhance intrastate coordination and execution of the statewide fusion process.

Interagency Threat Assessment and Coordination Group (ITACG): The ITACG facilitates information sharing between federal, state, local, tribal, and private-sector partners. Since March 2010, DHS Intelligence and Analysis (I&A) has solicited feedback on every intelligence product it has released, including products the ITACG is involved in producing. State and local feedback has been positive. Nearly 99 percent of the DHS products are either integrated into state and local finished intelligence products; shared with partners; or used for situational awareness, security preparations, or training purposes. Fusion center directors also indicated that reporting has become more frequent, more relevant, and more concise.

The Congress has recently expressed interest in knowing whether ITACG personnel have access to the information they need, within the scope of the ISE. ITACG personnel are exposed to the main stream of intelligence at the National Counterterrorism Center (NCTC). A significant indicator of the ITACG's access to information is their involvement with a special site exploitation effort currently ongoing at NCTC.

The second edition of the *Intelligence Guide for First Responders,* published in 2011*,* incorporates feedback from the field, and includes two new sections: "Reporting Suspicious Activity," which covers

participation in the NSI, and "Joint Partnerships," which highlights several joint federal, state, local, and tribal activities around the country.

Tribal Information Sharing: This past year the PM-ISE dedicated efforts to building a community to increase cooperation between federal, state, local, and tribal law enforcement agencies. The National Law Enforcement Telecommunications System (Nlets) links together state, local and federal law enforcement, justice and public safety agencies. This year, the first connectivity pilot program between four tribes in separate regions of the United States and Nlets was established.

PM-ISE has partnered with the NSI PMO to administer the NSI Line Officer Training to all tribal law enforcement partners, as an attempt to further integrate Indian Country into the NSI. Integration of tribal law enforcement personnel in fusion centers has occurred successfully in Oklahoma, Arizona, and Washington State.

Multimodal Information Sharing: ISE mission partners are pursuing information sharing initiatives aimed at protecting and reducing vulnerabilities at our borders, ports, and airports, and enhancing overall transportation security.

In January 2011, the Next Generation Air Transportation System (NextGen) Joint Planning and Development Office (JPDO) kicked off an effort to develop a Concept of Operations (CONOPS) for the Integrated Surveillance Initiative.

The U.S. Customs and Border Protection, U.S. Coast Guard, and Immigration and Customs Enforcement components of DHS are engaged in the Joint Targeting Architecture Project to improve information sharing relating to targeting protocols and procedures at seaports where the agencies have distinct authorities to protect the United States against persons, cargo, and other dangers posed by seaborne vessels.

The Multimodal Information Sharing Taskforce (MIST) is an interagency research effort designed to foster collaboration and to capture best practices in information sharing in a regional port environment. MIST has identified a number of best practices for collaboration, including the U.S. Customs Trade Partnership Against Terrorism program, the expansion of industry-run education programs for government employees, and the inclusion of industry in emergency preparedness activities and Integrated Operations Centers.

Weapons of Mass Destruction (WMD) Information Sharing: The PM-ISE supports DHS's Domestic Nuclear Detection Office by funding the initiation of their inter-governmental information sharing exchange. This mechanism will facilitate and standardize the real-time sharing of radiological and nuclear alarm adjudication data, as well as shipment and licensee data, and will improve analysis of post-seizure data.

Intelligence Community (IC) Intelligence Sharing Services: A variety of IC intelligence sharing services provides analysts, operators, and investigators on-demand electronic dissemination applications to facilitate information sharing at and across all levels of security. For example, NCTC CURRENT is the premier classified resource for counterterrorism (CT) reporting and analysis throughout the IC. *Intelligence Today*, the daily online compendium of analytic products from across the IC, marked its first anniversary on 22 March 2011 by posting its 48,450th article. Intelink recently crossed the 100 million

document threshold for records exposed to Intelink search services across the Unclassified, Secret, and Top Secret networks combined. In one month alone this year, Intelink recorded over two million searches. These milestones highlight the ability of IC personnel to access more information quicker and more effectively, enabling them to better share information and thus perform their missions.

Watchlisting and Screening: Since the development of the consolidated terrorist watchlist that is in use today, there have been many successes and improvements to watchlisting processes. Some of the more recent improvements include clearer definitions of the roles and responsibilities of federal agencies, streamlining and standardizing nominations processes, improving the use of biometrics for identification, and improving analytical and technological capabilities.

Private-Sector Information Sharing: Last year, the Office of the Director of National Intelligence (ODNI) and DHS I&A jointly established a program to develop partnerships between members of the private sector and teams of experienced IC analysts. The goal of this effort is to provide IC analysts with a better understanding of select national and homeland security-related industries.

The CIKR ISE is making substantial progress in providing useful critical infrastructure protection and resilience content to an increasing number of critical infrastructure sector partners to identify their risks, reduce their vulnerabilities, and respond to and recover from incidents.

Foreign Partner Information Sharing: Foreign partners are vital in the effort to combat terrorism by sharing key information, conducting surveillance, collaborating with U.S. overseas air passenger and maritime cargo screening, arresting members of terrorist cells, interdicting terrorist financing and logistics, and contributing to efforts in Afghanistan, Iraq, and other key places around the world. In February 2011, President Obama and the Prime Minister of Canada released the *Beyond the Border Declaration: A Shared Vision for Perimeter Security and Economic Competitiveness*, which identified information sharing, particularly along our shared border, as a key priority between the United States and Canada. The ISE is currently developing an online knowledge base that describes important core concepts, approaches, and best practices of the ISE, including governance, standards, policy, budget, performance management, privacy policies, and a process for SAR.

Recognizing the value that the National Information Exchange Model (NIEM) could provide for facilitating information sharing within the Canadian and Mexican governments and along their borders with the United States, both Mexico and Canada have shown interest in adopting NIEM in the public safety, law enforcement, and defense and disaster management domains.

Law Enforcement Information Sharing: The FBI's Criminal Justice Information Services (CJIS) is the focal point for some of the most important and relevant criminal history databases used by law enforcement. CJIS's National Data Exchange System (N-DEx) is a criminal justice information sharing system that provides nationwide connectivity to disparate local, state, tribal, and federal systems for the exchange of information. In March 2011, the final increment of the N-DEx system was delivered, increasing its power, speed, and accessibility while greatly improving the user's information-sharing experience.

Programs like the Technical Resource for Incident Prevention (TRIPWire), the National Law Enforcement Telecommunications System (Nlets), the Law Enforcement Information Sharing Initiative (LEISI) the Domestic Highway Enforcement Initiative (DHE), and INTERPOL I-24/7 have also provided significant improvements in information sharing.

In the wake of the tragic Fort Hood shootings in November 2009, a Department of Defense (DoD) board reviewing the incident cited the need to "adopt a common force protection threat reporting system for documenting, storing, and exchanging threat information. In 2010, the FBI's eGuardian system was selected by DoD.

Homeland Security Standing Information Needs: Documenting information needs is key to enabling effective information sharing. In 2010, DHS reorganized its Homeland Security Standing Information Needs into10 topics that align with the information needs of consumers. In November 2010, DHS launched a SINs development initiative for the private sector. This initiative included actively engaging interagency governmental partners, as well as owners and operators from the 18 CIKR sectors.

Establishing Standards for Responsible Information Sharing and Protection

PM-ISE is working with mission partners and standards organizations to identify the best existing standards for reuse and implementation across the ISE.

Advancing Existing Standards for Information Sharing and Protection: Functional standards set forth rules, conditions, guidelines, and characteristics of data and mission products to support ISE business process areas. The number of departments and agencies that are incorporating functional standards into the management and implementation of ISE-related mission business processes has steadily increased over the past year. The ISE Functional Standard for Suspicious Activity Reporting (ISE-SAR) is an example of a functional standard now advanced by mission partner-specific efforts via the NSI.

Coordination of Standards to Enable Interoperable Capabilities: Recognizing the critical role of standards in enabling the ISE and mission partner operations, in May 2011 the ISA IPC approved the creation of a Standards Working Group to coordinate efforts across departments, agencies, and levels of government.

The National Information Exchange Model (NIEM): NIEM is gaining significant adoption as a common framework for information sharing for a number of state, local and tribal agencies. In May 2011, PM-ISE collaborated with the NIEM PMO and members of the Object Management Group (OMG), a consortium of both industry and government members, in an effort to develop a Unified Modeling Language (UML) profile for NIEM that will further NIEM success and adoption.

PM-ISE is currently working with its mission partners on a strategic sourcing approach based on industry standards and implementation profiles. Strategic approaches like these will allow mission partners to procure products that are interoperable, cost-effective, and policy and standards-compliant.

Identity, Credential and Access Management: This year, the PM-ISE convened the leaders associated with the multiple logical access related management activities of the Federal Government. Leaders agreed to a broad vision of enabling these different standards to ultimately become aligned across all levels of government so that users accessing data could be authenticated and authorized appropriately for access.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) charts a course for the public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions.

Security, Auditing and Cross-Domain Frameworks: Information security and assurance helps partners manage connections between what data people are allowed to access and share, in a way that promotes responsible information sharing across partners. In August 2010, the President issued Executive Order (EO) 13549 "Classified National Security Information Program for State, Local, Tribal and Private Sector Entities," to all federal departments and agencies, which establishes a program designed to safeguard and govern access to classified national security information shared by the Federal Government with state, local, tribal, and private-sector entities.

Significant progress in the area of security reciprocity continued over the past year as evidenced by continued promulgation of harmonized National Institute for Standards and Technology (NIST)-Committee on National Security Systems (CNSS)-Intelligence Community Directive (ICD) standards. Progress also has continued with regard to developing the policy and procedural framework for reciprocity for information systems security.

Recently promulgated IC standards implement uniform information security requirements and procedures concerning audit information in the IC information environment, and address the use of collected audit data for insider threat detection. The IC's experience in audit functions presents an opportunity for leveraging best practices for other federal, state, and local networks to improve the overall assurance of the ISE.

Enabling Assured Interoperability Across Networks

The Information Integration Sub-Committee (IISC) of the ISA IPC coordinates high priority interagency efforts to accelerate the delivery of the ISE, including interoperability among Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI) and Secret networks, identification of best practices in support of data aggregation activities, and advancement of industry-based standards in support of all ISE activities.

Data Aggregation: The mission to disrupt terrorist acts before they occur is enabled by finding, sharing and collaborating on data that comes from trusted and reliable mission partners. The goals of data aggregation in the ISE are achieved through an established governance process that enables mission partners to obtain the data, through shared ISE enterprise services, that is necessary to perform their missions while protecting the privacy of persons for whom no nexus to terrorism exists.

Under the joint leadership of DHS and ODNI, the Data Aggregation Working Group (DAWG) was formally approved and chartered by IISC to focus on capabilities that are entity (identity)-focused, and to employ automated data discovery, data characterization, data correlation, and disambiguation algorithms to aggregate information from multiple domains into a mission-specific enterprise-level analytic service. The DAWG has completed a review of the U.S. Government oversight and governance structures that provide strategic policy as well as technical and mission guidance for terrorism-related data aggregation, data integration and data management efforts.

As DAWG identifies best practices and lessons learned, it is expected that mature technical solutions, that can be shared across the ISE will be identified.

Assured Secret Network Interoperability: The ability to effectively and responsibly share classified information among federal and non-federal mission partners is a key capability needed to support the counterterrorism mission and homeland security. In 2010 the ISA IPC chartered the Assured Secret Network Interoperability Working Group (ASNI WG) to serve as a forum for federal agencies operating Secret networks to work together to develop governance, to resolve interoperability issues, and to support assured information sharing among federal Secret networks. Over the past nine months, the ASNI WG has delivered a number of key incremental accomplishments towards increasing interoperability and information sharing. For example, ASNI WG partnered with the Fusion Center Sub-Committee to document, validate, and prioritize fusion center information needs. This establishes the foundational requirements needed to inform the development of technical connectivity and access to sensitive information for fusion centers.

The ASNI WG also supported progress on mission capabilities for fusion centers including: improved access to white-listed sites on DoD's Secret network, the Secret Internet Protocol Router Network (SIPRNet), via DHS's Homeland Secure Data Network (HSDN); preserved and expanded fusion center access via HSDN to *NCTC CURRENT* during its relocation to SIPRNet; expanded Secret-level video-conferencing capabilities as a shared service between FBI's Secret network and HSDN for fusion centers; and new access to the FBI's white pages and email directories through HSDN.

Assured Sensitive but Unclassified (SBU) Network Interoperability: The multiple SBU/CUI networks, portals, and systems currently in existence contain a rich variety of data and services. However, differences in policy and technology prevent authorized users from gaining access to many of those resources without having to individually log on to these multiple systems, using multiple credentials. The ability to login just once to an approved system, and to be granted access to an interoperable and protected SBU/CUI environment, commonly referred to as Simplified Sign On (SSO), is an overarching requirement for federal, state, local, and tribal law enforcement officers and analysts.

Over the past year, the Assured SBU Network Interoperability Working Group has made significant progress towards achieving SSO. For example, in December 2010, CJIS's Trusted Broker Version 2 became operational, providing SSO capabilities by allowing law enforcement online users to access Intelink-U, RISSNET, and many other systems. The Assured SBU Network Interoperability Working Group tracks the effectiveness of their efforts by monitoring a set of user metrics that are collected from partners on a monthly basis. Those metrics have been designed by the SBU partnership to indicate progress towards interoperability goals and to assist in fine-tuning particular interoperability efforts.

Controlled Unclassified Information (CUI): On 4 November 2010, President Obama signed EO 13556 "Controlled Unclassified Information," establishing a CUI program to manage all unclassified information that requires safeguarding and/or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. The EO identifies National Archives and Records Administration (NARA) as the Executive Agent to implement the EO and to oversee departmental and agency actions to ensure compliance.

On 9 June 2011, the NARA's CUI Office issued the "Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556." In the coming months, the CUI Office will lead an interagency process to establish an Executive Branch-wide definition and taxonomy of categories for CUI, and departments and agencies will submit CUI compliance plans by 6 December 2011. Federal agencies are expected to initiate efforts to develop CUI guidance specific to their agency and unique mission requirements.

Enhancing Privacy, Civil Rights, and Civil Liberties Protections (P/CR/CL)

IRTPA aims at the broadest possible sharing of information for counterterrorism purposes. It also explicitly recognizes that such sharing must respect P/CR/CL protections. A critical step in the safeguarding of P/CR/CL is the development and adoption of a written P/CR/CL policy that meets the standards of the White House ISE Privacy Guidelines. Nine out of 14 ISE departments and agencies have reported that they have developed ISE Privacy Policies. These agencies have also made measurable progress in implementing the ISE Privacy Policies by modifying business processes and updating sharing agreements to align with the new policies.

State, local, and tribal partners have worked to develop privacy policies that are "at least as comprehensive as" the ISE Privacy Guidelines, a standard prescribed as a prerequisite for receiving terrorism-related information from federal entitites. For example, all operational state and major urban area fusion centers were determined to have privacy policies that are "at least as comprehensive as" the ISE Privacy Guidelines. The NSI PMO has also worked diligently with NSI participants to implement all of the elements of the NSI Privacy Framework for SAR.

All federal agencies reported that personnel receive training with a specialized privacy and civil liberties protection component at least annually.

The Privacy and Civil Liberties (P/CL) Sub-Committee was established under the ISA IPC in September 2010. Over the past year, the P/CL Sub-Committee has established three working groups: the Privacy and Civil Liberties Legal Issues Working Group, the Privacy and Information Technology Working Group, and the Compliance Review Working Group.

Ten Year Anniversary of 9/11

> The biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information.[1]

"We have some planes!" The full import of that ominous sentence, spoken at 8:25 AM on September 11, 2001, by the hijacker pilot of American Airlines Flight 11, was not fully understood by Federal Aviation Administration and airline officials until more than a half hour later when Flight 11 had already crashed into the North Tower of the World Trade Center, United Airlines Flight 175 had crashed into the South Tower, and American Airlines Flight 77 was bearing down on Washington, DC for an attack on the Pentagon.[2] But those words were the first indications that the Nation was confronting multiple hijackings for the first time in its history and that the most devastating attack on the U.S. Homeland since Pearl Harbor—one that would kill almost 3,000 people from more than 70 countries —was underway.[3]

There is another quote from that day that serves as an effective counterweight. It was spoken by Todd Beamer to Lisa Jefferson shortly before 10:00 AM. Hearing on their cell phones of the earlier attacks, Beamer and fellow passengers on the fourth hijacked plane, United Airlines Flight 93, realized that the hijackers intended to use the plane to attack another target, possibly the U.S. Capitol or the White House, and decided to take action. The last words he spoke still resonate today as symbols of courage, resilience, and initiative in the face of chaos and mortal danger: *"Are you guys ready? Let's roll!"* Beamer and his fellow passengers then assaulted the cockpit, sacrificing their lives to thwart the hijacker's plans when the plane crashed in an open field near Shanksville, Pennsylvania.

The U.S. response to the events of 9/11 both honors and emulates the attitude and actions of Todd Beamer and his fellow passengers. We honor them by remembering and celebrating the lives and heroic actions of the victims, survivors, and families; we then seek to fully understand what happened and how

---

1 9-11 Commission Report, July 2004

2 *National Commission on Terrorist Attacks upon the United States*. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004. pp. 1-14. Available at http://www.9-11commission.gov/report/911Report.pdf.

3 "9/11 By the Numbers," http://nymag.com/news/articles/wtc/1year/numbers.htm

and why it did; and finally we have taken and continue to take the actions necessary to minimize the chances of it happening again.

The 9/11 Commission Report, issued in the summer of 2004, concluded that a combination of factors—not one single cause—prevented us from detecting and preventing the planned attack. One of the factors cited by the Commission as among the "most serious weaknesses" leading to the attacks was a breakdown in information sharing among federal agencies and with state, local, and tribal governments. The Commission specifically called for "unifying the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional government boundaries," the first reference to what would eventually become the Information Sharing Environment (ISE).[4] Removing legal, policy, procedural, and technological impediments to more effective sharing of terrorism-related information—in a way that still protects national security and privacy and civil liberties—thus became, and continues to be, one of the major focuses of the effort to help protect our nation against future attempts by terrorists.

This effort cuts across all levels of government and extends to the private sector and to international partners. It has been notably bi-partisan, championed by both Democratic and Republican administrations and congressional leaders. Even before the Commission Report was issued, Congress had taken preliminary steps to address some of the known information sharing deficiencies - both the USA PATRIOT Act and the Homeland Security Act of 2002 included provisions that improved information sharing among government agencies.[5]

It was, however, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) that gave the effort its focus and strategic direction. IRTPA implemented many of the Commission's specific recommendations including establishing an ISE for terrorism-related information and requiring the President to designate a program manager (PM-ISE) to "plan for and oversee the implementation of, and manage, the ISE," thus positioning the ISE as a critical part of the Nation's efforts to combat terrorism. Six years after passage of IRTPA, some of the most significant barriers to federal, state, local, tribal, and private sector collaboration have already fallen and others are being aggressively addressed by the PM-ISE and mission partners.

On 1 May 2011 Osama Bin Laden was killed near Abbottobad, Pakistan. In the words of President Obama, "Tonight, we give thanks to the countless intelligence and counterterrorism professionals who've worked tirelessly to achieve this outcome. We give thanks to the men who carried out this operation, for they exemplify the professionalism, patriotism, and unparalleled courage of those who serve our country. And they are part of a generation that has borne the heaviest share of the burden since that September day."[6]

---

4 9/11 Commission Report, p.400.

5 USA PATRIOT Act, PL 107-56, (October 26, 2001), Section 314, et al. and Homeland Security Act of 2002, PL 107-296, (November 22, 2002) Section 891, et al.

6 http://www.whitehouse.gov/the-press-office/2011/05/02/remarks-president-osama-bin-laden

In his remarks on the Senate floor regarding the resolution honoring the members of the military and the Intelligence Community (IC) who carried out the mission, Senator Reid stated, "Resolution is an appropriate name for this legislation. It honors the resolution to a problem that has lingered for nearly a decade—one whose weight has grown heavier each day on the shoulders of the families Osama Bin Laden traumatized and the many more he terrorized."[7]

The operation that resulted in Bin Laden's death was a significant achievement by the IC who collaborated across agencies to gather and analyze the information needed to conduct the assault. DNI Clapper stated, "In my nearly 50 years in intelligence, I have never seen a more remarkable example of focused integration, seamless collaboration, and sheer professional magnificence as was demonstrated by the Intelligence Community in the ultimate demise of Osama Bin Laden."[8] Former Central Intelligence Agency Director Panetta added, "The raid was the culmination of intense and tireless effort on the part of many Agency officers over many years…Along with our partners at the NGA [National Geospatial-Intelligence Agency], NSA [National Security Agency] and ODNI [Office of the Director of National Intelligence], we applied the full range of our capabilities (and) produced the results that the American people expect of their intelligence service."[9]

Notably, the co-chairs of the 9/11 Commission also connected the successful operation to the implementation of the intelligence reforms that included the creation of the ISE. In a joint statement they concluded, "As a result of these reforms, there is much closer collaboration between intelligence and military components of the Federal Government."[10]

Nearly 10 years after the attacks of 9/11, our government is challenged by the evolving nature of terrorism. While al Qaeda itself continues to threaten the United States, al Qaeda also inspires an array of affiliated terrorist groups and there is an escalation of a significant new threat that takes advantage of radicalized violent Islamic extremists within our borders.[11] We will remain vigilant and continue to work to ensure that terrorism-related information, properly managed and protected, is shared in time to be used effectively to counter threats to our people and institutions. We will do this consistent with our open society, federated democracy, equality, and traditional American values of democracy and individual liberties. In this endeavor we must work with all the energy and commitment that the challenge demands. We can do no better than to adopt as our guiding maxim the words of Todd Beamer—"Are you guys ready? Let's roll!"

---

7 http://democrats.senate.gov/newsroom/record.cfm?id=332678

8 http://www.dni.gov/press_releases/20110502_release_clapper.pdf

9 https://www.cia.gov/news-information/press-releases-statements/press-release-2011/justice-done.html

10 This statement is available at http://www.nydailynews.com/opinions/2011/05/09/2011-05-09_winning_the_postbin_laden_war.html

11 Hearing of the Senate Homeland Security And Governmental Affairs Committee, Subject: "Nine Years After 9/11: Confronting The Terrorist Threat To The Homeland," September 22, 2010

1 Introduction

"President Obama's highest priority is to keep the American people safe. Effective and efficient information sharing and access are essential to enhancing the national security of the United States and the safety of the American people. As we move forward together on this important issue, it will be important that we make tangible, meaningful progress on the development of an effective information sharing environment."

– John Brennan, Deputy National Security Advisor for Homeland Security and Counterterrorism, and Assistant to the President (2 July 2009)

1.1 Purpose and Scope of the Information Sharing Environment (ISE)

This Fifth Annual Report to the Congress on the state of the ISE is submitted in accordance with requirements in Section 1016(h) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended[12] and Section 210D(c) of the Homeland Security Act of 2002, as amended.[13] This Report builds upon the mission partner accomplishments highlighted in the 2010 Report and reflects:

- Progress on ISE implementation by the bureaus and agencies of federal, state, local, and tribal governments and our private sector and international partners;
- The collective accomplishments of the terrorism and homeland security information sharing and access community;
- Individual agency initiatives that stand out as best practices in information sharing and that help form the fabric of the ISE; and
- Successful partnerships between the PM-ISE and federal and non-federal mission partners, involving terrorism, homeland security, and weapons of mass destruction (WMD)-information sharing.[14]

12 Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, P.L. 108-458 (December 17, 2004), §1016(h).

13 Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, sec. 210D(c), codified as amended at 6 U.S.C. 124k(c), details specific reporting requirements pertaining to the Interagency Threat Assessment and Coordination Group (ITACG).

14 The IRTPA definition of Terrorism Information encompasses all terrorism-related information "whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities," and was explicitly amended in 2007 to include Weapons of Mass Destruction information. For brevity, these types of information are collectively referred to as "terrorism-related" information.

This year, the Program Manager, Information Sharing Environment (PM-ISE) orchestrated a comprehensive effort to ensure broad-based agency participation in compiling the Annual Report. To most accurately report progress on the extent to which the ISE has been implemented, we used inputs from the 2011 ISE Annual Performance Assessment Questionnaire, which was issued to ISE departments and agencies; we solicited input from the ISE governance bodies that define goals for and monitor the progress of ISE mission partners; and we solicited descriptions of accomplishments from all mission partners, federal and non-federal, to ensure the best possible representation of the state of the ISE and information sharing across the enterprise.[15] In addition, we leveraged data collected by the Office of Management and Budget (OMB) to determine the extent to which ISE priorities are being incorporated into agency Information Technology (IT) budgets.

Scope of the ISE

As depicted in Figure 1, the ISE provides integrated terrorism-related information to support analysts, operators and investigators as they carry out their responsibilities across the law enforcement/public safety, defense, intelligence, homeland security, and diplomacy communities. The ISE facilitates information sharing among federal agencies; across all levels of government—federal, state, local, and tribal; as well as with our private-sector partners and our international allies.

Figure 1. Scope of the ISE

The ISE comprises any mission process, anywhere in the United States, that is intended or is likely to have a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity. Examples include: terrorism watchlisting, person and cargo screening, suspicious activity reporting (SAR), and alerts, warnings and notifications.

15 IRTPA Sec 1016(i) requires the head or each department or agency that participates in the ISE to submit, at the request of PM-ISE, any reports on the implementation of the requirements of the ISE within its department or agency.

The ISE in Action

- ✓ A law enforcement officer conducting a routine traffic stop, queries the National Crime Information Center and is told to contact the Terrorist Screening Center to evaluate a potential match against the Terrorist Watchlist
- ✓ An intelligence analyst uses the Library of National Intelligence, or A-Space, to collaboratively develop new intelligence products
- ✓ Coast Guard personnel responding to the Gulf oil spill leverage DHS's Homeland Security Information Network and Federal Emergency Management Agency's (FEMA) Web Emergency Operations Center (these technologies and applications support ISE mission partners when responding to both man-made and natural disasters)
- ✓ A local law enforcement analyst, a DHS Intelligence Officer, and an FBI Analyst, co-located at a fusion center, collaborate to develop finished intelligence products that support FBI Joint Terrorism Task Force investigations and to inform line officers of potential indicators and warnings of terrorist threats
- ✓ A local law enforcement officer notices a suspicious activity and submits the information through eGuardian for vetting against the ISE-SAR Functional Standard.

The PM-ISE facilitates the development of the ISE by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices. Consistent with the direction and policies issued by the President and the Director of the Office of Management and Budget, the PM-ISE issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE.[16] The PM-ISE serves as a change agent and center for innovation and discovery in providing ideas, tools, and resources to mission partners and assists them in removing barriers, facilitating change, and ensuring that ISE implementation proceeds efficiently and effectively. The PM-ISE ensures that the ISE is built to improve sharing and protection of terrorism, homeland security, and weapons of mass destruction (WMD) information.

A practical way to think of the ISE is as an infrastructure and capability – analogous to the Interstate highway system. The ISE represents the structure and "rules of the road" – including commonly understood road signs, traffic lights, and speed limits – that allow information traffic to move securely, smoothly, and predictably. PM-ISE is not pouring the concrete – rather, it is providing leadership and

16 IRTPA Section 1016 (f)(2) requires the Program Manager to assist in developing policies, as appropriate, to foster the maturity and proper operation of the ISE.

coordinating a complex set of factors that make the highway safe and navigable: governance and engagement, strategy and policy alignment, business process harmonization, and guidelines, standards, and architecture. This leadership and coordination enables our mission partners – the general contractors building and managing the day-to-day operation of the highways – to build to common specifications. If built properly, everyone can use the roads within appropriate mission and policy context. Indeed, like other infrastructures, the ISE is a public good and has the potential to pay dividends by supporting information sharing and protection beyond its initial mission space. Terrorism-related information can flow between partners, as can other classes of information such as those related to non-terrorism intelligence and law enforcement while ensuring the protection of privacy, civil rights, and civil liberties.

PM-ISE enables our mission partners to better perform their operations by facilitating access to information and services that contribute toward our shared anti-terrorism mission.

Our tools in this effort are: governance and engagement; strategy and policy alignment; business process harmonization; guidelines; standards; and architecture.

In January 2005, the Government Accountability Office (GAO) designated terrorism-related information sharing as "high risk" because it determined that there were serious challenges in analyzing key information and sharing it among federal, state, local, and other security partners in a timely, accurate, and useful way in order to protect against terrorist threats. During the 2011 review, GAO found that the government has made progress during the past two years in sharing terrorism-related information among its many security partners, but that it does not yet have a fully-functioning environment in place. To facilitate the development of this environment, PM-ISE co-chairs, with the National Security Staff (NSS), the ISA IPC, which governs its direction and progress; and also partners with OMB.

It is primarily through the OMB/NSS–PM-ISE partnership that program direction, funding, and performance measurement are effectively achieved. Departments and agencies are responsible for developing, deploying, modifying and maintaining their respective investments; they play an active role in determining the policies, priorities, and direction of the ISE and are an integral part of the ISA IPC. In addition, the information they share and the tools used to share it are, by their nature, a part of the ISE. Working with OMB/NSS to provide integrated, cross-government guidance, we establish a framework for departments and agencies investments within the ISE. OMB/NSS programmatic guidance, our policy framework, and the ISE standards and guidelines provide the tools to effectively manage performance throughout the ISE and the ISA-IPC. These strategies, together with ISA IPC governance, the commitment of departments and agencies, and the above mentioned tools, support the strategic roadmap toward achieving a more robust ISE.

1.2 ISE Mission Partners

It is the mission of the bureaus and agencies of federal, state, local, and tribal governments, in cooperation with the ISE's mission partners in the private sector and internationally to help protect our people and our institutions. These agencies build, own and operate the ISE, and are accountable for information sharing that will enable end-to-end mission processes that support counterterrorism (CT).

The support of mission partners is critical to the success of the ISE. They have mission responsibility and a vital leadership role for the delivery, operation, and use of the ISE, and are accountable for delivering value by aligning policy, processes, and information. While the law granted the PM-ISE government-wide authority—a unique capability allowing the office to work with existing programs to facilitate assured information sharing—the actual point of implementation, the heavy lifting, is with mission partners. They are the engines that deliver the ISE. It is the agencies that conduct mission operations, develop and implement policy and procedures, and make investments to interconnect systems, networks, databases, and business processes.

> The ISE is realized by the investment of mission partners—the bureaus and agencies of federal, state, local, and tribal governments and our partners in the private sector and internationally—and it is made relevant through its use by front line law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel.

In the six years since the Congress directed the creation of the ISE, mission partners have taken significant steps toward establishing a strong foundation. Important mission initiatives, such as the Nationwide SAR Initiative (NSI), and core capabilities and enablers, such as the National Network of fusion centers, the Federal Bureau of Investigation's (FBI) Field Intelligence Groups (FIGs) and Regional Intelligence Groups (RIGs),[17] and the National Information Exchange Model (NIEM), have produced results and show ongoing promise. PM-ISE's role is to help mission partners find common mission equities, to help them implement functional and technical standards, and to drive resolution of policy issues.

Throughout this Report, mission partner achievements are highlighted to emphasize the many incremental steps taken throughout the ISE to build capabilities and ensure information sharing across domains and mission equities. The hallmark projects and achievements within the ISE have often been developed through many steps involving smaller combined efforts that have a significant cumulative effect. In the same way, we recognize the breadth of work and the investment our mission partners make to constantly enhance the success of the ISE. They are the essential pieces in a very large and important puzzle.

17 In 2010, the FBI created six Regional Intelligence Groups for the purpose of identifying regional threats and to facilitate information sharing from a national and local perspective. RIGs are also establishing a strong record in creating intelligence products regarding domain awareness to the state and local community, including the fusion centers. Information from the RIGs is also coordinated through the FIGs.

1.3 Strengthening Information Sharing and Information Protection

One of the biggest roadblocks to expanding information sharing is the fear by many agencies that other organizations will fail to adequately protect the information they are provided with. As the WikiLeaks story emerged, concerns were voiced that information sharing efforts would suffer a setback. This Administration is committed to improving information sharing by better protecting the information that is shared. Guidance throughout the Executive Branch has been consistent: we must continue to accelerate our information sharing in a responsible and secure way. As reinforced by Senate Homeland Security and Governmental Affairs' Chairman Lieberman, Ranking Member Collins, Secretary of Defense Gates, OMB Director Lew, and Director of National Intelligence Clapper, we must champion efforts to further strengthen information sharing as well as to protect that information.

"To ensure we share and protect information effectively, we must work to find the sweet spot between the two." – DNI Clapper

The WikiLeaks disclosures primarily involved classified information, but the fundamental challenges associated with sharing and protecting sensitive information span across all security domains. Missions do not stop at the security domain or at organizational boundaries. Fundamental policies and solutions should be framed to address all types of protected information, classified and unclassified, held by the Federal Government and by our state, local, tribal, private sector, and international mission partners. Across all mission partners, we need to establish structural elements such as strong governance, strategy, and policy to promote common, comprehensive solutions and to discourage individual agency-based, bilateral, and fragmented approaches.

PM-ISE is leading the process, along with ISE mission partners, of developing the National Strategy for Information Sharing and Protection, which will update and replace the 2007 *National Strategy for Information Sharing*. While the new Strategy is still under development, it is clear that to make the ISE work, we need to focus on information –discovering it, sharing it, protecting it, fusing it, and reusing it. The ISE needs an information-centric approach in alignment with the original mandate for the ISE. Further, to "open the aperture" to the totality of terrorism-related information as directed by law, efforts must continue to enhance partnerships with mission partners across all five communities—law enforcement/public safety, defense, intelligence, homeland security, and diplomacy. Moving forward, solutions must have broad applicability to a variety of mission needs, including CT and homeland security.

1.4 Structure of this Report

Building the ISE is not a short-term effort. It is a process that must evolve and adapt to emerging technologies and threats. To remain relevant and effective, enhancements and extensions to the foundations of the ISE are critical. While we celebrate the achievements and progress made towards sharing information and disrupting terrorist attacks, we also recognize that improvement is always both possible and necessary.

This Report describes information sharing progress since July 2010, including information on major ISE projects and activities launched by mission partners that have contributed significantly to inter-governmental information sharing. The Report is organized into five central themes encompassing the specific requirements set forth in IRTPA, the guidelines and requirements supporting the creation and implementation of the ISE[18] and the guiding principles and foundational elements included in the 2007 *National Strategy for Information Sharing*:

1. Strengthening Management and Oversight
2. Improving Information Sharing Activities
3. Establishing Standards for Responsible Information Sharing and Protection
4. Enabling Assured Interoperability Across Networks
5. Enhancing Privacy, Civil Rights, and Civil Liberties Protections

While primarily focused on terrorism-related initiatives, the Report also describes mission partner accomplishments, some of which may not have been developed explicitly to support CT, but which may ultimately become "best practices," with applicability to information sharing and collaboration government-wide, including within the ISE.[19]

Classified Supplement

The PM-ISE is responsible for reporting on the state of the ISE and information sharing across the Federal Government. To more accurately inventory important developments that encompass terrorism-related information sharing, it is necessary to include a classified supplement that will be sent to Congress under a separate cover letter.

18 White House Memorandum for the Heads of Executive Departments and Agencies, SUBJECT: Guidelines and Requirements in Support of the Information Sharing Environment, 16 December 2005

19 The fact that the ISE can leverage these achievements is consistent with one of its key attributes identified in IRTPA—to build upon existing systems capabilities currently in use across the government.

2 Strengthening Management and Oversight

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, established the position of a Program Manager to "plan for and oversee the implementation of, and manage" the Information Sharing Environment (ISE), and to be "responsible for information sharing across the Federal Government."[20] Consistent with the direction and policies issued by the President, the Director of National Intelligence (DNI), and the Director of the Office of Management and Budget (OMB), the Program Manager, Information Sharing Environment (PM-ISE) issues government-wide procedures, guidelines, instructions, and functional standards,[21] as appropriate, for the management, development, and proper operation of the ISE. In strengthening the management and oversight of the ISE, the PM-ISE actively governs, integrates performance and investment, engages stakeholders, and encourages a culture of information sharing.

ISA IPC members include:

- Central Intelligence Agency
- Department of Commerce
- Department of Defense
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of the Interior
- Department of Justice
- Department of State
- Department of Transportation
- Department of Treasury
- Federal Bureau of Investigation
- General Services Administration
- Joint Chiefs of Staff
- National Counterterrorism Center
- Office of the Director of National Intelligence

2.1 ISE Governance

The ISE is realized by the investment of mission partners and made relevant through its use by front line law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel. To effectively coordinate and govern the many information sharing activities, the PM-ISE has been leading interagency policy harmonization.

2.1.1 Information Sharing and Access Interagency Policy Committee (ISA IPC)

The ISA IPC is the interagency forum for overseeing the planning and implementation of the ISE. The ISA IPC was formed by a White House memo in 2009[22], which integrated the existing Information Sharing Council (ISC) established by IRTPA into the IPC framework and

20 IRTPA §1016(f)

21 Ibid.

22 White House Memorandum, "Strengthening Information Sharing and Access," 2 July 2009

strengthened national information sharing efforts by bringing the work of the ISC's Sub-Committees and working groups under the auspices of the Executive Office of the President (EOP). The ISA IPC prioritizes interagency efforts and aligns policy to facilitate the implementation of the ISE.

In its capacity as the ISC, the ISA IPC formally charters Sub-Committees to provide advice and support to the IPC on a range of related issues within their designated portfolios, and inform ISE planning and implementation. Sub-Committees are generally chaired by ISE mission partners and supported by PM-ISE staff. The ISA IPC directs the actions and tasks assigned to the Sub-Committees and regularly monitoring their progress on goals and objectives.

ISA IPC Sub-Committees have formed a number of Working Groups to address discrete issues or topics within the Sub-Committees portfolio. For example, on 1 June 2011, PM-ISE hosted an information sharing and protection Standards Summit, kick-starting a new interagency working group across federal, state, local, and tribal government representative partners, focused on identifying "best of breed" information sharing standards in government. Unlike other federal initiatives which focus on standards for just one set of partners, this working group will include all federal as well as state, local, and tribal government representative partners. This initiative will reuse the best existing government standards for responsible information sharing and protection, refine them, and encourage industry adoption of their standards into commercial products the government can buy with interoperable standards "baked-in" from the start.

Figure 2 shows the Sub-Committees and Working Groups of the ISA IPC. The five Sub-Committees and their corresponding Working Groups are discussed in greater detail in this chapter and throughout this Report.

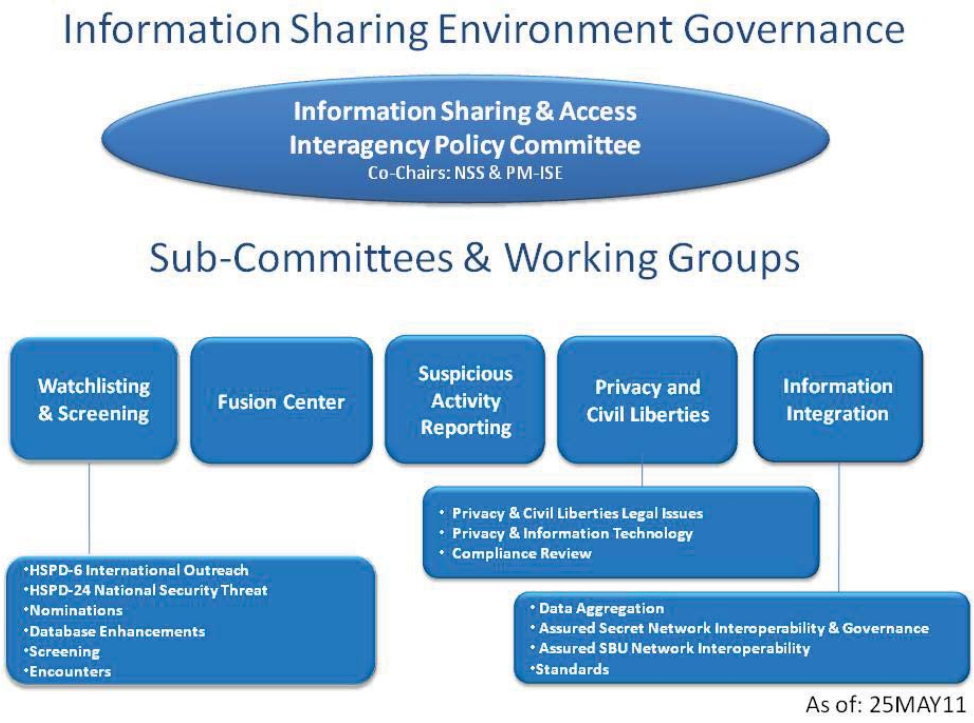


Figure 2. ISA IPC Sub-Committees and Working Groups

Since June 2010, the PM-ISE has served as a co-chair of the ISA IPC, along with a counterpart from the White House National Security Staff (NSS). This dual role for the PM-ISE is an acknowledgment that policies, business practices, architectures, standards, and systems developed for the ISE can be applicable to other types of information beyond terrorism and vice versa, because the scope of the IPC is broader than the scope of the ISE.[23] As co-chair, the PM-ISE helps ensure that there will be the closest possible alignment between the ISE and broader national security information sharing activities.

Since January 2011, ISA IPC Sub-Committees and Working Groups have organized and managed their efforts and report their accomplishments on a quarterly basis in line with annual and longer-term objectives and goals for the ISE. Sub-Committees and Working Groups derive these key objectives and areas of responsibility in the form of concrete goals aligned to the mission needs as specified in the annual ISE programmatic guidance, the *National Strategy for Information Sharing*, and priorities specified by the Administration. This process is discussed in the Performance and Investment Integration section below.

2.1.2 Working with State, Local, and Tribal Partners

Several of the ISA IPC Sub-Committees and Working Groups communicate and coordinate closely with representatives of non-federal organizations because they are recognized as valued partners by all ISE stakeholders. These representatives are chosen because they are members of an association, an advisory committee, or a wholly-owned national subsidiary of state or local governments. These representatives function as spokespersons for nongovernmental groups or stakeholders, providing the views and perspectives of their respective entities.

As of this Report, the following non-federal organizations coordinate closely with select ISA IPC Sub-Committees and working groups:

- **Criminal Intelligence Coordinating Committee (CICC)** – Fusion Center Sub-Committee and the SAR Sub-Committee
- **Global Justice Information Sharing Initiative (GLOBAL)** – Fusion Center Sub-Committee, SAR Sub-Committee, Information Integration Sub-Committee (Standards Working Group)
- **Regional Information Sharing Systems (RISS)** – Information Integration Sub-Committee (Assured SBU Network Interoperability Working Group)

23 White House Memorandum, Subject: Appointment of the Program Manager, Information Sharing Environment (3 June 2010)

2.1.3 Interdependencies

Responsible information sharing is cross cutting and a number of dependencies can be found across the ISE governance organization. A key role of Sub-Committee and Working Group Chairs is to assist the ISA IPC in identifying these interdependencies and to collaborate on developing solutions. For example, a joint effort of the Assured Secret Network Interoperability Working Group of the Information Integration Sub-Committee and the Fusion Center Sub-Committee led to the development of the *State, Local, Tribal User-Validated Fusion Center Mission Requirements Initiative* report. This document communicates fusion center information needs to federal mission partners and application owners, and informs the technical access and connectivity solutions that are being developed by the Federal Government to securely share information with fusion centers.

2.1.4 Department and Agency Information Sharing Offices

More than half of the ISE departments and agencies have dedicated information sharing offices, directorates, divisions or executives. These offices serve as focal points for federal information sharing issues and direct department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards. The establishment of a single office to ensure full cooperation in the development of the ISE is a best practice and is encouraged across the ISE.

In October 2010, the DNI strengthened the responsibilities and title of the Intelligence Community Information Sharing Executive (IC ISE). The IC ISE is now directly accountable to the Principal Deputy Director of National Intelligence and works in close coordination with the Deputy Director of National Intelligence for Intelligence Integration, the Assistant Directors of National Intelligence, the PM-ISE, and IC elements. The IC ISE is developing a coordinated and comprehensive plan for responsibly managing information sharing activities within the ODNI, across the IC, and with all of its mission partners. To this end, the IC ISE has established an internal governance process, the Information Sharing Executive Group, for ensuring a coordinated information sharing approach within ODNI, and has refashioned and reinvigorated the IC ISE's engagement activities and governance across the IC, via the Information Sharing Steering Committee, to do the same. A close working relationship with PM-ISE helps ensure that information sharing and protection activities within the IC are consistent and interoperable with the steps being taken across the entire U.S. Government, as well as with state, local, tribal, and private-sector partners.

The Department of Homeland Security (DHS) designated the Under Secretary for Intelligence and Analysis (USIA) to concurrently serve as the Department's Information Sharing Executive. In that capacity, the USIA chairs the Department's Information Sharing Governance Board (ISGB), which was established in 2007 to serve as the Department's senior-level governance body for information sharing. The ISGB develops departmental policy recommendations and resolves issues involving information sharing across DHS components, as well as with federal state, local, tribal, territorial, private-sector and foreign partners. For the past year, the ISGB has identified information sharing priorities using the Quadrennial Homeland Security Review strategic framework. To continue to strengthen and mature the

information sharing governance structure, the ISGB is working to ensure that the Department's information sharing priorities are integrated within the Department's overall, Planning, Programming, Budgeting and Execution processes and are reflected in the Future Year's Homeland Security program. DHS also works closely with the PM-ISE to ensure alignment and coordination with the ISE. In January 2011, the DHS Chief Information Officer (CIO) established and filled an Information Sharing Executive position to ensure the removal of technical barriers associated with implementing the ISE.

The FBI established an ISE and a Chief Information Sharing Officer (CISO) position in 2008 to serve as the senior FBI official for information sharing and the principal advisor to FBI executives for information sharing matters. The CISO is the Executive Secretary of the FBI's Information Sharing Policy Board and coordinates internal and external information sharing policies. In February 2011, the Directorate of Intelligence (DI) created a new DI Branch, the Intelligence Integration Branch (IIB), to enhance information sharing and outreach efforts. The IIB is specifically charged with engaging federal, state, local, tribal, and IC partners to increase the effectiveness of information sharing and to coordinate efforts to combat violent extremism.

2.1.5 Other Interagency Policy Coordination and Implementation Bodies

In addition to using the ISA IPC as the primary interagency policy coordination body for information sharing and access, ISE mission partners also coordinate through a number of other IPCs related to national information sharing and protection functions. These include: the Transborder Security Portfolio's IPC, and its associated Sub-IPCs and associated working groups, which include topics such as maritime security, surface transportation, global supply chain, and aviation security; the Records Access and Information Security IPC, which addresses the protection and handling of sensitive information; the Information Communications Infrastructure IPC, which addresses cybersecurity issues; the Critical Infrastructure Protection and Resilience IPC; and the Countering Nuclear Threat IPC.

Additionally, PM-ISE coordinates with strategic and tactical efforts across interagency governance bodies that involve information sharing and access issues. These bodies include: the Federal CIO Council and its component committees, including the Information Security and Identity Management Committee; the IC CIO Council and its component committees; the Committee on National Security Systems (CNSS) and its component working groups; the Unified Cross Domain Management Office; the National Information Exchange Model (NIEM) Program Management Office at DHS, and the Controlled Unclassified Information (CUI) Program Office at the National Archives and Records Administration (NARA). By leveraging these bodies, PM-ISE ensures that equities related to information sharing and access are fully coordinated and that they are represented consistently across all federal departments and agencies and across all related disciplines, without duplicating efforts.

2.2 Performance and Investment Integration

Governance and decision-making across the ISE are supported by the integrated performance and investment process, shown in Figure 3. The PM-ISE actively monitors agencies' progress toward information sharing performance objectives and goals and ensures the integration of performance with investment.

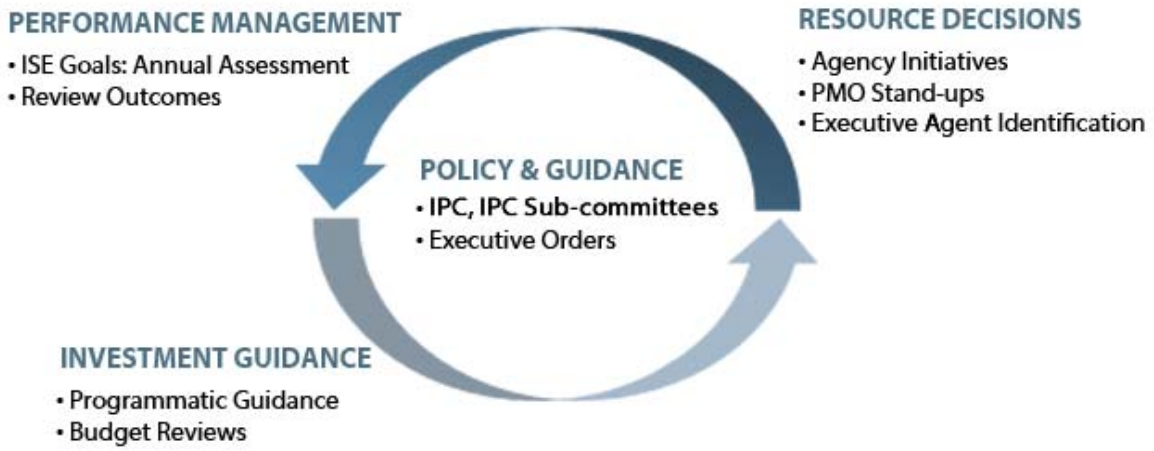


Figure 3. Performance and Budget Integration Process

2.2.1 Three-way Partnership (Agencies, OMB/NSS, and PM-ISE)

The ISE continues to embrace the whole of government approach as documented in the President's May 2010 National Security Strategy. Jointly, ISE member agencies, OMB/NSS, and PM-ISE are defining the way forward and have demonstrated their commitment to an interagency process dedicated to information access and sharing. The governance and decision-making process, tightly interwoven with budget and performance integration, has been keeping pace with this progress.

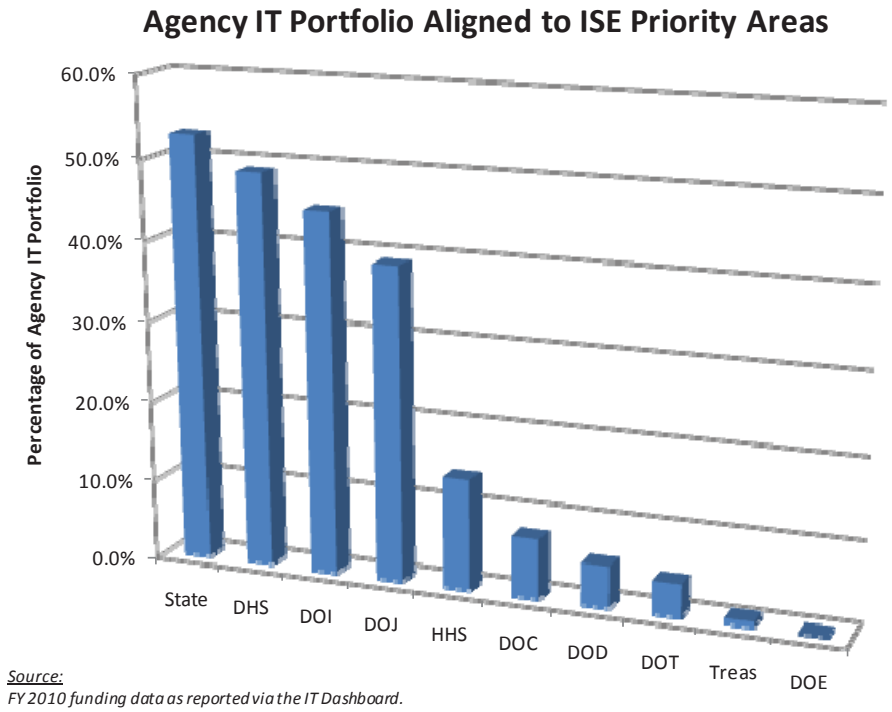
Performance and investment processes focus on ensuring that the ISE continues to make progress in advancing its goals and objectives. The ISE programmatic guidance, annual budgets and investments, and committee and staff work plans for each subsequent year are developed based on the prior year accomplishments and any relevant changes in policy, strategy, technology, and other external factors.

2.2.2 Programmatic Guidance

To codify the initiatives in the President's Budget, OMB/NSS issues programmatic guidance each year for the federal budget describing ISE priority areas. It provides direction to agencies for future spending on mission priorities, critical information resources, and supporting information technology investments focusing on increased federal collaboration with state, local and tribal governments, as well as with the private sector. The implementation of this programmatic guidance through the governance process moves each of the agencies closer to collaborative endeavors—eliminating redundancies, identifying re-use options, leveraging best practices, and consolidating similar projects across organizational boundaries.

Last year, ISE programmatic guidance was issued to agencies for the development of their fiscal year (FY) 2012 budget submissions. The FY 2012 ISE-specific programmatic guidance identified the following five priorities:

1. Building a national integrated network of fusion centers;
2. Continuing implementation of the NSI;
3. Establishing Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI) network interoperability; [24]
4. Improving governance of the classified National Security Information program; and
5. Advancing implementation of CUI policy.



Source:
FY 2010 funding data as reported via the IT Dashboard.

Figure 4. Percentage of the federal agencies' IT budget aligned with at least one of the ISE priority areas

24 On 4 November 2010, President Obama issued Executive Order 13556, "Controlled Unclassified Information," which addresses a broad scope of activities related to information previously labeled "Sensitive But Unclassified (SBU). On 9 June 2011, the CUI Office issued the "Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556." In implementing this guidance, references to "Sensitive But Unclassified (SBU)" will be phased out in future PM-ISE reporting.

2.2.3 Strategic Investment

Partner agencies continue to strategically invest in the ISE and indicate alignment of their information technology investments to the ISE priorities via OMB's annual agency Information Technology (IT) portfolio data request. The data captured via the OMB Circular A-11 Exhibit 53[25] reporting for FY 2012 is only one step of many used to understand the ISE priority area costs of mission partners. This data revealed that approximately 15 percent of the Federal Government IT spending is aligned to one or more of the ISE priorities. As reported by agencies, Figure 4 depicts the percentage of their agency's IT budget that is aligned with at least one of the ISE priority areas. This chart illustrates that several agencies—e.g. State, DHS, Department of the Interior (DOI) and the Department of Justice (DOJ)—continue to align a substantial portion of their IT budgets to the ISE priority areas.

Initial use of the enhanced Exhibit 53 reporting allowed analysis of federal agency IT spending aligned to the ISE priority areas focuses around the primary functional mappings to the lines of business (LOB) within the Federal Enterprise Architecture Business Reference Model (FEA BRM). As anticipated with IT investments, the strongest primary mapping was attributed to the FEA BRM IT management LOB (38 percent), as depicted in Figure 5. IT management is broad; it captures the coordination of information and technology resources and systems to support or provide a service.[26] The two largest sub-functions under the IT management LOB are IT Infrastructure Maintenance (30 percent) and Information Sharing (3 percent). The analysis also revealed significant primary mapping to other mission LOBs such as Homeland Security (18 percent), Community and Social Services (9 percent), Health (7 percent) and Law Enforcement (6 percent), demonstrating a focus of these investments toward advancing agency mission areas. Further analysis and improved data quality in future reporting will help to identify potential opportunities for investment decisions in these areas.

25 OMB Circular A-11 Section 53, 21 July 2010 (http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s53.pdf)

26 Federal Enterprise Architecture Consolidated Reference Model v2.3, October 2007 (http://www.whitehouse.gov/omb/e-gov/fea/)

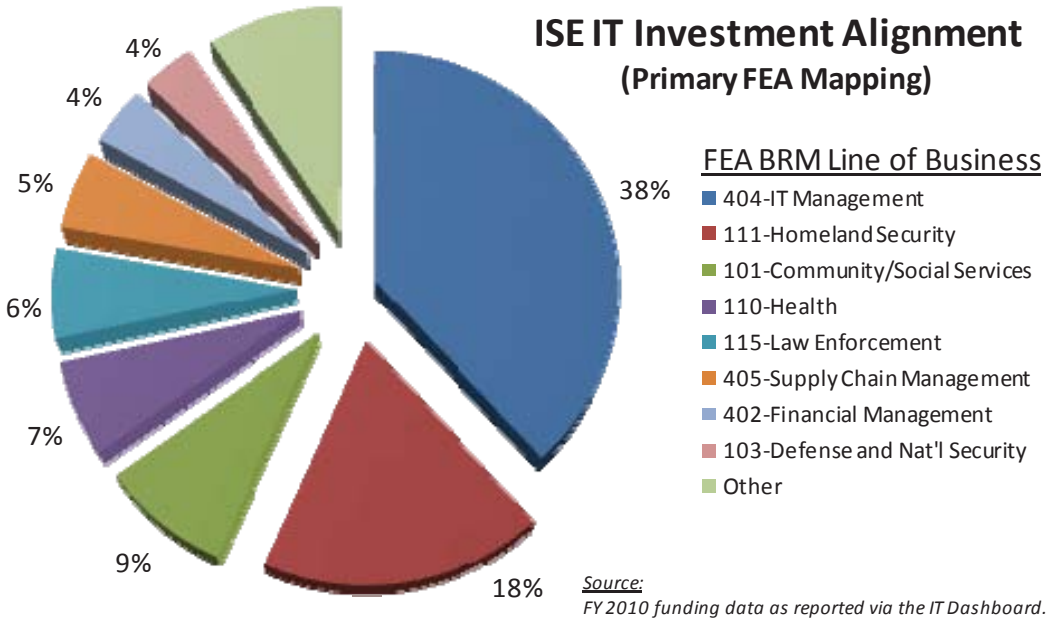


Figure 5. ISE IT Investment Alignment

Two of the ISE priority areas, SBU Interoperability and CUI, accounted for the vast majority of IT spending alignment. This is expected, as investments in these ISE priority areas tend to be larger, agency-wide IT initiatives. More detailed analysis will enable better understanding of how strategic investments in these areas can be effectively utilized, and how those investments can be encapsulated in larger IT infrastructure investments.

Based on agency reporting via the OMB Exhibit 53, depicted in Figure 6, more than half of agency IT investments aligned to ISE priority areas directly supported agency-specific mission objectives. This is an important perspective, as agencies with alignment to ISE priorities are focusing investments and resources toward supporting their mission objectives that capture the value of the ISE, versus focusing on supporting infrastructure-type activities.

Table 1 – Investments aligned to the SBU priority area

Agency	SBU Investments
Department of Commerce	2
Department of Defense	1
Department of Energy	16
Department of Homeland Security	99
Department of the Interior	3
Department of Transportation	11
Department of Treasury	10
Federal Bureau of Investigation	16

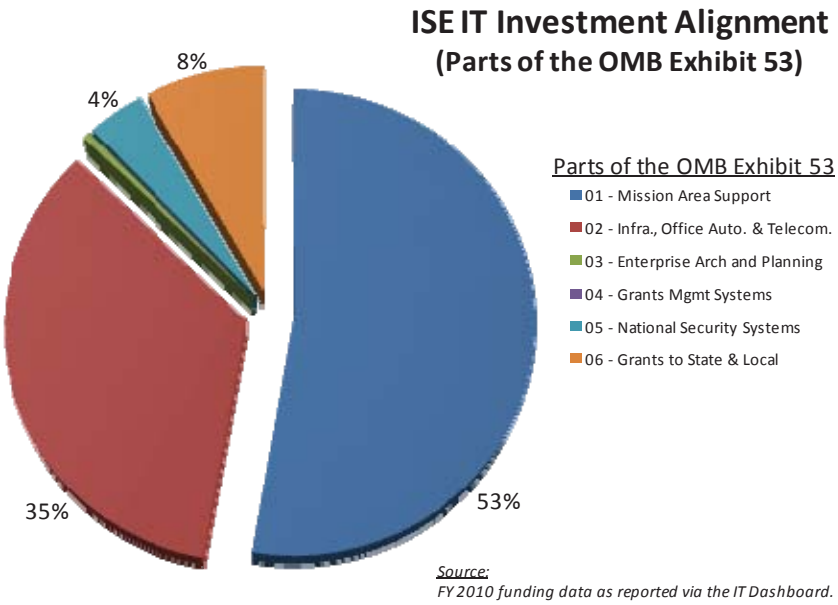


Figure 6. ISE IT Investment Alignment to Parts of OMB Exhibit 53

Continued collection of this data year-after-year will allow for trend analysis of programmatic efficiencies to better understand and account for ISE spending. For example, working closely with OMB/NSS, PM-ISE was able to focus on the ISE priority area for SBU systems, networks and portals. The initial funding submissions revealed 182 investments aligned to the SBU priority area. Based on this data, the PM-ISE created SBU inventory worksheets for agency validation and the current revised number of SBU investments is 158 investments, as depicted in Table 1. DHS identified the largest number of SBU investments, but already has efforts underway to reduce and consolidate the number of SBU systems. For example, the Homeland Security Information Network (HSIN) program, as a result of the Federal CIO TechStat session and recommendations in the 25 Point Plan to Reform Federal IT, has retooled its management and technical approach for the development of the new HSIN platform to ensure continuous user input and feedback, delivery of functionality in shorter timeframes, and will address recommendation that balance the need to share versus safeguard. Further analysis into the services and capabilities provided by these investments could potentially yield additional opportunities for increased SBU interoperability within and across partner agencies.

As data quality improves, PM-ISE analysis will be able to further identify gaps and areas of opportunities for strategic investments in innovative information sharing technologies and programs. Initial understanding of these gaps has led to focused investments for innovative ideas in the priority areas of cargo screening, SAR, standards, and privacy. Going forward, PM-ISE will continue to support innovative opportunity areas for advancements in ISE focus areas. The PM-ISE is working closely with OMB to improve the quality of data in subsequent cycles, and to support the strengthened use of data in resource allocation and planning processes.

2.2.4 Performance Management

The ISE continues to employ a performance management process to report on results. This will flow from the new National Strategy for Information Sharing and Protection (as discussed later in this chapter) and the priorities defined by the White House. As this process matures, ISE partners and stakeholders will be held accountable by monitoring operation and maintenance; self-reporting; mitigation of risks; and exercising the ISE through a combination of quantitative and qualitative measures. Each initiative will be assessed, measuring its progress and value to the overall ISE.

The PM-ISE works closely with each ISE agency to obtain feedback and gather insights on improving the processes and measures, with the intent of influencing the performance at each of the agencies. The results of this year's annual performance assessment can be found throughout this Report and in Appendix A.

The PM-ISE will continue to revise the existing performance framework to ensure alignment and build upon previous performance measurement best practices. The PM-ISE will monitor performance across strategic investments, mapping the ISE strategic vision to initiatives, and outlining clear measures. This systematic approach requires a clear strategic vision to define the expected mission capabilities, and requires full representation and performance measurement of all the ISE initiatives.

The Performance Framework will consist of the following four views:

1. **ISE Strategic View**: Defines the vision and scope and answers the questions, "Why?" and "Toward what outcomes are we working?"
2. **Initiative View**: Defines a work-breakdown structure that answers the question, "What are we doing to achieve the vision?"
3. **Measure View**: Describes the value to the community and answers the question, "How well are we doing in terms of achieving the vision?"
4. **Roadmap View**: Presents a schedule of the priority work that remains to be completed.

Because the ISE has made substantial strides in maturity, this effort will not only measure current progress, but also the community's collective capacity to achieve mission capabilities.

2.3 Stakeholder Engagement

Stakeholder engagement has remained a top priority for the ISE community this year and will continue to be a key component for strengthening management and oversight of the ISE in the months and years ahead. As such, the PM-ISE has focused on building a multi-tiered governance and engagement strategy driven by mission partners and inclusive of the technology industry.

First, the PM-ISE brings the voice of the analysts, operators, investigators, practitioners, and subject matter experts from across communities to a collective table. Regular engagement with these communities of interest (COIs), formed to promote collaboration, provides ISE mission partners with advice and recommendations on specific topics, activities, and operational needs. In January 2011, the PM-ISE met with the Executive Director of the International Association of Chiefs of Police (IACP). At this meeting a number of common goals were identified and related transactions were put into place to establish a partnership. For example, the IACP is now a listed partner on the ISE website, and information sharing success stories told in *Police Chief's* magazine (the official publication of the IACP) are highlighted on the ISE website.

The ISE also provides a means for mission partners to regularly communicate and collaborate with industry. Standards development organizations assist mission partners in developing, coordinating and maintaining technical standards that address the interests of their varied users.

Emphasis on Industry

This year, the PM-ISE placed a special emphasis on engagement with standards organizations and industry consortia. Standards organizations assist mission partners in developing, coordinating and maintaining technical standards that address the interests of their varied users. Industry consortia provide a means to communicate ISE requirements to industry and provide industry with a means to communicate potential solutions to mission partners. From here, mission partners can develop mission-driven requirements, standards and processes for the ISE which industry can then use for product development.

As COIs naturally form around agencies, mission partners, and ISE initiatives based on their specific domains of activity, PM-ISE strives to engage these communities through live events and roundtables scheduled across the country; the ISE website; and the use of social media. The PM-ISE has actively engaged with representatives from every level of government; state, local, and tribal partners; industry; international allies; and the public. The Program Manager, or his delegate, has spoken at more than 40 events, reaching thousands of people. In the last year, the PM-ISE participated in the Law Enforcement Information Management Conference, the National Fusion Center Conference, Integrated Justice Information Systems (IJIS) Institute Briefings, the DoD Identity Protection and Management Conference, and many others. A list of events is included in Table 2.

The PM-ISE also recognizes that the community does much of its work online. This venue for communications enables bi-directional interaction and is critical for bringing our state, local, tribal, and international partners together with industry. Online tools are an essential complement to direct outreach enabling us to support the interaction called for by IRTPA, Section 1016. Accordingly,

www.ise.gov received various upgrades and enhancements over the last year, and the site has become a robust, collaborative tool for our mission partners and stakeholders.

Intelink Symposium	Cisco Public Service Summit	Excellence in Government	Averting Armageddon
Google Innovation for the Nation	Central Command Visit	FBI InfraGard Critical Sector Forum	Special Operations Command Visit
National Fusion Center Conference	West Virginia Fusion Center Opening	GLOBAL Executive Steering Committee	National Indian Gaming Conference
Symantec Government Symposium	GLOBAL Intelligence Working Group	Northern Virginia Technology Council	Tribal Police Chiefs Mid-Year Meeting
Computers, Freedom, and Privacy Conference	Domestic Highway Enforcement Conference	Interagency Air Domain Awareness Summit	Object Management Group Technical Meeting
Symposium on Identity and Trust on the Internet	Maritime Information Sharing Taskforce	Global Maritime Information Sharing Symposium	TechAmerica Homeland Security Committee
FOSE Institute: Knowledge Management Conference	High Intensity Drug Trafficking Area Directors Meeting	South by Southwest Interactive Conference	Major Cities Chiefs Association Conference
FBI Criminal Justice Information Services Advisory Policy Board	Annual Symantec Government Symposium	Digital Policy Management Technical Exchange Meeting	Air Domain Awareness Summit Executive Session
FBI Global Justice Advisory Committee	International Open Government Data Conference	Architecture for Leaders Course at National Defense University	Regional Information Sharing Systems Policy Board Summit
IJIS Institute Summer and Winter Industry Briefings	Face Recognition Workshop: From Bones to Bits	TechAmerica's IdentEvent: Cyber Security and Identity	Federal Cybersecurity Conference and Workshop
Department of Defense Enterprise Architecture Conference	Regional Information Sharing Systems National Policy Meeting	Executive Board of International Association of Chiefs of Police	Committee on National Security Systems Annual Conference
International Association of Chiefs of Police Annual Conference	National Maritime Intelligence Center Conference on Collections	Homeland Security Information Network Advisory Council Meeting	Major Cities Chiefs Association Intelligence Commanders Meeting
Department of Defense Identity Protection and Management Conference	Forum on Leveraging Technology to Revolutionize Content-Centric Security	Government Technology Research Alliance Defense Gov Council Meeting	Legal Roadblocks to National Strategy for Trusted Identities in Cyberspace
Office of the Director of National Intelligence Identity Intelligence Conference	International Association of Chiefs of Police – Law Enforcement Information Management Conference	Armed Forces Communications and Electronics Association Homeland Security Conference	National Native American Law Enforcement Association Annual Conference
Association for Enterprise Information – Interagency Series on Responsible Information Sharing	Center for Strategic and International Studies National Strategy for Information Sharing Event	Oxford Internet Institute – Information Sharing for Counter-Terrorism and National Defence	NextGen Interagency Architecture Engineering Board – Joint Planning and Development Organization

Table 2 –Events with PM-ISE Participation

Specific upgrades include:

- **Mission Partner Pages** featuring our information sharing mission partners, latest news and social media updates
- **Multimedia Gallery** with informative podcasts, videos, and news
- **Collaboration Tools** that allow the community to provide feedback and discuss initiatives and policies
- **Calendar** to keep track of upcoming events and trainings
- **Document Library** offering important documents easily in our comprehensive repository
- **ISE Partners Resource Directory** to help locate key information sharing partners' websites
- **Improved timeliness** for news, featured stories, blog posts, and job opportunities

Figure 7. *www.ISE.gov*

2.3.1 Refreshing of the Vision for Information Sharing

In 2010, the EOP asked the PM-ISE to refresh the 2007 *National Strategy for Information Sharing* in order to outline an updated vision and strategy for responsible information sharing and protection. Leveraging the 2007 Strategy, the refreshed strategy will bring forward the foundational pieces of the 2007 document and will provide a target vision for the ISE which embraces a trusted, data-centric information sharing and protection vision. The new strategy will also anchor on the National Security Strategy's call for a 'Whole of Government' approach and focus on the mandates within the IRTPA to empower investigators, analysts, and operators with actionable and timely information and intelligence.

Input from ISE mission partners is critical to ensure this refreshed strategy supports the CT mission and provides complete solutions for ISE mission partners. To accomplish this, the PM-ISE is inviting mission partners and agencies to provide their vision for the ISE, as well as their valuable input on various topics

for incorporation into the new Strategy. For example, upon the request of the PM-ISE, the DOJ Global Justice Information Sharing Initiative (GLOBAL) Criminal Intelligence Coordinating Council (CICC) convened a task team to coordinate state, local, and tribal intelligence-related input and recommendations regarding the Strategy refresh. The PM-ISE efforts to develop a strategy for responsible information sharing and protection will continue over the next several months. The PM-ISE has engaged or anticipates engaging with the mission partners and agencies listed in Table 3.

Outreach To	Agency/ Partner
Information Assurance / Data Aggregation	CIA
DEA Chief of OPS & Intel	DEA
Special Operations Division	DEA
High Intensity Drug Trafficking Areas	ONDCP
Information Sharing Governance Board/Information Sharing Coordinating	DHS
DHS Intelligence and Analysis	DHS
DHS I&A State and Local Program Office	DHS
DHS Chief Information Officer Council	DHS
Directorate for National Protection and Programs (NPPD)	DHS
Office of Infrastructure Protection, NPPD	DHS
Office of Cybersecurity and Communications, NPPD	DHS
Critical Infrastructure and Key Resources (CIKR)	DHS
Private Sector Office	DHS
US VISIT, NPPD	DHS
DHS Technology Topics (DHS CIO)	DHS
U.S. Coast Guard	DHS
Customs and Border Protection	DHS
Immigration and Customs Enforcement	DHS
United States Secret Service	DHS
Transportation Security Administration	DHS
Federal Emergency Management Administration	DHS
U.S. Citizenship and Immigration Services	DHS
OSD CIV Policy	DoD
DoD CIO	DoD
Directorate of Information Sharing and Partner Engagement (ISPE), OUSD(I)	DoD
Office of the Under Secretary of Defense for Intelligence USD(I)	DoD
National Drug Intelligence Center	DOJ
Criminal Intelligence Coordinating Council (CICC)	DOJ/CICC
Global Justice Information Sharing Initiative	DOJ/GLOBAL
FBI National Security Branch	FBI
FBI Fusion Center Integration Unit	FBI
FBI Criminal Justice Information Services	FBI

FBI Directorate of Intelligence	FBI
FBI Intelligence Operations Branch	FBI
FBI Intelligence Integration Branch	FBI
FBI Counterterrorism Division	FBI
FBI Fusion Center Integration Unit	FBI
FBI National Threat Center Section	FBI
FBI Guardian Management Unit	FBI
FBI Information Technology Branch	FBI
FBI Office of the Chief Knowledge Officer	FBI
FBI Chief Information Sharing Officer	FBI
Privacy/Civil Liberties Executive Committee	Interagency
ISA IPC and Sub-Committees/Working Groups	Interagency
Identity Credential and Access Management (ICAM) Sub-Committee	Interagency
Tribal Working Group/DOJ Office of Tribal Justice	Interagency
NCTC Organization (general outreach)	NCTC
– Watchlisting Business Process	NCTC
– Information Integration Center/Gentle Breezes Tiger Team (GBTT)	NCTC
– Office of National Intelligence Management, Information Sharing Program and	NCTC
– Chief Scientist	NCTC
Information Assurance	NSA
R6	NSA
White House Coordination	NSS
– Transborder IPC	NSS
– Cyber Directorate	NSS
– Resiliency Directorate	NSS
– Counterterrorism	NSS
– WMD	NSS
– Office of National Drug Control Policy (ONDCP)	NSS
IARPA	ODNI
National Maritime Intelligence Center (NMIC)	ODNI
Private Sector Partnership Group (Industry)	ODNI
Partnership Engagement Office	ODNI
IC Information Sharing Executive	ODNI
Information Sharing Executive Group	ODNI
National Counter Intelligence Executive (NCIX)	ODNI
Consular Affairs	State
Office of Management Policy, Rightsizing, and Innovation	State
IJIS Biannual Meeting	IJIS
Office of Intelligence, Security, and Emergency Response	DOT

Table 3. Stakeholders Engaged in the Development of a Refreshed National Strategy for Information Sharing

2.4 ISE Culture Initiatives

Achieving a culture where responsible information sharing is the norm rather than the exception is a major goal of IRTPA that was further expressed in the 2005 *Presidential Guidelines and Requirements in Support of the ISE*.[27] The 2007 *National Strategy for Information Sharing* called for changing "government culture to one in which information is regularly and responsibly shared and only withheld by exception."[28] However, changing the culture of an organization, particularly a large organization, is a formidable challenge. The breadth and complexity of the ISE compounds the task since the environment extends across all levels of government in the United States, into parts of the private sector, and includes foreign government partners as well.

Leaders who endorse and advocate for responsible information sharing are essential to meeting mission objectives in the post- 9/11 era. Information sharing has traditionally been an organizational prerogative, with a bias for protecting information, due to the perceived risks associated with information sharing. However, the events of 9/11 clearly demonstrated that the aversion to information sharing among governmental agencies in fact created risks to national security that far outweighed the benefits of protecting information.

In order to achieve a change in the culture, leaders at all levels of federal, state, local, and tribal government must set expectations and clearly demonstrate their commitment to responsible information sharing policies and goals. Positive use of appraisal system tools, commitment to quality training, and judicious, credible use of incentives by leaders at all levels of government can contribute to the imperative for cultural change.

The FBI reports that 16,082 employees (13,515 Special Agents and 2,567 Intelligence Analysts) have formally adopted ISE requirements for information sharing into their performance work plans.

(2011 ISE Annual Performance Assessment)

The PM-ISE identified concrete steps and business practices that could facilitate change in three broad areas: making information sharing an evaluation factor in performance appraisal systems; incorporating information sharing and collaboration modules into agency training programs; and encouraging agencies to recognize information sharing as part of their awards programs. These three key areas—appraisals, training, and incentives—are essential elements for changing behaviors of employees and promoting accountability.

Creating a culture of sharing involves changing the way people value information sharing and collaboration by encouraging behaviors that foster sharing and discouraging those that do not. Rewarding behaviors that foster information sharing and adoption of collaborative cross-agency work

27 Memorandum for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment President's Guidelines, December 16, 2005

28 NSIS, p.11.

teams will improve performance throughout the government and enhance efforts conducted with non-governmental partners. People who are held accountable, properly trained, and rewarded for sharing and collaborating not only provide short-term improvements but, by serving as role models for others, effect lasting long-term culture change.

While tangible progress has been made in all three areas, we recognize that culture change encompasses a much broader range of activities and involvement of all mission partners. For example, work underway to support building communities of trust has been instrumental in changing the way that law enforcement agencies work with local communities—an important culture shift. In addition, other activities related to the Administration's Open Government Initiative are also relevant to culture change. PM-ISE also continues to utilize performance management and investment tools such as programmatic guidance to motivate, facilitate and reward information sharing behaviors and practices. Essentially, all of the work done within the ISE facilitates the development of a culture of information sharing, as we develop the capabilities, policies, and mutual trust necessary to ensure that sharing information is the way we do business.

2.4.1 Appraisal/Information Sharing Behavior

Federal agencies continue to expand their programs to include information sharing and collaboration as part of the recruitment, orientation and performance evaluation of all employees; to increase and improve mission specific training programs; to encourage the use of incentive awards for collaborative efforts; to encourage joint duty-like assignments to foster knowledge sharing; and to create COIs around particular topics. In October 2009, the Director, Office of Personnel Management (OPM) issued a memorandum to federal Chief Human Capital Officers in which he stated "information sharing and collaboration should be a common, core behavior across all departments and agencies." Information sharing is also a component of the Performance Management System Requirements under Intelligence Community Directive (ICD) 651, requiring IC agencies to take steps to include sharing and collaboration in their professional standards and evaluation processes.

Each respondent to the 2011 ISE Annual Performance Assessment reported that their ISE-related employees have information sharing and collaboration as components of their performance appraisals, showing a 14 percent growth from 2010. Moreover, 10 out of 14 of these same responding agencies reported that these information sharing and collaboration components were even included in the performance appraisals of employees without ISE responsibilities. This marks an improvement of 30 percent over the past year and consistent commitment to promoting this value within the ISE. The FBI's Senior Executives as part of their performance evaluations, are rated on "Collaboration and Integration" indicative of the Bureau's interest in rewarding information sharing efforts. The DoD provides authority to individual components and managers to include information sharing in performance appraisals and organizations such as the Joint Intelligence Task Force for Combating Terrorism Defense Intel Unit have incorporated these criteria into performance evaluations. The Assistant Secretary of Defense for Homeland Defense and America's Security Affairs also evaluates employees on information sharing and collaboration. Further, the CIA, DHS, DNI, DoD, DOI, DOJ, and NCTC reported that they have specific policies to ensure that information sharing and collaboration are included in personnel appraisals.

2.4.2 Information Sharing Training

Training staff to both appreciate the importance of information sharing at all levels of operation and to effectively share information through existing and emerging mechanisms is essential to ensuring progress. In 2009, PM-ISE issued an ISE Core Awareness Training as an introduction to the ISE and its components; this module continues to be publically available online and generates a foundational understanding of the ISE. This year, DHS continued to work towards ensuring all required staff completes the ISE Core Awareness Training. In addition to ISE Core Awareness Training, the FBI provides numerous courses to contractors and personnel, including U.S. Persons and Information Sharing and how to use various FBI information sharing systems such as LEO, N-DEx, and eGuardian. Various seminar opportunities are also provided such as the Knowledge Week Seminar on IC Information Sharing and the Information Sharing Technology Speaker Series, which often addresses information sharing.

Information sharing training promotes not only the importance of information sharing, but also the importance of teambuilding, collaboration, best practices, and the specific skill development needed to execute sharing activities. Ten out 14 (71 percent) of respondents to the 2011 ISE Annual Performance Assessment reported that they have implemented mission-specific training that supports information sharing and collaboration; compared to 2010, this equates to a positive growth rate of seven percent. Training efforts in the ISE have been ongoing since the passage of the IRTPA, beginning with basic foundational training, and now advancing to more focused, mission-specific efforts. PM-ISE is dedicated to linking mission partners with similar interests and training priorities in order to identify potential joint projects resulting in better products and cost efficiencies. Almost all partners with a CT mission report having implemented training that supports information sharing. In fact, all departments under the purview of the DNI reported implementing mission specific training to support information sharing and collaboration in this year's ISE Annual Performance Assessment. The DoD provides several related training opportunities through its Joint Knowledge On-Line portal, enhancing availability and ease of education. DHS not only has information sharing training for its own employees; it has also initiated a project with the Federal Law Enforcement Training Center to develop an information sharing training tailored to the law enforcement community. Meanwhile, the DOI has implemented information training for both sworn and non-law enforcement personnel. All of these efforts reflect a collective commitment to enabling information sharing through personnel training.

The NSI Program Management Office (NSI PMO) has developed and conducted extensive training including executive briefings, analytic training, and line officer training. According to the NSI First Quarter 2011 Activity Summary, the NSI is making great strides in providing SAR training to law enforcement and support personnel to help ensure that they are trained to recognize behavior and

incidents identified by law enforcement officials and CT experts from across the country as being reasonably indicative of criminal activity associated with terrorism. The NSI has been working with the IACP, the Major Cities Chiefs Association, the Major County Sheriffs' Association, the National Sheriffs' Association, the Association of State Criminal Investigative Agencies, and others to help deliver this training as quickly and efficiently as possible to all law enforcement officers.

- The Washington State Patrol (WSP) posted the SAR Line Officer Training video on the WSP Web site, and as of 31 March 2011, more than 1,400 WSP employees have viewed the training.
- The Virginia Fusion Center pushed the training out to the Virginia State Patrol staff, officers, and personnel, and has successfully trained every state trooper.
- The Georgia Bureau of Investigation has worked to get POST credit for officers who take the required SAR line officer and CICC privacy trainings, and will mandate that training be completed by 15 July 2011.
- The Southern Nevada Counter-Terrorism Center (SNCTC) posted the line officer training to the SNCTC Web site, which has allowed access to all law enforcement officers in the state of Nevada.
- The Florida Fusion Center is one of the first fusion centers to develop a customized line officer training program through LEAPS.TV, which also offers individual jurisdictions the opportunity to customize the program by adding information on specific procedures and practices within their agencies to the basic NSI PMO program.
- The Los Angeles County Sheriff's Office and the Memorial Institute for the Prevention of Terrorism have partnered to provide training to all deputies.

In response to the 2010 Baseline Capability Assessment (BCA), the DHS Office of Intelligence and Analysis (I&A) and the Homeland Infrastructure Threat and Risk Analysis Center sponsored three deliveries of the Introduction to Risk Analysis Course. The five-day course was offered in September 2010, December 2010, and February 2011 and was intended to support fusion centers in building the capability to regularly assess the local implications of time-sensitive and emerging threat information, contributing to risk analysis. Participant feedback, collected voluntarily after the conclusion of each course, suggests that the course provided fusion centers with the resources they need to enhance their ability to assess the local implications of threat information through the use of a formal risk assessment process.

The Watchlisting community, led by the NCTC and FBI's Terrorist Screening Center (TSC), in coordination with nominating and screening agencies, is developing a standardized training course to educate the community on the updated Watchlisting Guidance. The course is designed to help standardize watchlisting and screening processes and decisions and to improve the quality of information regarding known and suspected terrorists. To date, NCTC has facilitated pilot training sessions and is planning additional pilots in late spring/early summer. The classroom-based training is scheduled to be fully implemented by July 2011. An additional, web-based training module is scheduled to for development after implementation of the classroom-based training.

Another indicator of success regarding the production and availability of appropriate training and educational materials to support information sharing, is that all mission partners responding to the ISE 2010 ISE Annual Performance Assessment responded that the currently available ISE training is sufficient to support their mission. In addition, all federal agencies reported that their personnel receive training with a specialized privacy and civil liberties protection component at least annually.

2.4.3 Incentives

Positive reinforcement also plays an important role in encouraging an information sharing culture. Routinely recognizing and rewarding effective information sharing, as well as expertise and competency development, will serve to increase its frequency and the desire of personnel to improve efforts. To this end, 86 percent of ISE departments and agencies reported offering an award that includes information sharing and collaboration directly or indirectly as criteria. Moreover, the number of responding ISE departments and agencies that have identified an increase in information sharing and collaboration award nominations has doubled over the past year. But only three agencies—the DOJ, the Department of Transportation (DOT), and the FBI—report offering agency-specific incentives to encourage information sharing, indicating a clear area for improvement. FBI created the Chief Information Sharing Officer Award to enhance awareness of information sharing goals and the central role they play in the FBI's National Security and Criminal missions. DOT offers cash awards to employees to acknowledge their involvement in information sharing efforts. And DHS reports that they continue to work towards implementing an award program to recognize information sharing.

2.4.4 Exercises

As information sharing becomes institutionalized, we expect to see elements of the ISE reflected in organizational exercises. For example, the FBI recently created a "National Level Exercise (NLE) Coordinator" position to ensure that the FBI's intelligence component is being fully integrated with the NLE process.

In 2011, PM-ISE began looking at exercises being conducted at the national and interagency levels to understand how operational reality impinges on theory. While neither conducting nor directly participating in the exercises, PM-ISE will endeavor to collect lessons learned, to identify exercise-driven requirements for the ISE, and as necessary, to provide general guidance on incorporating ISE elements into operational exercises.

Federal Geospatial Concept of Operations

Now in its third year of development, the Federal Geospatial Concept of Operations (Federal GeoCONOPS) effort, led by the DHS, has reached a state of maturity for inclusion in National Level Exercises and transition to routine operational use. The goal of the Federal GeoCONOPs is to assure that sharing geospatial information for situation awareness is conducted effectively and in alignment with the Incident Command System, Homeland Security Presidential Directive (HSPD) 5 "Management of Domestic Incidents," and National Response Framework policy and doctrine. In accordance with incident response doctrine, the Federal GeoCONOPS is being developed as an all-threats, all-hazards, all phases of the emergency management lifecycle resource. The Federal GeoCONOPS provides comprehensive guidance on authoritative sources of information, defines the roles of Emergency Support Functions for the development and sharing of geospatial information, and addresses mission-specific areas such as life saving and damage assessment.

2.4.5 Best Practices

In order to facilitate the quick integration of new ideas, and more importantly, those that are proven to generate results, the ISE must readily identify, communicate, and implement best practices. Identifying and packaging them in a way that allows replication and innovation based on proven concepts is critical. To this end, PM-ISE is developing "Building Blocks of the ISE," a toolkit that includes the many components of the ISE which work together to facilitate information sharing and protection. This web-based resource will allow ISE mission partners at any level (state, local, tribal, or international) to better understand what makes the ISE function with guidance on how replication is possible in different environments.

Building the Foundation

Six years after passage of IRTPA, some of the most significant barriers to federal, state, local, tribal, and private sector collaboration have been overcome and others are being aggressively addressed by the PM-ISE and mission partners.

- Comprehensive ISE Privacy Guidelines and implementation guidance are in place;
- A comprehensive program for designating, handling, and marking Controlled Unclassified Information (CUI) has been developed and will standardize more than 100 unique markings currently used for Sensitive But Unclassified (SBU) information;
- A solid blueprint for a standards-based ISE, founded on the National Information Exchange Model (NIEM)—ISE Enterprise Architecture Framework—is in place and helps guide federal agency architectures and IT investment planning;
- Common information sharing standards, such as the ISE Functional Standard for Suspicious Activity Reporting (SAR) Version 1.5, documents the rules, conditions, guidelines, and characteristics of business processes, production methods, and products that support information sharing; and
- An Executive Order designed to safeguard and govern access to classified national security information shared by the Federal Government with state, local, tribal, and private-sector entities, has been released.

In addition, much work has been done to improve sharing with state, local, tribal, and territorial (SLTT) governments. The establishment of a national, integrated network of state and major urban area fusion centers permits SLTT governments to: (1) receive classified and unclassified information from federal partners; (2) assess local implications of threat information through the use of a formal risk assessment process; (3) further disseminate threat information to SLTT authorities, and private-sector entities within their jurisdiction; and (4) gather, aggregate, analyze, and share locally-generated information with federal partners as appropriate.

Another significant example is creating the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The NSI builds on what law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents associated with criminal activity—and establishes a standardized process whereby that information can be shared among agencies to help detect and prevent terrorism-related criminal activity. The NSI provides an interrelated set of common policies and mission processes which leverage ISE core capabilities and enable fusion centers, as well as the men and women on our nation's counterterrorism front line, to access and share the information they need to keep the country safe.

There has also been significant information sharing improvements by other mission partners. Perhaps the most significant and visible change in terrorism-related information sharing was the establishment of the National Counterterrorism Center (NCTC). Further, the Director of National Intelligence, in partnership with the Intelligence Community (IC) advanced integration of information sharing processes by issuing ground breaking Intelligence Community Directive (ICD) 501—*Discovery and Dissemination or*

Retrieval of Information. This directive promotes responsible information sharing by distinguishing between discovery (obtaining knowledge that information exists) and dissemination or retrieval (obtaining the contents of the information). And finally, the Interagency Threat Assessment and Coordination Group was established to bridge the intelligence information gap between traditional intelligence agencies and state, local, tribal, territorial, and private-sector partners.

3 Improving Information Sharing Activities

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) makes it clear the PM-ISE's responsibilities extend to addressing and facilitating improved information sharing between and among the components of the Intelligence Community (IC), the Department of Defense (DoD), as well as the homeland security and law enforcement communities. In addition, the PM-ISE is required to address and facilitate responsible information sharing between federal departments and agencies and state, local and tribal governments; federal departments and agencies and the private sector; and federal departments and agencies and foreign partners and allies. In ensuring responsible information sharing between all of these mission partners, the PM-ISE must also ensure the protection of privacy, civil rights, and civil liberties (P/CR/CL).[29]

> We are improving information sharing and cooperation by linking networks to facilitate Federal, state, and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate. We are coordinating better with foreign partners to identify, track, limit access to funding, and prevent terrorist travel. Recognizing the inextricable link between domestic and transnational security, we will collaborate bilaterally, regionally, and through international institutions to promote global efforts to prevent terrorist attacks.
> – *National Security Strategy, May 2010*

Since Congress called for the creation of the ISE, significant progress has been made to build a broad foundation for information sharing across the Federal Government, as well as with our state, local, and tribal partners and the private sector and international community. This chapter speaks to a wide range of mission partner activities improving information sharing between and among these vital ISE mission partners, encompassing the full range of mission activities.

Although the focus of this Report remains on terrorism-related initiatives, this chapter also describes mission partner activities, some of which may not have been developed explicitly to support counterterrorism (CT), but indirectly support the CT mission, or may ultimately serve as "best practices" with applicability to information sharing and collaboration government-wide, including the ISE.[30]

29 IRTPA Sec. 1016 (f)(2).

30 The fact that the ISE can leverage these achievements is consistent with one of its key attributes identified in IRTPA—to build upon existing systems capabilities currently in use across the government.

3.1 Suspicious Activity Reporting

The findings in the 9/11 Commission Report[31] and the Markle Foundation[32] clearly demonstrated the need for a nationwide capacity to share information that could detect, prevent or deter a terrorist attack. IRPTA, followed by the 2007 *National Strategy for Information Sharing*, indicates both legislative and executive intent to establish locally controlled, distributed information systems wherein potential terrorism-related information could be contributed by the 18,000 state, local and tribal law enforcement agencies for analysis, to determine if there are any significant emerging patterns or trends. Following this guidance, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) was born.

The NSI is a partnership that establishes a capacity for sharing terrorism-related Suspicious Activity Reports, also known as ISE-SAR. "An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism)."[33] The NSI provides analysts, operators and investigators with another tool for "connecting the dots" in combating crime and terrorism, by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR—referred to as the SAR process—in a manner that rigorously protects the privacy and civil liberties of Americans.

The SAR process is critical to preventing crimes, including those associated with domestic and international terrorism. In developing the standards and processes, the NSI leveraged the guidance and expertise provided by GLOBAL which serves as a federal advisory committee and advises the U.S. Attorney General on justice information sharing and integration initiatives. This includes leveraging the National Information Exchange Model (NIEM), which is the backbone of the technology component of the NSI process, as well as privacy guidelines and checklists, to develop a comprehensive program.

NSI in Action

In January 2010, a Los Angeles Police Department (LAPD) line officer who was trained in SAR discovered a store owner who was selling illegal cigarettes, brass knuckles, counterfeit name-brand purses and wallets, and drug paraphernalia. While conducting a search at the store, LAPD officers observed a bomb-making recipe taped to the wall. Subsequently, the store owner was arrested, the recipe was determined to be a viable bomb-making formula, and an investigation into possible terrorism financing is ongoing.

31 9-11 Commission Report, July 2004

32 Nation At Risk: Policy Makers Need Better Information to Protect the Country, 1 March 2009

33 ISE-SAR Functional Standard v. 1.5, http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf.

3.1.1 Implementation of the NSI – Building on Success

Every day, law enforcement officers observe suspicious activity or receive reports from concerned civilians, private security, and other government agencies about behaviors that could have a potential nexus to terrorism. Until recently, this information was generally stored at the local level and shared within the agency—or, at most, regionally shared–as part of an incident reporting system. Since the standup of the NSI PMO—led by the DOJ, Bureau of Justice Assistance (BJA), and implemented in partnership with the FBI and DHS–the NSI has made substantial progress with standardizing these ad hoc methods of reporting and analysis, and implementing these standards, policies, and processes within the National Network of fusion centers so that timely, relevant information can be shared across federal, state, local, and tribal law enforcement agencies, while also working to ensure that the privacy civil rights, and civil liberties of citizens are protected.

NSI Privacy Framework

The protection of P/CR/CL is paramount to the success of the NSI. Given this importance, the NSI has worked with key partners—including the American Civil Liberties Union and other advocacy groups—to develop protections that, when consolidated, make up the NSI Privacy Framework, which is derived from the protection requirements of the ISE Privacy Guidelines and has elements specific to NSI operations. The NSI requires each site to consider privacy throughout the SAR process by fully adopting the elements within the NSI Privacy Framework prior to NSI participation: development and adoption of a written privacy policy which addresses specific SAR protection requirements; designation of an official for privacy and civil liberties; adhering to the business processes of the ISE-SAR Functional Standard Version 1.5; and providing personnel with information on P/CR/CL protections through the NSI role-based training modules.

> "In my twenty-five years of law enforcement experience this was without a doubt the best training session I have ever attended. I left Oklahoma City excited to bring this information back to my agency and get this training to the front line officers. I look forward to participating in the next phases of the InCop training program. I truly believe in this training and believe it is in the best interests of our nation's safety to have every front line officer in every law enforcement agency trained in the InCop techniques."
>
> *– Sergeant, Jersey City Police Department, April 2011*

In addition, NSI participant sites are strongly encouraged to engage in outreach with privacy, civil liberties, and community-based advocacy groups to foster transparency and trust as well as to obtain feedback and perspective on information sharing initiatives.

NSI Training

The 850,000 uniformed officers in the United States are the foundation for the NSI. To ensure that these officers are properly trained, the NSI PMO takes a multifaceted approach designed to increase the effectiveness of state, local, and tribal law enforcement professionals in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism. The overarching goals of the training strategy are to facilitate agency implementation of the SAR process and to enhance a nationwide SAR capability. The NSI

has developed training for front line officers, analysts, and chief executives regarding the behaviors and indicators of terrorism related criminal activity. These training efforts focus on behaviors that have been previously established as potential precursors to criminal acts leading to terrorist activity – the "what," not the "who." Training is offered through direct and indirect programs, such as the Memorial Institute for the Prevention of Terrorism's Information Collection on Patrol (InCop) and Train-the-Trainer (TtT) programs, and online through training videos. Participant feedback on these programs has been very positive. To date, nearly 50,000 officers have received direct, indirect, or on-line training.

NSI training will be enhanced this year to include language about placing a behavior into the NSI Federated Space and eGuardian if, based on their own training, experience, or location (target or critical infrastructure), a participant feels that an observation has a reasonable nexus to a potential terrorism event. In the end, the "totality of the environment" is the defining guidance. Also, leveraging resources and advancing integration, all FBI Joint Terrorism Task Forces (JTTF) personnel will receive full recognition of their own training.

To provide support to front line officers in particular, the NSI PMO, in partnership with the IACP, Major Cities Chiefs Association (MCCA), Major County Sheriffs' Association (MCSA), National Sheriffs' Association (NSA), the Association of State Criminal Investigative Agencies (ASCIA), and the National Network of fusion centers, is working to deliver a training video for law enforcement and support personnel, training them to recognize those behaviors and incidents that are potentially indicative of criminal activity associated with terrorism. The goal is to have all officers trained by the fall 2011.

Implementation of NSI on America's Rails

The SAR process has been fully implemented throughout the entire East Coast Amtrak network, which including SAR training for all Amtrak police and rail staff. Commuter rail systems that have implemented most elements of the NSI include: the Maryland Transportation Authority, Southeastern Pennsylvania Transportation Authority, New Jersey Transit, New York/New Jersey Port Authority, Massachusetts Bay Transportation Authority, and the New York Metropolitan Transportation Authority. Elements introduced or in place include staff and police training in behavioral recognition, messaging, SAR reporting, SAR analysis, entry of data into the Shared Space or eGuardian, and implementation of privacy policies that are in compliance with the ISE Privacy Guidelines. The next steps are to complete the East Coast implementation; move on to the national freight rail systems and Midwest Amtrak and Chicago; and begin implementation on the West Coast.

Stakeholder Outreach

The success of the NSI largely depends on the ability of law enforcement to earn and maintain the public's trust. Therefore, NSI sites are encouraged to engage in outreach to members of the public, including privacy and civil liberties advocacy groups and private-sector partners, to explain how these new tools will be used, while ensuring the protection of citizens' P/CR/CL. This has resulted in the creation of the Building Communities of Trust (BCOT) initiative, discussed later in this chapter.

Over the past year the NSI PMO has also been coordinating closely with DHS on the "If You See Something, Say Something™" campaign. This campaign—originally implemented by New York City's Metropolitan Transportation Authority—is a simple and effective program to raise public awareness of the indicators of terrorism, crime, and other threats, and to emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities. Campaigns have been launched over the past several months with the National Football League, the National Collegiate Athletic Association, the Indianapolis 500, the National Basketball Association, the Mall of America, and the Pentagon Force Protection Agency.

DHS is also working to align the efforts of the "If You See Something, Say Something™" campaign with a similar program within the Coast Guard, "America's Waterway Watch" (AWW). AWW engages public and private stakeholders to be aware of suspicious activity along U.S. ports and waterways and report suspicious activity via a 24x7 hotline, 877-24WATCH. The "If You See Something, Say Something™" campaign and AWW recently developed a joint outreach program for the Washington State Ferry System and are planning on rolling out this joint awareness campaign to include all major ferry systems.

The NSI also recognizes the importance of incorporating the private sector—which owns and operates more than 80 percent of the Critical Infrastructure and Key Resources (CIKR) in our country—and has therefore been working with the DHS Office of Infrastructure Protection (IP) to incorporate the 18 identified sectors into the future NSI process.

Interagency Coordination Bolsters the NSI

DHS IP is providing additional avenues of communication between critical infrastructure owners and operators and the SAR process through the Critical Infrastructure and Key Resources Information Sharing Environment (CIKR ISE), the primary private-sector component of the ISE. In support of Secretary Napolitano's "If You See Something, Say Something™" campaign, IP created a standardized format for stakeholders to submit reports. The SAR for Critical Infrastructure tool, currently in the pilot phase for two sectors, will allow stakeholders to share SAR reporting within their sector and with the National Infrastructure Coordinating Center (NICC) through portals on the Homeland Security Information Network-Critical Sectors (HSIN-CS). The NSI PMO's strategic engagement plan for critical infrastructure highlights and supports expanded availability of the tool for additional sectors upon the completion of this pilot.

Since the inception of the "If You See Something, Say Something™" campaign in July 2010, the NICC Watch has observed a significant increase in SAR reporting. Once a SAR is received from sector partners, the NICC analyzes the information and, if the SAR has a potential

nexus to terrorism, generates a report called a "Patriot Report." A redacted version of the Patriot Report is shared with cross-sector critical infrastructure stakeholders through HSIN-CS and with the National Operations Center (NOC) Fusion Desk. The NICC Watch also disseminates the full Patriot Report within the Federal Government to include the DHS Office of Intelligence and Analysis (DHS I&A), the NOC-Intelligence Watch and Warning, the FBI, and the NSI.

Enabling Technology

To support the operational mission, the NSI Federated Search facilitates information sharing using NIEM. NIEM enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations, with data formatted in a semantically consistent manner. NIEM is being used to standardize content (actual data exchange standards), provide tools, and managed processes. By utilizing NIEM, the NSI has made it possible for agencies to search and share terrorism-related SAR across a federated environment.

There are several ways in which NSI participants can make their SAR information available to the NSI Federated Search: by installing an NSI Shared Space Server; by using an existing legacy Computer Aided Dispatch/Record Management System that is in line with NIEM standards; or by creating an eGuardian account. NSI participants can access NSI Federated Search through either RISSNet or LEO, and participants will be able to access the search through Homeland Security Information Network-Law Enforcement (HSIN-LE) sometime in the future.

Standardized Processes

The standardized processes and policies established by the NSI PMO provide federal, state, local, and tribal law enforcement with the capability to share timely, relevant SAR information that has been determined to have a potential nexus to terrorism while ensuring that P/CR/CL are protected. The National Network is a critical part of this connectivity. The NSI PMO has closely coordinated with the State and Local Program Office within DHS I&A, which has the lead for providing support to fusion centers and has also been tasked with providing NSI training and implementing NSI processes within all relevant DHS components. This continued relationship will be critical as the NSI completes the initial implementation and capability of accessing these tools within state and major urban area fusion centers, and moves toward sustainment and utilization of these capabilities.

Focus over the next year will turn to continued implementation within the Federal Government, including all DHS and DOJ law enforcement components, as well as key partners within the private sector and non-traditional homeland security sectors.[34]

34 DoD is already using eGuardian as discussed later in this chapter

Information from Public Yields Arrest

On 28 October 2010, the FBI Public Access Center Unit received information submitted from an individual, via the Internet, reporting what he or she believed to be threats to the Washington D.C. Metro system. According to the source, the subject indicated, through his Facebook account, his intentions of placing pipe bombs on Metro trains in Washington, DC. The subject also discussed planting bombs in sewers in Georgetown neighborhoods. This information was entered into the FBI Guardian system where a terrorism assessment was initiated. At the same time, the information was pushed down from Guardian to the eGuardian system, ensuring that more than 1,000 eGuardian agency partners were also informed of the threat information.

Upon conclusion of the assessment, on 2 December 2010, the FBI Washington Field Office opened a case to investigate the threats. The investigative efforts resulted in the 14 December 2010 arrest of Awais Younis, a.k.a. Mohhanme Khan, a.k.a. Sundullah Ghilzai for communicating threats via interstate communications. On 14 December 2010, Younis was ordered to undergo a mental evaluation. He was subsequently indicted by a federal grand jury.

On 11 April 2011, Younis pled guilty to conspiring to provide material support to al-Qaida and collecting information for a terrorist attack on a transit facility. Younis' guilty plea was part of a negotiated plea agreement with federal prosecutors, and he apologized in court for his conduct. Younis is a naturalized U.S. citizen from Pakistan, who resided in Northern Virginia. He had conducted video surveillance of DC's Metro rail system and had suggested ways of bombing the Northern Virginia subway stations to inflict the highest number of casualties.

3.1.2 Suspicious Activity Reporting (SAR) Sub-Committee

The SAR Sub-Committee of the ISA IPC focuses on a standardized process in which SAR information can be shared among agencies to help detect and prevent terrorism-related criminal activity. The Sub-Committee is chaired by the DOJ, BJA with additional membership from the FBI, DHS, NSI PMO, PM-ISE, and ODNI.

In the last year, the SAR Subcommittee and the FBI's Joint Terrorism Task Forces (JTTF) worked together to incorporate the eGuardian system with the NSI shared spaces.

The SAR Sub-Committee is responsible for leading the development of strategy, guidance, and policy documents for gathering, analyzing and sharing SAR information; ensuring interagency coordination on related efforts; and resolving interagency issues. In the last year, the SAR Subcommittee and the FBI's JTTFs worked together to incorporate the eGuardian system with the NSI shared spaces. This helps formalize information sharing between state, local, and tribal partners, and leverages the already successful relationships between SLT

partners and the FBI's Joint Terrorism Task Forces. It also streamlines processes and aligns privacy policies among various partners.

In the coming year, the SAR Sub-Committee will focus on several initiatives aimed to further mature the NSI. These efforts include leveraging the Sub-Committee members to identify and improve the use of SAR in intelligence and homeland security threat documents; identifying the scope and requirements for development of an ISE SAR Functional Standard v2.0; creating a roadmap to better align SAR technology solutions; seeking the most efficient training and communications processes; and providing policy recommendations on incorporation of the private sector, including CIKR into the NSI.

3.1.3 Enhancing SAR Analysis

To further strengthen the strategic analysis of SAR data, the DHS SAR Initiative Management Group (DSI MG) is assisting components with engaging the NSI PMO. In addition to sharing their respective SAR with other NSI participants, components are providing an enriched SAR data set that can be leveraged by I&A for the purpose of producing analysis. Some of the products serve as tactical intelligence that assists the decision-making efforts of state, local, tribal and federal law enforcement agencies as they provide protective measures.

SAR Analysis Survey

DHS I&A conducted a survey in April 2011 with the goal of documenting SAR Analysis products that are being produced at the federal as well as the state, local, and tribal (SLT) levels, and recommending areas for future production by the community. The survey has spurred I&A's initiation of a regional analytical working group that will discuss current tradecraft and best practices as they relate to SAR-related intelligence products.

As of May 2011, the FBI, in addition to various offices within DHS, is regularly producing SAR products for use by DHS components, the IC, SLTT law enforcement, and the private-sector. Products range from stand-alone SAR products to routine analytic products that incorporate SAR data.

DOI Establishes Dam Sector Intelligence Working Group to Share and Coordinate SAR

This year, the DOI stood up the Dam Sector Intelligence Working Group to share and coordinate SAR on dams across the United States. The Working Group includes representatives from DHS, the U.S. Army Corps of Engineers, the Tennessee Valley Authority, and DOI. This effort has significantly improved the overall situational awareness regarding the safety and security of dams, some of which are national critical infrastructure. DOI is a member of the National Infrastructure Protection Plan's Sector Partnership as part of the Dams Sector and participates in the information sharing activities of the entire Dams Sector. The Dams Sector, under the CIKR ISE, initiated the first form of a sector-wide SAR process among the critical infrastructure sectors two years ago.

3.1.4 Building Communities of Trust (BCOT)

The BCOT initiative focuses on developing relationships of trust between police departments, fusion centers, and the communities they serve—particularly immigrant and minority communities—to prevent terrorist-related crime and to help keep our communities safe. Under the leadership of the NSI, the BCOT initiative expanded in 2010, with roundtables held in Chicago and Los Angeles. Several more meetings are planned for 2011. The NSI also partnered with the DHS Countering Violent Extremism (CVE) efforts with meetings held in Dearborn, MI and Minneapolis, MN.

In the fall of 2010, the *Guidance for Building Communities of Trust* was released at the International Association of Chiefs of Police (IACP) annual conference in Orlando, Florida. This guidance provides advice and recommendations to law enforcement, fusion center personnel, and the community on how to initiate and sustain trusting relationships that support meaningful sharing of information, responsiveness to community concerns and priorities, and the reporting of suspicious activities that appropriately distinguish between innocent cultural behaviors and behaviors that may legitimately reflect criminal enterprise or terrorism precursor activities.

Maritime SAR initiative

The Maritime SAR initiative, led by the National Maritime Intelligence Center (NMIC), aims to establish a process or to leverage NSI's process for maintaining and disseminating all maritime SAR; to work with the global maritime community of interest to populate the NSI Shared Space with maritime-related information to maximize information sharing; and to establish and designate a Federal Maritime SAR entity with analytical responsibilities. This initiative is also aimed at training maritime-related industry employees on SAR reporting. Further, it is imperative that as a nation we ensure that maritime SAR data is brought together for dialog and trending analysis.

3.1.5 Leveraging the SAR Experience

In addition to its successful use in the reporting of suspicious activities, the SAR process and its innovative use of common terminology to describe incidents, its use of NIEM as a methodology for data exchange, and its focus on training to achieve consistency of reporting are potentially scalable to other information sharing processes. In particular, the SAR process and its functional standard is being considered as a repeatable best practice which can be applied to the sharing of cybersecurity incident reporting information, a key element of the Comprehensive National Cybersecurity Initiative.[35] Accordingly, the NIEM Program Management Office is developing a NIEM Information Exchange Package Documentation (IEPD) for cybersecurity incident reporting, and PM-ISE is promoting the use of the SAR Functional Standard as a model for collaboration across six centers that are responsible for carrying out U.S. cyber activities.

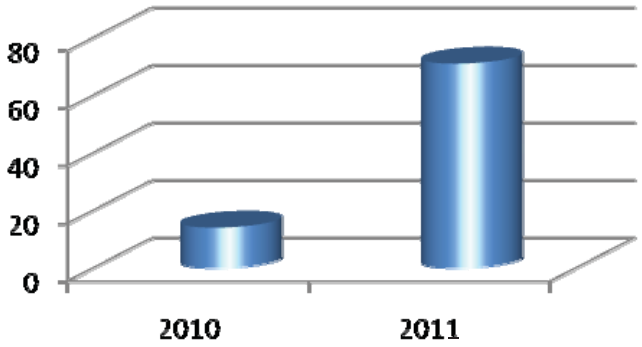
35 http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

3.2 National Network of Fusion Centers

Fusion centers serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and state, local, tribal, and private-sector (SLTPS) partners. Located in state and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, CIKR protection, and private-sector security personnel to understand local implications of national intelligence, enabling local officials to better protect their communities. Fusion centers provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, and connectivity to federal systems, technology, and grant funding. Since June 2010, DHS has provided the following support to fusion centers:

- In partnership with DOJ, assisted 57 fusion centers with privacy policies, bringing the total number to 71 fusion centers with privacy policies, which represents a 407 percent increase since the last Annual Report (see Figure 8)
- Deployed the Homeland Secure Data Network (HSDN) to an additional 15 fusion centers, bringing the total number to 52 fusion centers with HSDN, which represents a 41 percent increase since the last Annual Report
- Deployed 12 DHS Intelligence Officers to fusion centers, bringing the total number to 70 deployed officers, which represents a 21 percent increase since the last Annual Report
- Granted 1,173 security clearances for state, local, and tribal fusion center personnel
- Delivered security liaison training to 68 fusion center security liaisons
- Deployed the CIKR ISE to five pilot fusion centers to support local and regional critical infrastructure protection

Figure 8. Number of Fusion Centers with Privacy Policies



3.2.1 Fusion Centers and the FBI

In 2010, all 56 FBI field offices conducted self-assessments on their relationship with fusion centers, providing a comprehensive understanding of how the FBI is currently engaged with fusion centers. During this process, the FBI program managers also worked closely with PM-ISE and DHS to evaluate and validate fusion center baseline capabilities and to address areas of common concern discovered during this process.

The FBI continues to assess and develop field office-fusion center engagement based on lessons learned and knowledge gleaned from the assessments, as well as improvements in fusion center capabilities.

The FBI plans to continue close collaboration at both the field office and headquarters levels to standardize processes; clarify procedures; and facilitate more effective engagement with fusion centers. The FBI understands the value of collaboration with other law enforcement entities in maintaining homeland security, and remains committed to strengthening ties at all levels of government.

FBI in Fusion Centers

Currently, 103 FBI personnel are assigned to 59 fusion centers, with 48 embedded full-time in 26 fusion centers and 55 working on a part-time basis in 33 fusion centers. Of these, 32 are Special Agents (SAs) and 71 are Intelligence Analysts (IAs). FBINet, the FBI's primary network system for the daily investigative and administrative functions of the FBI, is available to 37 fusion centers. The FBINet presence enables assigned FBI personnel to more fully collaborate with all fusion center personnel since FBI information is at their fingertips. Plans and equipment for FBINet installation in 15 additional fusion centers is scheduled to commence in 2011 and be completed by fiscal year 2012.

3.2.2 Baseline Capabilities Assessment (BCA)

The most notable interagency effort in support of the National Network in 2010 was the BCA. In September 2010, federal, state, and local officials completed the first nationwide, in-depth assessment of fusion centers to evaluate their capabilities and to establish strategic priorities for Federal Government support. The BCA was designed to evaluate the fusion centers' Critical Operational Capabilities (COC) in an effort to understand the overall maturity of the National Network and to aid fusion centers in reaching their full potential as focal points within the state, local, tribal, and territorial environment for the receipt, analysis, gathering, and sharing of threat-related information. The BCA also evaluated the fusion centers' capability to protect P/CR/CL, a key enabling capability for the fusion process. On behalf of the DHS, the 2010 BCA was conducted by the PM-ISE, in coordination with Fusion Center Directors, the DHS, the FBI, and other federal interagency partners.

In September 2010, PM-ISE, in coordination with Fusion Center Directors, DHS, FBI and other federal interagency partners, completed a comprehensive assessment of each of the operational fusion centers' capabilities. While the assessment reflected that some fusion centers were more mature than others, efforts are underway to strengthen the capability of the National Network.

In response to DHS Secretary Napolitano's challenge for state and major urban area fusion centers to reach an enhanced level of capability for all four COCs and P/CR/CL protections by 31 December 2010, DHS, in coordination with Fusion Center Directors and interagency partners, developed the COC Gap Mitigation Strategy. This strategy consisted of both short- and long-term activities for mitigating gaps in fusion center capabilities. The short-term approach outlined immediate actions to help fusion centers execute the COCs during situations involving time-sensitive and emerging

threat information. The long-term COC gap mitigation activities will support fusion center efforts to maintain the COCs and P/CR/CL protections. From September 2010 through December 2010, DHS, in coordination with interagency partners, focused its support to state and major urban area fusion centers on the activities identified in the short-term strategy. These activities provided fusion centers with the skills, tools, and resources to support the development and implementation of their plans, policies, and standard operating procedures, enabling the effective execution of the fusion process in situations involving time-sensitive and emerging threat information.

Beginning in January 2011, DHS launched an effort to evaluate both the results of the short-term COC gap mitigation activities and the effectiveness of their support in building fusion center capabilities in line with each COC. As part of this effort, a survey was developed for Fusion Center Directors to help assess each center's progress toward achieving the short-term gap mitigation objectives. To help gauge the Department's support, the survey asked questions regarding the federal assistance to fusion centers. Fusion Center Directors overwhelmingly responded that DHS provided a clear understanding of the intent and expected timeframe associated with the short-term strategy and offered adequate guidance to meet the short-term gap mitigation objectives. A majority of the Directors also agreed that DHS offered adequate resources to meet those objectives. In addition to the survey, DHS also leveraged a variety of other data sources, including the 2010 BCA, official activity after action reports, and data from other federal departments and agencies. Based on the results of this evaluation, fusion centers made progress from September 2010 to December 2010 in building their capabilities and addressing gaps identified in the BCA in each of the four COCs and P/CR/CL protections. Fusion centers continue to build their capabilities in these critical areas. These findings have been captured in the April 2011 COC Short-Term Gap Mitigation Strategy Progress Report.

Fusion Centers in Action

In October 2010, an advisory was sent out by the New York Police Department concerning a suspicious tractor-trailer whose driver reportedly diverted its route to Times Square in New York City in exchange for $10,000. The deployed DHS Intelligence Officer (IO) in New York informed several fusion centers in the affected area. Subsequently, the Rhode Island Fusion Center discovered that the original owner of the truck was a California native and requested a background check from the Northern California Regional Intelligence Center. Within two hours of the advisory's release, information from these two fusion centers was used to coordinate with the Connecticut Intelligence Center, which assisted the Connecticut State Police in locating the vehicle before it reached its reported target. Ultimately, officials concluded that there was no threat, but the fact that these fusion centers, supported by the DHS IO, were able to resolve this SAR in a matter of three hours demonstrates the value of the National Network.

* * *

The Arizona Counter Terrorism Information Center supported a five-month investigation led by a tribal partner, the Tohono O'odham Nation (TON) Police Department and the Bureau of Indian Affairs (BIA) Division of Drug Enforcement. This investigation led to the arrest of 10 suspects and the apprehension of weapons, cash, vehicles, cocaine, marijuana, and Ecstasy–the largest drug enforcement operation in TON history. The investigation marked a key opportunity to collaborate with tribal partners and opened information sharing initiatives between several other agencies, including the FBI, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and other police departments in the area.

* * *

In the fall of 2010, the FBI's Western Regional Intelligence Group and Sacramento Field Intelligence Group began collaborating with the California State Threat Assessment Center on threats to the Southwest Border. As a result of this federal and state partnership, in April 2011, the Center released their first detailed assessment on widespread criminal effects of Mexico's drug war. This product drew accolades from the Los Angeles Police Department, the DHS, and state executives from Texas and California. Due to this partnership with the FBI, collaboration has increased throughout the state of California.

3.2.3 Fusion Center Sub-Committee

The Fusion Center Sub-Committee of the ISA IPC focuses on coordinating federal support to fusion centers by providing the guidance and standards necessary to support interconnectivity to help ensure information sharing between and among fusion centers and all levels of government. The Sub-Committee is chaired by DHS and the FBI, and includes members from DoD, the Joint Staff, DOJ, ODNI, PM-ISE, and the White House Office of National Drug Control Policy (ONDCP). The Fusion Center Sub-Committee advises and supports the ISA IPC by:

- Recommending priorities for federal support to fusion centers;
- Developing strategies for strengthening and maturing the National Network;
- Preparing guidance and policy on fusion center-related activities;
- Providing a forum for sharing best practices, lessons learned, and resolving interagency issues; and
- Serving as a resource to SLTTPS partners for the sharing of homeland security, terrorism, and law enforcement information.

The Fusion Center Sub-Committee is facilitating a number of near- and mid-term projects intended to mature the National Network including the development and implementation of a Federal Resource Allocation Criteria Policy; a common operational and sustainment cost reporting system; and a repeatable BCA and gap mitigation process.

3.2.4 Federal Resource Allocation Criteria (RAC)

One of the Federal Government's first priorities for coordinating support to fusion centers was to clearly define the parameters for the allocation of federal resources to fusion centers. The Fusion Center Sub-Committee developed the Federal Resource Allocation Criteria (RAC) policy, which was formally issued in June 2011. This policy defines objective criteria and a coordinated approach for prioritizing the allocation of federal resources to fusion centers. The goal of this policy is to enhance the effectiveness of federal support to the National Network and strengthen support to fusion centers to execute the statewide fusion process.

Recognizing that while the Federal Government does not dictate where fusion centers should be built and maintained, it does have a shared responsibility with state and local governments to promote the establishment of a National Network to facilitate effective information sharing. Since 2001, the Federal Government has provided significant grant funding, training, technical assistance, exercise support, federal personnel, and access to federal information and networks to support fusion centers.

In the face of increasing demands and limited resources, the prioritized resource allocation established through the criteria in the RAC policy will enable the Federal Government to concentrate resources in a manner that will improve the efficiency of its support to fusion centers. The implementation of the RAC policy will enable fusion centers to mature their capabilities in order to effectively execute the statewide fusion process and fulfill their roles in the ISE.

The RAC policy is intended to guide the allocation of federal resources to fusion centers in a manner that:

- Collectively supports the development of a National Network;
- Effectively balances the need for supporting SLT as well as federal imperatives; and
- Ensures efficient information sharing across federal and SLT partners.

Implementing the RAC policy will help bring consistency and transparency to the process of prioritizing the allocation of federal resources to fusion centers. It is a key first step in establishing coordinated, long-term sustainment of the National Network.

The New York State Intelligence Center's Vigilance Project

The New York State's fusion center—the New York State Intelligence Center (NYSIC)—recently published a report titled, *The Vigilance Project: An Analysis of 32 Terrorism Cases Against the Homeland*. This report identifies trends and themes among 32 terrorism cases in the United States that have been investigated since 11 September 2001. The Center plans to regularly update the product with new terrorism investigation case information, so that it may be shared with law enforcement personnel to support their efforts in identifying patterns and trends that may be indicative of criminal or terrorist activity. The product

identifies 25 variables for analysis when looking for trends among the terrorism cases, including demographics of individuals, plot targets, and tactics. According to the report, "The variables selected for analysis best capture potential indicators of terrorist activity." Fusion center staff can use this tool to enhance their efforts in detecting and preventing terrorist activities by maintaining awareness of the trends noted in this product. It is also meant to provide law enforcement officers in the field with a greater ability to recognize and report suspicious activity and keep them engaged in the fight against terrorism.

3.2.5 Fusion Center – High Intensity Drug Trafficking Area (HIDTA) Partnership

On 10 February 2011, approximately 30 representatives from federal, state, and local agencies—including HIDTAs, fusion centers, DHS, ONDCP, DOJ, the FBI, the National Drug Intelligence Center (NDIC), and PM-ISE—met in Atlanta to explore how best to leverage fusion centers and HIDTAs as uniquely valuable resources and partners for its customers and participating entities. This session was a part of the Fusion Center Sub-Committee's effort to establish stronger partnerships between HIDTAs and fusion centers, and to further define the operational roles, responsibilities, and relationships among these unique yet complementary intelligence and information sharing entities.

The significant breadth of expertise and the cumulative years of experience represented at this meeting produced an incredibly valuable discussion. Throughout the session, several key themes continued to emerge:

- When done properly, the collocation and/or integration of fusion centers and HIDTA Investigative Support Centers into a unified command structure may bring significant benefits; but this should not be advocated as a universal approach.
- Directors do not generally view each other as competing for mission space as they do for quality resources, e.g. well-trained analysts; but mission drift can potentially dilute the unique value of each program.
- There is a need to continually reeducate and revalidate with customers, i.e. police chiefs and sheriffs, the value and respective capabilities available to their agencies through BOTH fusion centers and HIDTAs.
- Formalized requirements and collection processes would enable fusion centers to convey what to look for, but would also provide a process for better understanding what line officers are seeing, and feeding the NSI, as well as ultimately benefiting HIDTA investigations.
- Enhanced concepts of operation and commonly understood terminology (e.g. national security vs. criminal intelligence and threat vs. target) are necessary to help clear the uncertainty in the delineation between HIDTA and fusion center missions among both leadership and customers, as well as those working within the respective entities.

This meeting underscored the importance of the role of the National Network to the greater national security enterprise, as well as the need to ensure appropriate operational relationships with existing entities such as the HIDTAs.

In addition to the meeting in Atlanta, a panel at the National Fusion Center Conference (NFCC), entitled *Promoting Stronger Partnerships with Fusion Centers*, highlighted ongoing efforts to strengthen relationships between fusion centers and major cities intelligence units, as well as fusion centers and HIDTAs. Building upon the meeting in Atlanta, the objectives of this panel were to further discuss the common obstacles and key enablers to effective coordination and communication among fusion centers and stakeholders; to learn about best practices currently being implemented throughout the network to address information sharing challenges, and to discuss tools and resources to assist fusion centers with building more effective partnerships with their customers and partners.

As a result of discussions at the NFCC, these partners will continue to build and formalize relationships within their states through business processes and concepts of operation, and to enhance intrastate coordination and execution of the statewide fusion process. Both fusion center and HIDTA directors are essential partners in leading these efforts.

3.2.6 Improving Information Sharing On Threats to the Southwest Border

On 27 April 2011, DHS hosted the "2011 Southwest Border Law Enforcement Intelligence and Information Sharing" meeting for more than 100 local, state, and federal law enforcement and IC participants at the El Paso Intelligence Center. The purpose of the meeting was to bring Southwest Border security stakeholders together to examine ways to improve information sharing on threats to our Southwest Border.

The meeting focused on perceptions of the threats along the Southwest Border, intelligence needs to combat those threats, information sharing challenges, and information holdings which might be useful to a broader group. This meeting recognized that state and local authorities require more focused and timely analysis from their federal partners and need better collaboration with federal, state, and local authorities, as well as with the HIDTAs and fusion centers. It was also noted that increased HIDTA and fusion center collaboration will support efforts to meet state and local information sharing needs and to avoid duplication of efforts.

3.2.7 Major City Chiefs Intelligence Unit Commanders Group

Over the past year, DHS hosted a series of regular meetings with the Major City Chiefs Intelligence Commanders Group. These meetings provided an opportunity to improve information sharing efforts among these stakeholders, discuss existing information sharing challenges, and examine and identify agency-specific information needs. These meetings also provided an opportunity to discuss best practices, lessons learned, and opportunities to further enhance the operational roles and relationships between major city intelligence units and fusion centers.

3.2.8 National Fusion Center Conference (NFCC)

In March 2011, nearly 1,000 federal, state, local, tribal and territorial fusion center stakeholders attended the fifth annual NFCC in Denver, Colorado. The conference served as a forum for fusion center stakeholders to discuss key policy issues and receive training, technical assistance, and other support to achieve a baseline level of capability through a series of plenary and breakout sessions. Attendees included Fusion Center Directors, state Homeland Security Advisors, fusion center analysts, and homeland security and law enforcement professionals representing all levels of government. This annual

conference also informs and advances the efforts of the Fusion Center Sub-Committee, providing a vital feedback loop to the directors, and an opportunity to engage them in preparing future work plans. In Denver, fusion center personnel and federal partners collectively identified priorities for the upcoming year to enhance the national network:

- Reaffirm the four COCs;
- Continue to use partnerships to advocate for fusion center sustainment;
- Strengthen statewide fusion process activities; and
- Engage in performance management efforts

National Terrorism Advisory System (NTAS)

The NTAS went live on 26 April 2011.[36] Under the new, two-tiered system, DHS will coordinate with other federal entities to issue formal, detailed alerts regarding information about a specific or credible terrorist threat. Each of these alerts will include a clear statement that there is an "imminent threat" or "elevated threat." Each alert will also provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals and communities can take.

Depending on the nature of the threat, the alert may be sent to a limited, particular audience like law enforcement, or a segment of the private sector, like shopping malls or hotels. Or the alert may be issued more broadly to the American people distributed—through a statement from DHS—to the news media as well as via the DHS website and social media channels such as Facebook, Twitter and blogs.

A key component of the new NTAS process is that it incorporates points of contact from across the Federal Government, state and local representatives, and the public sector, as applicable, to coordinate input prior to issuing the NTAS alert. This process will ensure that NTAS alerts are tailored for a specific sector, including components of the Federal Government; state, local, and tribal entities; critical infrastructure entities; and selected private-sector partners, as needed, to facilitate appropriate action. In addition, all NTAS alerts require a set duration date, so that information can be re-evaluated on a regular basis.

NTAS was developed in that same collaborative spirit: it was largely the work of a bi-partisan task force that included law enforcement, former mayors and governors, and members of the previous Administration.

36 Presidential Policy Directive – 7, National Terrorism Advisory System (NTAS), directed the Secretary of Homeland Security to establish the NTAS as a refinement to the Homeland Security Advisory System.

3.3 Interagency Threat Assessment and Coordination Group (ITACG)

The end-state goal of the ITACG is improved information sharing between federal and state, local, tribal, territorial, and private-sector partners to help deter and prevent terrorist attacks. To achieve this goal, the ITACG Detail, housed at the NCTC, assists analysts in integrating, analyzing, and otherwise preparing versions of intelligence products, derived from information within the scope of the ISE, that are either unclassified or classified at the lowest possible level and suitable for dissemination to these mission partners. The ITACG Detail is directed by a senior intelligence official appointed by the DHS. A deputy director is appointed by the FBI. ITACG detailees, who are representatives of state, local and tribal homeland security, law enforcement, fire, and health agencies, serve on a one-year fellowship sponsored by the DHS. PM-ISE is responsible for monitoring and reporting on the efficacy of the ITACG.[37,38]

3.3.1 Assessment of the Detail's Access to Information

The Congress has recently expressed interest in knowing whether ITACG detailees have access to the information they need, within the scope of the ISE, at the NCTC to accomplish their mission.[39] In December 2010, the ITACG Detail was realigned under NCTC's Deputy Director for Operations Support (DD/OS). Based on interviews with NCTC leadership and ITACG personnel, this realignment served to improve detailees' access to information by exposing them to the main stream of intelligence at NCTC. According to the DD/OS, the detailees have more than adequate access to information at NCTC for what they are expected to do.

A significant indicator of the ITACG detailees' access to information is their involvement with a special site exploitation effort currently ongoing at NCTC. From the outset, the detailees were brought in "front and center" for the primary purpose of determining what is important to SLTTPS consumers for classified and unclassified "tearline" products.[40] According to the DD/OS, the decision to involve the detailees was easy—"no one even had to think about it." The ITACG Detail is integrated into NCTC operations and their involvement with the special site exploitation effort is evidence of both their access to information at NCTC, and their centrality to the effort to produce relevant information for SLTPS partners. ITACG Detailee Lieutenant Sam McGhee, from the Aurora (Colorado) Police Department, summarized it best by stating, "In my 30

> "In my 30 year tenure as a law enforcement officer, I never would have thought I would have this level of access. It's a testament to the commitment in improving information flow to prevent something bad from happening again."
> *– ITACG Detailee Lieutenant Sam McGhee, Aurora Police Department (Colorado)*

37 Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, sec. 210D(c), codified as amended at 6 U.S.C. 124k(c).

38 The last report was dated November 2010, and can be found at: www.ise.gov. Future reporting on the ITACG will be included in PM-ISE's Annual Report to the Congress on the State of the ISE.

39 Reducing Over-Classification Act, Pub. L. No. 111-258, 124 Stat. 2648, sec. 5(c).

40 Portion of an intelligence report which has been cleared for disclosure or release.

year tenure as a law enforcement officer, I never would have thought I would have this level of access. It's a testament to the commitment in improving information flow to prevent something bad from happening again."

While all detailees are faced with a steep learning curve initially, they become quickly acclimated and gain a deep appreciation of how much information is available to them. According to one detailee, "access is not an issue—it's more than adequate. The real challenge is how to manage the deluge of information, and use it in a manner that makes a difference." The permanent federal intelligence analysts assigned to the ITACG—by the FBI, NCTC, and DHS—are key to the ITACG detailees' success. These analysts provide the detailees with on-the-job training, assistance in performing their day-to-day activities—including conducting intelligence-related activities—and help in preparing and delivering presentations.

3.3.2 ITACG Involvement in Intelligence Production

Since June 2010, the ITACG Detail reviewed 128 draft intelligence products and 254 daily summaries in support of SLTTPS partners. In addition, the Detail authored, co-authored, or recommended the production of 27 Roll Call Release products—a collaborative DHS, FBI, and ITACG product line—intended for "street-level" first responders.

> "NYPD and FDNY find the Roll Call Releases to be extremely useful…it's just what the doctor ordered. The bullet point format is ideal for police officers and firefighters who must retain a great deal of information which is necessary to help them protect their own lives and the lives of others, and which makes them alert to questionable activities that they may witness in a given situation."
> – *NYPD Representative*

Another critical function of the ITACG Detail is to identify intelligence products that should be downgraded in classification, for release to SLTTPS partners. Since June 2010, the ITACG Detail has requested 64 product downgrades of which 39 have been approved and disseminated.

3.3.3 ITACG Performance

Since March 2010, DHS I&A solicited a customer feedback survey on every intelligence product it released, including products the ITACG is involved in producing. While this feedback is not necessarily a *direct* reflection on ITACG's performance, since the ITACG *is not responsible for* DHS I&A intelligence production, the surveys provide insight into how customers use products ITACG is involved with, to include a rating on how relevant the product is to the their missions.[41]

State and local survey feedback during the period March 2010 to March 2011 was positive. Approximately 80 percent of the respondents rated the intelligence products as either "very important" or "critical" to their mission. In addition, DHS I&A tracks product

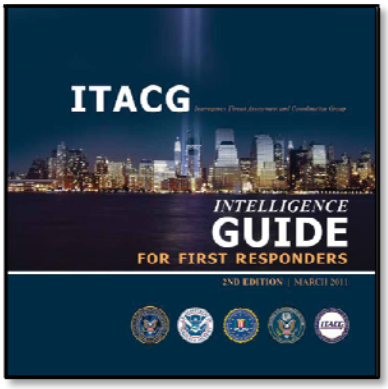
41 DHS I&A also submits an annual report to the Congress on voluntary feedback on DHS intelligence or other information products, as required by Section 210A9(g) of the Homeland Security Act of 2002, as amended. The third annual report was submitted in November 2010.

utilization and found nearly 99 percent of its products are either integrated into state and local finished intelligence products; shared with federal, state, local, and private-sector partners; or used for situational awareness, security preparations, or training purposes.

Another indicator of ITACG's performance is reflected in the feedback gathered from state and major urban area fusion centers. During the Fusion Center BCA, fusion center directors were asked to comment on the utility of federally-produced intelligence. The majority of the directors noted distinct improvements in the intelligence products provided to them, especially over the past year. They indicated that intelligence reporting has become more frequent, more relevant, and more concise, and attributed these improvements to the leaderships' focus on improving intelligence dissemination. They specifically indicated that joint-seal DHS I&A and FBI products, including Roll Call Releases, contribute significantly to their ability to fulfill their missions.

3.3.4 Intelligence Guide for First Responders, 2nd Edition

The first edition of the *Intelligence Guide for First Responders* was published in October 2009. Seventy-five thousand copies of the guide were mailed to more than 16,000 police departments and more than 32,000 fire departments across the country, including to Hawaii, Guam, Puerto Rico, and the Virgin Islands. The state and local response to the Guide has been overwhelmingly positive, and based on continued requests for additional copies, the ITACG has requested to print an additional 50,000 copies.



The 2nd edition of the *Intelligence Guide for First Responders* incorporates feedback from the field, and includes two new sections—"Reporting Suspicious Activity," which covers participation in the NSI, and "Joint Partnerships," which highlights several joint federal, state, local, and tribal activities around the country. This edition has been sent to the fusion centers and the JTTFs for further dissemination to state, local, and tribal partners. The guide is also posted to ise.gov, nctc.gov, leo.gov, and all HSIN portals.

3.3.5 Guide for Public Safety Personnel

In addition to the First Responders Guide, ITACG, in collaboration with DHS, DOJ, the FBI, and NCTC, has produced the *Countering Terrorism: ITACG's Guide for Public Safety Personnel.* This reference guide is designed to assist first responders in recognizing activities or conditions that may be indicative of potential terrorist activity. The Guide focuses on three key areas: Indications and Warning; Tactics and Targets; and Chemical, Biological, Radiological, Nuclear, and Explosive threats. ITACG is producing 250,000 copies of this Guide for dissemination to fusion centers and JTTFs, for further dissemination to state, local and tribal mission partner.

3.3.6 Federal Community Orientation Program

A critical function of ITACG is educating and advising intelligence analysts about the needs of SLT homeland security and law enforcement officers, and other emergency response providers. Last year, ITACG instituted the Federal Community Orientation Program to facilitate direct interaction with IC member agencies in the Washington, DC region. During each site visit, ITACG personnel explain the

ITACG mission, receive briefings about the host agency's mission, and tour the components' operations centers. To date, ITACG detailees visited the Terrorist Screening Center, the Transportation Security Operations Center, the National Security Agency, and the Open Source Center.

3.4 Tribal Information Sharing

3.4.1 Information Sharing Implications of the Tribal Law & Order Act (TLOA)

On 29 July 2010, President Obama signed into law the TLOA.[42] The TLOA establishes accountability measures for the federal agencies responsible for investigating and prosecuting reservation crime, and provides Indian tribes with additional tools to combat crime locally. Specifically, the TLOA strengthens tribal law enforcement agencies' criminal intelligence information sharing capabilities by permitting federally-recognized Indian tribes to access national criminal information databases for the purpose of either entering information into these databases or obtaining information from these databases.

Indian Country covers an expansive area of the United States; nearly 56.2 million acres, encompassing ports and spanning international borders. For example, the Chippewa Tribal Nation is located at the port of Sault Ste Marie, Michigan—a key point where cargo passes into the United States from Canada—and the Tohono O'odham Indian Reservation includes 75 miles of the U.S. Southwest Border. Tribal governments counter threats to homeland security, alongside their federal, state, and local counterparts, every day. Gaps in information sharing with tribal partners could result in either criminal and/or violent extremist activity going undetected. According to the DOJ's National Drug Intelligence Center, most illicit drugs available in the United States and thousands of illegal immigrants are smuggled into the United States across the Southwest Border. Of some concern to law enforcement officials is the potential for cross-border drug smuggling routes to be used to move terrorists or weapons of mass destruction (WMD) into the United States.[43] Therefore, seamless information sharing between federal, SLT, and international partners is necessary to address smuggling and to combat transnational threats.

3.4.2 Building the Community

This past year PM-ISE dedicated efforts toward building a community to increase cooperation between federal and SLT law enforcement agencies. Increasing Indian Country representation in the ISE required focused outreach efforts, including outreach to:

- DHS I&A
- Fusion centers
- NSI PMO
- FBI Criminal Justice Information Services (CJIS)

---

42 Public Law 111-211

43 U.S. Southwest Border Smuggling and Violence, National Drug Threat Assessment 2010, February 2010, available at: http://www.justice.gov/ndic/pubs38/38661/swb.htm

- FBI Indian Country Unit
- DOI Bureau of Indian Affairs
- National Law Enforcement Telecommunications System (Nlets)
- International Association of Chiefs of Police (Indian Country Section, Intelligence-Led Community Policing, and Victim Services)
- Michigan Tribal Chiefs Association
- California Tribal Police Chiefs Association

3.4.3 Providing Access to all Tribal Front Line Officers

The National Law Enforcement Telecommunications System (Nlets) links together and supports every state, local, and federal law enforcement, justice and public safety agency for the purposes of sharing and exchanging critical information. Because tribes are sovereign nations, each tribe interacts with state, local, and federal law enforcement in different ways. Tribes in some states, for example, have comprehensive law enforcement agencies that can access Nlets through their state-owned systems. However, the majority of tribes with law enforcement organizations have less sophisticated systems that limit their access to the state systems. The sharing of information between law enforcement and tribes is essential to ensure that state, local, and tribal law enforcement officers approach vehicles with all the information necessary for a safe traffic stop. Recently, the Nlets Program Management Office asked PM-ISE to assist in improving Nlets access for tribal law enforcement organizations. PM-ISE reached out to Indian Country, expanded their knowledge of Nlets benefits, and established the first ever connectivity pilot with four tribes in separate regions of the United States.

KOMOnews.com

3.4.4 Tribal Integration with NSI and Fusion Centers

The Tribes have used SAR-like approaches for many years, particularly those that have gaming facilities. PM-ISE has partnered with the NSI PMO to administer the NSI Line Officer Training to all Tribal law enforcement agencies, as an attempt to further integrate Indian Country into the NSI. As a result of this initiative, NSI PMO has mailed NSI training materials to 172 out of approximately 200 tribal law enforcement agencies.

Fusion centers are also expanding their participation with Indian Country. PM-ISE, in coordination with federal partners and various state authorities, is supporting the integration of tribal law enforcement personnel in fusion centers. Successful examples of these efforts have occurred in Oklahoma, Arizona, and Washington State. Tribal presence in fusion centers is most often realized through their participation in liaison programs, serving as liaison officers, or as embedded analysts. These programs allow the fusion centers to support robust information sharing on lands that are under the complete control of tribal governments, giving a full threat picture of the region.

3.4.5 FBI and Tribal Integration

The FBI is responsible for developing and implementing strategies to address the most egregious crime problems in Indian Country where the FBI has responsibility, as well as supporting joint investigative efforts with the Bureau of Indian Affairs-Office of Justice Services (BIA-OJS), tribal law enforcement, and Safe Trails Task Force (STTF) personnel.

The FBI has approximately 105 Special Agents working in support of Indian Country investigations. Criminal jurisdiction in Indian Country is a complex maze of tribal, federal, and state jurisdictions. The FBI has investigative responsibility for approximately 200 Indian Reservations out of the 565 federally-recognized Indian Tribes in the United States. The FBI initiated and leads the STTF, program which is designed to unite federal and SLT law enforcement agencies to combat crime and enhance information sharing practices in Indian Country. There are 19 active FBI-led STTFs in the United States.

3.5 Multimodal Information Sharing

Building on a strong foundation of information sharing between and among federal, state, local, and tribal governments as well as international and private-sector partners, ISE mission partners are pursuing information sharing initiatives aimed at protecting and reducing vulnerabilities at our borders, ports, and airports, and to enhance overall air, maritime, and transportation security, consistent with the National Security Strategy. PM-ISE supports multiple aspects of information sharing in the air and maritime domains, primarily to promote cross domain information integration, and is also participating in efforts to develop core concepts for the *National Strategy for Global Supply Chain Security*.[44]

Air Domain Awareness Initiative

The Department of Transportation (DOT), in coordination with the Federal Aviation Administration (FAA), played a leadership role in the Information Sharing Working Group within DHS's ongoing Air Domain Awareness (ADA) initiative. The initiative was begun to develop an integrated, 'whole of government' approach to ADA, with the ultimate goal of fusing intelligence, surveillance data, and analysis across federal, state, local, and tribal governments, as well as private entities and foreign partners with aviation safety and security responsibilities. Throughout this past year, the Information Sharing Working Group established a Sub-Committee focused on identifying and offering solutions to existing information sharing barriers, and coordinated with DHS to stand up a collaborative online ADA information sharing portal for the ADA community of interest.

44 This strategy, and the subsequent National Action Plan for Global Supply Chain Security, will provide the framework to better secure the global supply chain and identify opportunities to improve the sharing of threat information as it relates to intermodal cargo transport.

3.5.1 Information Sharing in the Air Domain

In response to the need for a whole of government approach to achieving Air Domain Awareness (ADA), stakeholders participated in a series of ADA Summits that provided the impetus for development of a governance structure to provide direction and oversight for ADA implementation. From these summits, the concept for an ADA Board emerged, along with four working groups: the Information Sharing Working Group; the Capabilities and Resources Working Group; the Policy, Guidance, and Governance Working Group; and the Air Surveillance Working Group. The ADA Board will coordinate interagency activities and leverage the National Security Staff Transborder Security Interagency Policy Committee (IPC) when required.

In January 2011, the Next Generation Air Transportation System (NextGen) Joint Planning and Development Office (JPDO) kicked off an effort to develop a Concept of Operations (CONOPS) for the Integrated Surveillance Initiative. The goal of this effort is to provide multi-agency integrated aviation surveillance capabilities by 2016. The CONOPS includes cross-community sharing of pre-flight information, enhanced information sharing and situational awareness, and automated sharing of in-flight updates and changes to flight characteristics. The planning and creation of the Integrated Surveillance Initiative will facilitate the use and reuse of data from the entire aviation community of interest, saving time, money, and efficiencies.

PM-ISE is supporting these air domain initiatives by actively participating at the ADA Summits and in the working groups; by providing technical assistance in their development of information sharing architectures; and by sharing ISE best practices and tools to promote information sharing in the air domain.

The DoD Civil Aviation Intelligence Analysis Center (CAIAC)

In July 2010, the Under Secretary of Defense for Intelligence designated the Department of the Air Force as the lead DoD intelligence representative for the civil aviation intelligence mission, to establish the DoD CAIAC. This new Center, which is expected to reach Full Operating Capability in FY 2013, will serve as a Department-level shared resource that brings in-depth knowledge and expertise of the global commercial aviation industry to the nation's most challenging intelligence problems. The CAIAC will also provide a critical link in an emerging coordinated interagency approach to Air Domain Awareness.

3.5.2 Information Sharing in the Maritime Domain

The National Maritime Intelligence Center (NMIC) and PM-ISE are analyzing opportunities to improve information sharing between federal and SLTPS entities in the maritime domain. Currently several port-based, cross-governmental programs and initiatives exist to monitor and track vessel, cargo, and passenger data. The standardized sharing of vessel, cargo, and passenger data would maximize situational awareness and emergency response across transportation domains. Some of the agencies and offices that can contribute to dissemination methods, such as a common or user-defined operating picture, shared space, or dashboard, include the DOT's MARVIEW, the Coast Guard's Interagency

Operations Centers, Navy Maritime Operations Centers, JTTFs, port authorities, and state, county, tribal, and municipal law enforcement and safety offices.

The U.S. Customs and Border Protection (CBP), U.S. Coast Guard (USCG), and Immigration and Customs Enforcement (ICE) components of DHS are engaged in the Joint Targeting Architecture Project to improve information sharing relating to maritime targeting protocols and procedures, since all three agencies have distinct authorities to protect the United States against persons, cargo, and other dangers in the seaports. In addition, in March 2011, DHS held an Executive Summit for the DHS Small Vessel Security Implementation Plan Report to the Public. This included stakeholders from the private sector, USCG, CBP, and other federal and SLT authorities.

To increase Maritime Domain Awareness (MDA), the National MDA Coordination Office approved the MDA Interagency Solutions Analysis to identify and prioritize interagency MDA capability gaps and to identify collaborative interagency solutions to address and mitigate those gaps.[45] The Office has also asked the DoD Executive Agent for MDA to develop a national architecture for sharing unclassified MDA information. This funded effort is tasked with improving the real-time sharing of data regarding vessel arrivals, vessel tracking, and related U.S. threat response activity. PM-ISE is providing planning, technical, and governance support to this whole of government initiative.

Additionally, on the MDA Information Portal—www.mda.gov—the "Maritime Domain Awareness Information Exchange" has been implemented and designed to provide a collaborative environment where members of the maritime community of interest can learn and share information that will enhance and improve situational awareness within the maritime domain.

Maritime Safety and Security Information System

The Maritime Safety and Security Information System is a multilateral non-classified data-sharing system to improve the MDA of the United States and its allies and partners through the sharing of Automatic Identification System data through an Internet-based system. This initiative has obtained international acceptance as a standard for the exchange of maritime data and has become a maritime data sharing system of choice by more than 60 nations.

Multimodal Information Sharing Taskforce (MIST)

The MIST is an interagency research effort designed to foster collaboration and capture best practices in information sharing in a regional port environment. MIST creates a structure for collaborative problem solving that focuses on uncovering unique local issues and communicating these to national policy makers. The fourth MIST workshop, held in Philadelphia in September 2010, provided a venue for private-sector input into the development of information sharing processes. MIST findings show that industry-government collaboration is improved by providing financial and social incentives to industry; by improving two-way communication; by addressing issues with interagency collaboration; and by increasing cultural awareness. MIST also surfaced a number of best practices for collaboration, including

45 These issues were captured in the MDA Interagency Solutions Analysis 1.0 Report, 31 January 2011.

the U.S. Customs Trade Partnership Against Terrorism program, the expansion of industry-run education programs for government employees, and the inclusion of industry in emergency preparedness activities and Integrated Operations Centers.

The Maritime Exchange

To promote and protect maritime commerce for the Delaware River maritime community, the Maritime Exchange[46] developed and operates the electronic information center for ship and cargo processing in the Delaware River and Bay. Maritime On-Line provides comprehensive web-based services to fulfill a variety of commercial, security, and safety-related maritime needs. The system includes ship schedules, navigational safety information, electronic cargo and vessel clearances through multiple federal agencies, notice of arrival/departure, real-time position information, and crew list reporting. Developed under the specific direction of the members of the maritime business community and the federal and state government agencies that regulate them, Maritime On-Line is the one-stop information source for Delaware River and Bay international commerce activity. Live data feeds are also provided, in real-time, to the Pennsylvania Criminal Intelligence Center. There, analysts review data and collaborate on tactical operations in concert with federal, state, and local partners.

3.6 WMD Information Sharing

As introduced in the 2010 ISE Annual Report, PM-ISE supported DHS's Domestic Nuclear Detection Office (DNDO) by funding the initiation of their inter-governmental information sharing exchange. This mechanism will facilitate and standardize the real-time sharing of radiological and nuclear alarm adjudication data, shipment and licensee data, and will improve analysis of post-seizure data.

In July 2011, DNDO, with the cooperation of DHS/CBP, Defense Threat Reduction Agency (DTRA), and state and local representatives in Los Angeles and Kansas City will demonstrate the real-time information exchange of radiological/nuclear alarm adjudication data derived from the screening, scanning, or inspection of transient cargo. Participants committed to this live exchange include: LAPD, LA County Sheriff, LAFD, LA County Fire, Long Beach Fire Department, federal entities (DNDO, CBP, DTRA), and the Kansas City Terrorism Early Warning Center. This effort is included in DHS's Information Sharing Governance Board for executive sponsorship, oversight, and intra-departmental support.

46 The Maritime Exchange for the Delaware River and Bay is a non-profit trade association which serves as “the voice of the port” for the Delaware River maritime community.

3.6.1 Securing the Cities (STC)

STC was launched in July 2006 as way to protect a high-risk urban area, such as the New York City (NYC) region, from a potential radiological or nuclear attack. The initial emphasis was on building a regional enterprise architecture for the NYC region that will allow real-time sharing of data from fixed, mobile, maritime, and human portable radiation detection systems. The NYC program is entering into a new phase where a greater emphasis will be placed on integration of state and local Preventive Radiological Nuclear Detection (PRND) capabilities into federal operations. In addition, the President's FY 2012 budget has called for the expansion of STC into one additional Urban Areas Security Initiative region.

3.6.2 West Coast Maritime Pilot

The West Coast Maritime Pilot was intended to assess capabilities that reduce vulnerabilities from nuclear and radiological weapons and materials delivered via small vessels across maritime borders. DNDO provided technical assistance to local authorities in the Puget Sound and San Diego areas to develop a nuclear detection architecture that reduces high-consequence maritime vulnerabilities. The pilot, which began in 2007, involved four phases: 1) collect information on existing maritime PRND capabilities in each port area; 2) design an enhanced maritime PRND architecture including development of response protocols; 3) deploy capability, including training and equipment; and 4) assess and document each pilot. The pilot training evolutions, exercises, and drills successfully concluded in 2010, and a final report was released in February 2011.

3.7 Intelligence Community (IC) Intelligence Sharing Services

A variety of IC intelligence sharing services provide analysts , operators, and investigators with on-demand electronic dissemination applications to facilitate information sharing at and across all levels of security.[47] Through these services, intelligence products are shared to appropriately cleared consumers via the Joint Worldwide Intelligence Communications System (JWICS), the Secret Internet Protocol Router Network (SIPRNet), and the Internet.

3.7.1 NCTC CURRENT

In September 2010, *NCTC CURRENT* replaced *NCTC Online*. *NCTC CURRENT* is the CT Community's premier web site for reporting and analysis. It allows users to easily browse titles and summaries, with full text articles, graphics, and multimedia presentations just a point and click away. *NCTC CURRENT* also features links to related articles, maps, photos, and videos, as well as the ability to search analytical products published by the IC and other important partners. *NCTC CURRENT* is available on JWICS with a valid public key infrastructure (PKI) certificate and on SIPRNet with a valid Passport account.

3.7.2 Worldwide Incidents Tracking System (WITS)

NCTC's WITS is the U.S. Government's authoritative database of terrorist attacks, compiled exclusively from open source information. WITS supports both the NCTC Report on Terrorism and the State

47 IRTPA, Sec. 1016(b)(2)(F)

Department's annual Country Report on Terrorism. Policymakers, intelligence analysts, adjudicators, academics, and foreign partners use WITS data for a variety of purposes.

NCTC has recently launched the next generation of the WITS. WITS NextGen includes a page that incorporates all of the information and links from the previous WITS Classic public site, which was decommissioned on 31 August 2010. WITS NextGen is available to the public at https://wits.nctc.gov and includes the following features:

- Incident maps – WITS NextGen enables users to plot incidents using Google Maps or Google Earth (Google Earth plug-in required). The data can be plotted using cluster maps, heat maps, or density maps.
- Time maps – This feature allows users to plot incidents on maps over time, showing chronological changes by merely sliding a pointer.
- Improved search filters – WITS users can easily add and remove search filters to tailor their searches and find the exact data that is desired.
- Intuitive menu tabs – Once the WITS database delivers search results, users can "tab" through the results, further tailoring the results by criteria such as event types or locations.
- Customizable views – Column headings for search results can be added or removed, allowing for greater flexibility in viewing the data.

3.7.3 Intelligence Today

Intelligence Today, the daily online compendium of analytic products from across the IC, marked its first anniversary on 22 March 2011 by posting its 48,450th article. *Intelligence Today* uses the power of the secure Internet to produce an online newspaper for more than 9,600 IC and policymaker subscribers. Products are drawn from more than 60 sites, and organized into a "front page" with links to top stories, individual sections devoted to geographic and subject matter areas, and archives of previously published material. *Intelligence Today*'s readers are drawn from more than 30 agencies and organizations across the policymaking realm, the IC and the military. About 1,150 readers visit the site on a daily basis.

3.7.4 Intelink

Intelink is a suite of web-based applications, tools, and services (including search) provided by the Intelink Enterprise Collaboration Center. It exists on JWICS, SIPRNet, and on the Unclassified network DNI-U. Intelink recently crossed the 100 million document threshold for records exposed to Intelink search services across the Unclassified, Secret, and Top Secret networks combined. In one month alone this year, Intelink recorded over two million searches. These milestones highlight the ability of IC personnel to access more information quicker and more effectively, enabling them to better share information and thus perform their missions. In addition, Intelink's user base passed the 200,000 mark in the spring of 2011. Increased use by the DoD and the law enforcement community over the past year have contributed to the growth, nearly doubling use on the Secret and Unclassified networks.

3.8 Watchlisting and Screening

The Watchlisting and Screening Sub-Committee of the ISA IPC focuses on the identification of watchlisting, screening and sharing policies, business processes, and technology, with particular focus on the Counterterrorism Watchlisting Community's end-to-end nomination and screening processes. The Sub-Committee is chaired by the National Security Staff and includes additional members from the CIA, DOT, DHS, DoD, DOJ, DOS, ODNI, the FBI, and the FBI-managed TSC.

Since the development of the consolidated terrorist watchlist that is in use today,[48] there have been many successes and improvements to watchlisting processes. Some of the more recent improvements include clearer definitions of federal agencies' roles and responsibilities, streamlining and standardizing nominations processes, improved use of biometrics for identification, and improved analytical and technological capabilities.

Despite the many successes and improvements to terrorist watchlisting and screening that have been institutionalized across the community since 9/11, the attempted bombing of Northwest Airlines Flight 253 on Christmas Day 2009 demonstrated that challenges still remained and improvements to the watchlisting and screening processes were necessary to keep our nation safe.

The National Security Staff led an effort to review current processes and provided recommendations to improve watchlisting business processes and rules while safeguarding the P/CR/CL of Americans.

3.9 Private-Sector Information Sharing

3.9.1 Collaborative Partnerships between the Private Sector and the IC

In March 2010, the ODNI Private Sector Partnerships office and the ODNI Analysis office sponsored a joint pilot project that brought together experts from the private sector with experienced IC analysts to develop collaborative partnerships. The goal of this effort is to provide IC analysts with a better understanding of select national and homeland security-related industries. It seeks to increase the depth of expertise among the participating analysts and is not intended as a mechanism either for operational activities or for formal coordination between industries and the IC.

The six-month pilot was successful and in March 2011 the Analyst-Private Sector Program was launched as a joint ODNI and DHS I&A program. Beginning in 2012, DHS I&A will serve as the executive agent of the program for the IC with oversight from the ODNI Private Sector Partnerships office.

3.9.2 InfraGard

InfraGard is an FBI information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants who are dedicated to sharing information and

48 Per HSPD-6

intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories and have more than 42,000 members.

3.9.3 Domestic Security Alliance Council (DSAC)

The DSAC is a strategic partnership between the FBI and the U.S. private commercial sector and enhances communications and promotes the timely and effective exchange of information. The DSAC advances the FBI mission in preventing, detecting, and investigating criminal acts, particularly those affecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information. The DSAC membership consists of 400 individuals representing 211 companies.

3.9.4 Tripwire Program

The FBI's "Tripwire" program is designed to involve private-sector entities in identifying groups or individuals whose suspicious behavior may be a precursor to an act of terrorism. Tripwires are used by the private sector to alert authorities to activities which may not have risen to the level of law enforcement or intelligence scrutiny.

Terrorist Plot Thwarted in Texas

On 22 February 2011, Khalid Aldawsari, a chemical engineering major studying at South Plains College in Levelland, Texas, was arrested by federal authorities on the charge of attempted use of a weapon of mass destruction. One of the many targets of his plot was the home of former President George W. Bush in Dallas, Texas. Aldawsari came to the United States on a student visa to study at Texas Tech University, transferring to South Plains College in the fall of 2010.

Aldawsari raised the suspicions of North Carolina chemical supply company representatives when he unsuccessfully tried to receive a shipment of phenol, a chemical that can be used to manufacture explosives.[49] Aldawsari was informed that such a shipment could not be sent to his residence due to safety regulations. Aldawsari subsequently provided a Texas address of the freight company as an alternative shipping destination. When the shipment arrived at the freight company, officials refused receipt and it was sent back to the chemical supply company.

When the shipment was returned to them, representatives from the chemical supply company in North Carolina contacted the FBI to report Aldawsari's attempted purchase. Additionally, in Texas, officials from the freight company contacted the Lubbock Police Department with their concerns. These two phone calls placed by private citizens, provided critical information that assisted in the investigation and the subsequent arrest of Aldawsari.

---

49 As outlined in the ISE-SAR Functional Standard 1.5, the acquisition of unusual quantities of chemicals is one of the behaviors reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

3.9.5 Critical Infrastructure Information Sharing

The CIKR ISE, developed and operated by DHS IP, supports the critical infrastructure protection and resilience homeland security mission. It is making substantial progress in providing useful critical infrastructure protection and resilience content to an increasing number of Critical Infrastructure Sector partners to identify their risks, reduce their vulnerabilities, and respond to and recover from incidents. It has also demonstrated that it successfully supports two-way information sharing across agencies, between all levels of government, and between public and private sectors.

The CIKR ISE includes Sensitive But Unclassified/Controlled Unclassified Information (SBU/CUI) and classified information. It delivers more than 12,000 SBU/CUI or unclassified products, reaching more than 30,000 federal and SLTTPS partners. The CIKR ISE also provides the private sector entry into the NSI via the SAR Tool for Critical Infrastructure, and is a mechanism for fusion centers to share regional infrastructure protection information directly with their private-sector partners via the Homeland Security Information Network–Critical Sectors (HSIN-CS) platform. IP also operates the Private Sector Clearance Program, which has granted more than 1,300 national security clearances for CIKR owners and operators of nationally critical assets in order to receive classified physical and cyber threat and vulnerability briefings as well as to provide subject matter expertise to the IC to develop useful actionable products at the unclassified level for broader distribution.

In addition to core information exchange, the CIKR ISE also serves as a comprehensive training, education, and collaboration tool. Accomplishments in critical infrastructure information sharing include a marked increased in the number of active users participating in the environment, increased availability and dissemination of actionable content, and the development and usage of relevant training, a form of information delivery in itself.

- The increase in new and active users registered on the CIKR ISE information-sharing platform HSIN-CS exemplifies its relevance for enabling decisions to protect and enhance the resilience of the nation's critical infrastructure. The number of active users grew by 67 percent over the last year. Currently, a new user registers every 1.5 hours.
- New content is made available on HSIN-CS at a rate of every 2.5 hours. As of the end of the 2nd quarter of FY 2011, 12,250 documents were available, representing a 100 percent increase over the same time last year.
- During the Deepwater Horizon Oil Spill, the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produced and posted 31 products to HSIN-CS and the Homeland Security Information Network-Emergency Management (HSIN-EM) to facilitate information-sharing across the broad spectrum of response operations.
- TRIPwire Community Gateway (TWCG), part of HSIN-CS, is designed to provide improvised explosive device (IED) awareness information specifically for the nation's critical infrastructure owners, operators, and private security personnel. TWCG provides expert threat analyses, reports, and relevant planning documents to help key private-sector partners anticipate, identify, and prevent IED incidents. Over the past year, the number of registered users increased by 63 percent.
- HSIN Connect was utilized over the past year to host more than 28 educational events for approximately 17,500 critical infrastructure stakeholders. Briefing topics include CIKR resilience, threat detection, protective actions, best practices, and specific methodologies or CIKR tool training.

The foundation for the development and sustainment of the CIKR ISE is the National Infrastructure Protection Plan (NIPP) Sector Partnership, under the Critical Infrastructure Partnership Advisory Committee (CIPAC) framework. It consists of more than 700 active private sector and government leaders from every critical sector and from relevant government agencies at all levels, who develop the requirements, promulgate the processes, and execute the information sharing operations on a regular basis. They drive and deliver the CIKR ISE.

Most of the information that is shared day-to-day within the CIKR ISE consists of information necessary for the coordination and management of risks resulting from natural hazards and accidents. There is substantial overlap between how the CIKR sectors secure and build resiliency against natural disasters, accidents, and terrorist attacks. Natural disasters occur on a relatively predictable annual basis in the United States–hurricanes in the Southeast and on the East Coast, tornadoes in the Midwest, earthquakes and floods on the West Coast, snowstorms in the Northeast, and wildfires in the Southwest. Consequently, the foundation for sustainability for CIKR information sharing comes from leveraging the structures, processes, and mechanisms already in place. When there is a terrorist incident, the relationships will already be in place, and training for the use of tools, as well as familiarity and experience with executing the roles and responsibilities for operational coordination and information sharing will already be established.

Additionally, DHS, DoD, and the Financial Sector signed a memorandum of agreement in December 2009 initiating a pilot to address cyber threat information sharing. This pilot, which is ongoing, is based on lessons learned developed as a result of DoD's ongoing collaboration with approximately 35 companies in the voluntary Defense Industrial Base Cyber Security/Information Assurance program. This program is in the process of transitioning from a pilot to a program in 2011 and is opening up to all qualified cleared defense contractors through a rule in the Federal Register.

DHS Information Sharing Partnerships in the Field

The DHS investment in federal, state, local, tribal, public and private information sharing is much more than its investment in fusion centers alone. Fusion centers depend on and benefit from the expertise and information resources of tens of thousands of DHS component field personnel whose partnerships and collaboration venues turn information sharing into operational action nearly every day. Direct support to the fusion centers is one of many information sharing responsibilities of DHS components in the field. Here are just a few of the numerous examples of DHS information sharing partnerships in the field.

U.S. Customs & Border Protection (CBP)

CBP is developing an Operational Integration Center near Detroit which supports and improves information sharing, threat assessment, and joint response tactics between border security stakeholders in the Great Lakes region, so that CBP and its mission partners have a complete view of Northern Border security across their operating areas.

Immigration & Customs Enforcement (ICE)

Information sharing between fusion centers and the ICE Border Enforcement Security Task Force teams has increased the effectiveness of law enforcement operations, resulting in several major arrests and seizures within four ICE areas of operations. Also, through ICE's administration of the DHS Law Enforcement Information Sharing Initiative (LEISI), LEISI has engaged in extensive outreach to law enforcement partners within and external to DHS in an effort to promote law enforcement information sharing.

U.S. Secret Service (USSS)

The USSS leads a nationwide network of 31 Electronic Crimes Task Forces, bringing together federal, state and local law enforcement as well as prosecutors and representatives of private industry and academia. Their common purpose is to prevent, detect, mitigate, and aggressively investigate cyber-related crimes and cyber attacks on our nation's financial and critical infrastructures, with a primary focus on prevention. The USSS also makes the Targeted Violence Information Sharing System available to federal, state, and local law enforcement agencies with protective responsibilities to facilitate threat assessments.

U.S. Coast Guard (USCG)

USCG, as designated lead agency for the DHS Interagency Operations Centers program, is developing new information sharing procedures and capabilities to support federal, state, local, tribal, public and private partners in up to 35 U.S. critical ports. This program is improving joint targeting, prevention, and response collaboration with DHS and non-DHS partners in seven ports to date.

3.10 Foreign Partner Information Sharing

The United States and its foreign partners are committed to information sharing and cooperation in the prevention, investigation, and prosecution of terrorism-related offenses. Foreign partners are vital in the effort to combat terrorism by sharing key information, conducting surveillance, collaborating with U.S. overseas air passenger and maritime cargo screening, arresting members of terrorist cells, interdicting terrorist financing and logistics, and contributing to efforts in Afghanistan, Iraq, and other key places around the world.

3.10.1 International Information Sharing Pacts

In December 2010, the United States and the European Union (EU) began negotiating a new Passenger Name Record (PNR) agreement, to replace the 2007 pact that is temporarily in force. The United States is also in the process of negotiating an umbrella Data Privacy and Protection Agreement with the EU that will further facilitate the sharing of information. These negotiations began on 28 March 2011.[50]

The State Department, along with DHS and DOJ, also continues to work bilaterally on Preventing and Combating Serious Crime (PCSC) initiatives with countries that participate in the Visa Waiver Program. PCSC agreements, like HSPD-6—Integration and Use of Screening Information—are designed to increase border security and law enforcement cooperation between the U.S. government and its foreign partners, and also authorize the spontaneous sharing of information for the purpose of detecting and preventing terrorist and criminal activity. Under PCSC, each party agrees to provide the other with electronic access to their fingerprint databases.[51]

One of the notable projects that the US-VISIT program is involved in is the Five Country Conference High Value Data Sharing Protocol. This protocol allows for biometrically-based information sharing among the United States and the four other member countries: Australia, Canada, New Zealand, and the United Kingdom. Separate bilateral Memoranda of Understanding (MOUs) that facilitate the matching of immigration and nationality cases against each others' biometric databases, and the exchange of relevant information in cases where biometric matches are made, for the collective benefit of the participants, were developed between all of the partner countries. All participating countries are using this biometric-information exchange to aid in immigration decisions. There have been several cases where immigration or law enforcement officials of participating countries have received new case information and/or taken direct action as a result of this biometric information sharing.

In February 2011, President Obama and the Prime Minister of Canada released the Beyond the Border Declaration: A Shared Vision for Perimeter Security and Economic Competitiveness, which identified information sharing, particularly along the northern border, as a key priority between the United States and Canada.

The FBI has also expanded its operations and is viewed as a global organization for a global age. Besides its 56 field offices and almost 400 resident agencies in the United States, the FBI has more than 250 special agents and support professionals in more than 60 overseas offices, pursuing terrorist, intelligence, and criminal threats with international dimensions in every part of the world. The Legal Attaché Program and the strategic placement of FBI offices has enhanced information sharing with international law enforcement and intelligence agencies The FBI also takes part in all manner of global and regional crime-fighting initiatives, including with INTERPOL and Europol; the Budapest Project; and Resolution 6, which co-locates FBI agents in DEA offices worldwide to combat drugs.

---

50 Statement for the Record, Ambassador Daniel Benjamin, Coordinator For Counterterrorism, Counterterrorism Cooperation With Europe And Eurasia, House Foreign Affairs Committee, Subcommittee On Europe And Eurasia, 5 May 2011

51 Ibid.

Finally, in February 2011, President Obama and the Prime Minister of Canada released the *Beyond the Border Declaration: A Shared Vision for Perimeter Security and Economic Competitiveness*, which identified information sharing, particularly along the border, as a key priority between the United States and Canada. In response to the Declaration, the National Security Staff formed an interagency working group to prioritize initiatives and develop action plans for implementing the cross-border information sharing priorities outlined in the Declaration.[52]

3.10.2 Sharing Best Practices

A goal of the ISE's efforts for international information sharing is the sharing of ISE best practices. The ISE is currently developing an online knowledge base that describes important core concepts, approaches and best practices of the ISE, including governance, standards, policy, budget, performance management, privacy policies, and a process for suspicious activity reporting. The knowledge base will be available to international partners, including Canada, to assist them in developing and adopting similar models and applying ISE concepts to new environments. As this initiative is underway, Canada and Mexico have already reached out to their U.S. counterparts to inquire and learn about some of these concepts, such as utilizing NIEM and interoperability standards and solutions for inter-departmental and inter-jurisdictional information sharing with international allies. In addition, the United States, Canada and Mexico are considering several pilot programs using NIEM to demonstrate information sharing in the public health or law enforcement arenas. The ISE is supporting and encouraging these information exchanges through outreach with international partners and participation in internationally attended conferences.

3.10.3 Cross-Border Sharing Empowered by the National Information Exchange Model (NIEM)

Recognizing the value that NIEM could provide for facilitating information sharing within the Canadian government and along the border with the United States, the Canadian government has shown strong commitment to adopting NIEM in the public safety, law enforcement, defense, and disaster management domains.

Recognizing the value that NIEM could provide for facilitating information sharing within the Canadian and Mexican governments and along their borders with the United States, both Mexico and Canada have shown interest in adopting NIEM in the public safety, law enforcement, defense, and disaster management domains. The ISE is supporting and encouraging these information exchanges through outreach with international partners and participation in internationally-attended conferences and forums, such as North American Day.

Annually, the United States, Canada and Mexico participate in the North American Day conference, a meeting of national Chief Information Officers (CIO) and government

52 http://www.whitehouse.gov/the-press-office/2011/02/04/declaration-president-obama-and-prime-minister-harper-canada-beyond-bord

representatives. The purpose of North American Day is to exchange ideas and approaches for improving electronic government (e-government), including information sharing programs, interoperability, standards, investments, and partnerships between the private and public sector, among others. One of the outcomes from North American Day 2010 included a commitment from the three countries to conduct an international information sharing pilot program using NIEM. Since then, portions of the Canadian government, particularly Public Safety Canada, in coordination with the NIEM PMO, have explored and initiated two NIEM proofs-of-concept with Canada's Royal Canadian Mounted Police and the Canadian Association of Chiefs of Police. In addition, Canada has launched a web presence through the NIEM website, *niem.ca,* for public use and consumption.

The next North American Day, scheduled for July 2011, will include a continued and renewed commitment to e-government and information sharing among the three countries. One of the goals of the meeting is to confirm a three-way, pilot project between the United States, Canada, and Mexico, using NIEM to demonstrate information sharing in the public health or law enforcement arenas. The meeting is planning to conclude with the signing of an MOU, formalizing the commitment of the three countries to international information sharing, which has been agreed to in principle.

Canada's Chief Information Office is also working to develop common interoperability standards and solutions for inter-departmental and inter-jurisdictional information sharing. To address this challenge, Canada is standing up an Interoperability Centre of Excellence that is investigating interoperability frameworks that are likely to be instrumental in forming an interoperability solution for the Government of Canada, which includes the solutions and ideas currently underway with U.S. NIEM and ISE efforts. PM-ISE and the ISE (particularly the NIEM PMO) have been supporting this effort by providing information on the current NIEM-ISE architecture, best practices, and lessons learned from the ISE's interoperability efforts.

3.11 Law Enforcement Information Sharing

Because of the threat of terrorism within our homeland, state, local, and tribal law enforcement agencies have adopted an "all crimes, all threats, all hazards" business model to protecting life and property within their jurisdictions. Coupled with an arsenal of law enforcement information sharing systems, police officers today are better able to identify threats. While the focus of the ISE is terrorism-related information, public safety information sharing techniques and tools are not bifurcated between terrorism and law enforcement. For a trooper patrolling America's highways, his or her next stop might be a potential terrorist.

3.11.1 Criminal Justice Information Services (CJIS)

The FBI's CJIS is the focal point for some of the most important and relevant criminal history databases used by law enforcement including: wanted persons, stolen property, stolen vehicles, the national sex offender database, and the national domestic violence database, as well as databases for offenders who may not legally purchase firearms. The nationwide reach and application of CJIS proves that information can be shared and accessed securely on a large scale and ensures that an officer can discover if a suspect in rural Texas presents a danger to his safety, even if the criminal history was documented in urban California.

National Data Exchange System (N-Dex)

FBI's National Data Exchange System (N-DEx) is a criminal justice information sharing system that provides nationwide connectivity to disparate local, state, tribal, and federal systems for the exchange of information. Through N-DEx, law enforcement officers have the ability to search, link, analyze, and share investigative information (e.g., incident and case reports), but the data that is shared through N-DEx remains with the law enforcement agency that provided it. In March 2011, the final increment of the N-DEx system was delivered, increasing its power, speed, and accessibility while greatly improving the user's information-sharing experience. As of April 2011, the N-DEx system had approximately 8,000 registered users and approximately 100 million records contributed by 26 local, state, regional, and federal information sharing systems, consisting of the FBI and more than 3,600 other agencies.

N-DEx in Action

A Hood River County detective in Oregon investigating a homicide developed a list of persons of interest living outside the state using N-DEx. The detective found that one of the subjects of the investigation had contacts in California, and two of the records provided a telephone number in the Los Angeles area. The Oregon detective contacted the Los Angeles Sheriff's Department, which provided vital information on the subject. As a result, the detective located the suspect in Los Angeles, and the Sheriff's Department arrested the suspect. After the detective interviewed the suspect in Los Angeles, the suspect was then extradited to Oregon and is currently awaiting trial.

A Colorado state trooper was assigned to assist in an organized crime case initiated by a local law enforcement agency. During the investigation, a person of interest was identified, but a current address and other valuable information could not be found in accessible databases. Through N-DEx however, the trooper discovered prior charges against the subject in a closed federal drug case in another state; additional drug-related cases in California; and learned that the subject was a known Armenian Power Gang member. This investigation uncovered the Armenian Power Gang's presence in Colorado. Colorado is now preparing awareness reports to notify law enforcement and is working on adding this gang to the state's database.

3.11.2 eGuardian Adopted by DoD

In 2010, the FBI's eGuardian system was selected by DoD to replace its previous threat reporting structure, which was terminated in 2007. After two years of analysis, review of more than 60 systems, and the culmination of a six-month pilot program in June 2010, DoD selected eGuardian.

The eGuardian system was developed by the FBI's Counterterrorism Division in response to mandates by IRTPA, other statutes and Executive Orders, and the National Strategy for Combating Terrorism. eGuardian is a complete, web-based reporting system where federal, state, local, and tribal law

enforcement officers, state fusion centers, regional intelligence centers, and FBI task force officers can share timely information about suspicious activity and terrorist threats. This system gives law enforcement and IC partners a greater degree of connectivity with regard to the collection and dissemination of suspicious activity and threat reporting.

By sharing such information in a near real-time system, partners can avoid jurisdictional and bureaucratic impediments that may delay communication between agencies. All partner organizations are able to contribute to and extract information from eGuardian according to their needs and can keep their reports continually updated.

In the wake of the tragic Fort Hood shootings in November 2009, a DoD board reviewing the incident cited the need to "adopt a common force protection threat reporting system for documenting, storing, and exchanging threat information related to DoD personnel, facilities, and forces in transit."[53] The answer to this need for the DoD was the FBI's eGuardian system.

3.11.3 Technical Resource for Incident Prevention (TRIPwire)

TRIPWire is DHS's 24/7 online, collaborative, information-sharing network for bomb squad, law enforcement, and other emergency services personnel to learn about current terrorist IED tactics, techniques, and procedures, including design and emplacement considerations. Developed and maintained by the Office for Bombing Prevention within DHS IP, the system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to assist law enforcement in anticipating, identifying, and preventing IED incidents. Over the past year, the number of registered users has increased by 88 percent.

3.11.4 Next Generation Identification System (NGI)

The NGI program will incrementally replace the FBI's CJIS Division's existing Integrated Automated Fingerprint Identification System, in service since July 1999. The NGI improves, expands, and creates new biometric services, providing identification, criminal history, and investigative information to more than 18,000 law enforcement agencies, multiple federal partners, and authorized screening/ employment agencies. On 25 February 2011, the FBI achieved Initial Operating Capability for its NGI System, with the deployment of the Advanced Fingerprint Identification Technology (AFIT). The AFIT provides the foundation on which the rest of the NGI services will reside and provides new advanced matching algorithms, elevating the systems current accuracy to greater than 99 percent. Due to the improved NGI AFIT accuracy, 910 additional candidates were identified during the first five days of service, quickly validating the anticipated superior AFIT performance. One noteworthy success resulting from this new technology emerged with a civil applicant fingerprint background check submission. The FBI received a submission for a person who was applying to provide housing for foster care and child placement. The NGI's AFIT led to the identification of a subject with prior violent criminal charges, including armed robbery.

53 Protecting the Force: Lessons from Fort Hood, Report of the DoD Independent Review, January 2010

Another example of how the new services delivered by the NGI can benefit specific organizations and individuals is through the Repository for Individuals of Special Concern (RISC) Pilot project. The RISC Pilot allows officers on the street to use a mobile ID device to rapidly search a national repository of 1.2 million fingerprint records of "the worst of the worst" to quickly assess the threat level of any subject encountered during their normal law enforcement activities, receiving a response within seconds. In this pilot, Ohio, Florida, Maryland, Georgia, and Texas law enforcement agencies, using mobile ID devices, employ the CJIS Wide Area Network to securely transmit "live" fingerprints from the field to the RISC for a rapid search. As of 13 June 2011, 76,791 total RISC live submissions have been received, resulting in 1,357 hits. This RISC Pilot functionality will be enhanced and will be available nationwide in September 2011. One example of success with the RISC Pilot occurred on 23 January 2011 in Ohio, in the early morning hours, when the West Chester Police Department encountered an individual who was stopped for a vehicle equipment violation. The subject was nervous and was unable to provide proper identification. Officers captured the individual's fingerprints on the mobile ID device and received a response from the state database as well as the FBI RISC. The responses confirmed the identity of the individual and provided information that the subject had warrants in Dearborn County, Indiana for felony drug charges.

3.11.5 United States Visitor and Immigration Status Indicator Technology (US-VISIT)

DHS's US-VISIT Program provides homeland security decision-makers with a consolidated source of biometric and biographic information on visitors and immigrants entering and exiting the United States or applying for immigration benefits. Although the vast majority of US-VISIT information is non-derogatory immigration information, US-VISIT's watchlist includes information about criminals, immigration violators, and known or suspected terrorists. US-VISIT helps federal, state, local, and international partners quickly and accurately identify individuals and assess whether these individuals pose a risk to homeland or national security.

US-VISIT and FBI Fingerprint Records Tie Suspected Serial Killer to Arrest Warrants

In August 2010, CBP officers at Atlanta's Hartsfield-Jackson International Airport arrested a man after fingerprint records confirmed there were outstanding warrants for his arrest in connection with a murder in Michigan. The interoperability between FBI and US-VISIT systems helped CBP obtain the information they needed in a timely fashion. The man, suspected of several murders and assaults in Michigan and Virginia, was arrested as he attempted to board a flight bound for Tel Aviv, Israel. CBP officers took the man into custody and turned him over to law enforcement authorities.

US-VISIT Assists Joint Terrorism Task Force by Identifying Counterfeit Document

In November 2010, US-VISIT assisted in a case to determine the true identity and overstay status of a Turkish man attempting to gain employment at a nuclear power plant. It was determined that the subject was using a false document under a false identity to prove his legal status to reside and work in the United States. The subject was subsequently arrested by local DHS law enforcement authorities as an "overstay" and placed into federal custody awaiting removal proceedings.

US-VISIT Helps CBP Identify Illegal Alien with Outstanding Homicide Warrant and Considered Armed and Dangerous

In August 2010, the Border Patrol in Yuma, Arizona apprehended a man who had entered the United States illegally. The subject's fingerprints were checked against the Automated Biometric Identification System and it was determined that he had two outstanding warrants, including one for homicide, and that he was considered armed and dangerous. He was taken into custody and faces charges in the 2004 stabbing death of his girlfriend in Oregon.

3.11.6 Law Enforcement Information Sharing Initiative (LEISI)

The DHS LEISI has engaged in numerous partnerships with law enforcement agencies in order to share and exchange law enforcement information. These bi-directional information sharing collaborations not only allow federal, state, local, and tribal agencies to access DHS law enforcement information, but they also afford DHS law enforcement officers access to critical law enforcement information held by their external law enforcement partners. This sharing of information is usually through access to computerized law enforcement information systems, and can sometimes be accessed from mobile devices. This quick access to law enforcement information can allow officers to make tactical adjustments in ongoing operations so as to increase the chances for a safe and successful operation.

- ICE agents in Arizona, using a Portable Digital Assistant (PDA), were able to access state and local law enforcement information through the Tucson Police Department's law enforcement information sharing system and were able to make last-minute changes in the direction of travel during the surveillance of Drug Trafficking Organization suspects. With updated address information obtained through the PDA, the agents were able to maintain surveillance of the suspects and achieve the goals of the surveillance. The information also provided a mug shot of one of the suspects who was previously unknown to agents. The newly identified suspect was found to be armed during the surveillance, and the identification of the suspect allowed other agents to be alerted.

In the past year, through its LEIS Service, the LEISI has established a direct connection to Nlets making DHS criminal and enforcement biographic data available to all law enforcement personnel connected to Nlets. The LEISI is also in the process of establishing LEIS Service connections to the FBI/CJIS N-DEx. LEISI is also a proponent of NIEM and is currently developing metrics to measure the success of DHS law enforcement information sharing.

The LEISI continues to engage international law enforcement agencies in developing partnerships that will aid in international law enforcement information sharing. These efforts have been through PCSC initiatives with Spain, Germany, and South Korea, and have also been through negotiations with the government of Canada. Currently, DHS law enforcement information is made available to the Royal Canadian Mounted Police through the Nlets. DHS LEISI is also negotiating an information sharing agreement with Canada that will allow a bi-directional exchange of law enforcement information between RCMP and DHS.

3.11.7 National Law Enforcement Telecommunications System (Nlets)

Nlets paved the way for information sharing by implementing Extensible Markup Language (XML) and off-the-shelf technologies and spearheading the effort to provide crucial information, like criminal histories, to the CBP in real time. Currently, Nlets is teaming with the DOJ to pursue the necessary security measures for enhanced law enforcement information sharing. Recently, the Nlets Program Management Office asked PM-ISE to assist in improving Nlets access for tribal law enforcement organizations. PM-ISE reached out to Indian Country, expanded their knowledge of Nlets benefits, and established the first ever connectivity pilot with four tribes in separate regions of the United States.

3.11.8 Domestic Highway Enforcement Initiative (DHE)

U.S. highway troopers are a critical line of defense against all crimes, all threats, and all hazards, including terrorism in the homeland. For example, in July 2001, a police officer stopped and ticketed Muhammad Atta in Florida. In September 2001, Atta crashed a plane into the North Tower of the World Trade Center. In August 2001, Hani Hanjour was pulled over for speeding in Arlington, Virginia. Hanjour piloted the plane that crashed into the Pentagon. On 9 September 2001, a Maryland trooper stopped Ziad Jarrah for speeding. Two days later, Jarrah piloted the plane that crashed in Shanksville, Pennsylvania.

The DHE initiative promotes collaborative, intelligence-led, unbiased policing in coordinated and mutually supportive multi-jurisdictional law enforcement efforts on the nation's highways. The DHE improves the investigative efforts of HIDTAs and has a significant impact on traffic safety, homeland security, and other criminal activity. The DHE operational model has contributed to numerous success stories regarding the disruption of significant criminal activity along U.S. highways. For example, in February 2011, a DHE-supported Iowa Highway Patrol trooper seized more than $49,000 during a routine traffic stop. Iowa Department of Narcotics Officers shared the information with their state fusion center, which passed along information to Minnesota authorities. Authorities in Minnesota seized another $25,000 from a second suspect at the Minneapolis Airport. Intelligence information on the original suspect revealed that he had recently shipped $40,000 in cash California. DHE-supported analysts and officers in Aptos, California, worked the case. They seized guns, processed marijuana and 1,400 marijuana plants in an indoor grow operation.

Information Sharing Improves Training and Enhances Interdiction

The Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA) has partnered with the Drug Enforcement Administration (DEA) and the ONDCP in support of its Drug Interdiction Assistance Program (DIAP). This multi-agency information sharing effort has directly contributed to the apprehension of suspects on the terrorism watchlist, illegal aliens, and multiple seizures of contraband and drugs. In 2010, seizures from commercial vehicles included 769,696 pounds of marijuana, 16,612 pounds of cocaine, 297 pounds of methamphetamine, 15 pounds of heroin, and $59.2 million dollars in illicit U.S. currency. Two recent examples include:

- In March 2011, an Alabama state trooper stopped a tractor trailer for a traffic violation. The trooper, remembering his FMCSA-DIAP criminal activity indicators training, decided to make inquires to various law enforcement systems and determined that the driver was a known smuggler and a wanted fugitive. Subsequently, the trooper discovered 1,403 pounds of marijuana mixed in with the trailer's cargo.
- Also in March 2011, an Iowa state trooper stopped a tractor trailer for a traffic violation. Based on his FMCSA-DIAP training, the trooper observed a number of visual threat and criminal indicators. The trooper obtained consent to search the vehicles which resulted in the discovery of $2.5 million dollars of illicit currency in the trailer's modified wall and refrigeration unit.

3.11.9 INTERPOL I-24/7

The U.S. National Central Bureau of INTERPOL (INTERPOL Washington) serves as the statutorily-designated U.S. representative to the International Criminal Police Organization (INTERPOL) on behalf of the Attorney General. Through INTERPOL Washington, local, state, federal, and tribal law enforcement authorities can communicate in near real-time with their counterparts in the 187 other member countries of INTERPOL, either individually or with multiple countries simultaneously, by means of an encrypted, Internet-based virtual private network (VPN) known as I-24/7. This highly secure system provides a full messaging capability and access to INTERPOL databases containing vital international investigative information on wanted and missing persons, terrorists, fingerprints, biometric information, stolen and lost travel documents, stolen motor vehicles, as well as stolen and recovered works of art and significant cultural artifacts. In addition, I-24/7 supports the exchange of international humanitarian assistance requests involving death notifications, threatened suicides, and health and welfare checks on U.S. citizens overseas, and foreign nationals in the U.S. INTERPOL Washington has established secure network partnerships with the Nlets, RISS, the FBI's Law Enforcement Online (LEO), DOJ, DHS, and a number of other government law enforcement agencies, to facilitate secure information exchange and to allow access to the INTERPOL database for investigative assistance.

By providing access to INTERPOL's worldwide police-to-police communications and criminal intelligence network, INTERPOL Washington significantly enhances international investigative support and cooperation between U.S. law enforcement agencies and their foreign counterparts–cooperation that is oftentimes critical in the apprehension of a fugitive or the recovery of an abducted child.

INTERPOL in Action

In January 2011, a foreign national arrived in the United States and proceeded to travel to his ex-wife's residence in Alabama, where he kidnapped his five-year-old daughter. The father and daughter left the United States for France, but had to travel through the Netherlands. INTERPOL Washington coordinated communications and information with U.S. Justice Department officials, the Alabama Police Department, INTERPOL The Hague and INTERPOL France. Based on this exchange of information, the offender was arrested upon arrival in the Netherlands. The child was taken into protective custody and reunited with the custodial parent within three days.

In February 2011 a Colorado Police Department contacted INTERPOL Washington advising that an offender wanted for a sexual assault with serious injury had fled the United States on a commercial flight with a destination of Libya. As the offender's travel was to take him through the United Kingdom (UK), INTERPOL Washington immediately contacted INTERPOL London. Upon arriving in the UK, the offender was denied entry and placed on a flight back to the United States. After landing in Chicago, the offender was immediately taken into custody on the Colorado warrant.

In all instances, INTERPOL Washington coordinates U.S. law enforcement action and response, ensuring that the exchange of information is consistent with U.S. interests and law, as well as INTERPOL policies, procedures, and regulations. Even for U.S. law enforcement agencies with a well-developed international criminal investigative presence, INTERPOL Washington's services are complementary–not competitive or duplicative–and are available 24/7/365.

Law Enforcement Integrated Information Architecture

In October 2010, ONDCP, the Joint Interagency Task Force South, DHS's Office of Counternarcotics Enforcement, and DHS I&A sponsored an Interdiction Committee initiative to apply technology in the fight against drugs. Titled the Law Enforcement Integrated Information Architecture, this program will develop an information sharing architecture to create advanced analytical awareness, resulting in more actionable law enforcement intelligence, ultimately resulting in increased interdictions. This effort, focusing on the Southwest Border initially, is undertaken in partnership with ONDCP, DHS, the Southwest Border Intelligence Integration Working Group, and the DEA.

3.12 Homeland Security Standing Information Needs

Documenting information needs is essential to the production of intelligence that is responsive to consumers, and is key to enabling effective information sharing. In 2010, DHS reorganized its Homeland Security Standing Information Needs (HSEC SINs) into10 topics that align with the information needs of other IC and HSEC Community of Interest (COI)[54] members. This alignment enhances the ability of federal, state, local and tribal partners to collaborate during every step of the intelligence cycle.

For example, HSEC COI partners have been asked to tag raw information reports and finished intelligence products with relevant HSEC SINs. The practice of tagging items using common categories enables partners throughout the HSEC COI to more effectively share information and intelligence with target audiences, ensuring that homeland security stakeholders are receiving what they have identified as important and relevant to their operations. DHS continues to work with state, local and tribal partners, through the fusion centers, to develop SINs that are relevant to each fusion center's area of responsibility. Documenting SINs provides fusion centers with a baseline to guide their information collection activities and it further enables fusion centers to effectively communicate their information needs with the broader HSEC COI.

In November 2010, DHS launched a SINs development initiative for the private sector. This initiative included actively engaging interagency governmental partners, as well as owners and operators from the 18 CIKR sectors, in the information needs identification process. The effort began with a pilot between DHS and the Oil and Natural Gas sector owners/operators, private-sector analysts, key trade association representatives, sector leadership, and analysts from the Department of Energy (DOE), DOT, and Transportation Security Administration (TSA). The pilot brought together interested government sector and intelligence personnel with private-sector personnel to educate each another about their respective missions, roles, and business processes. These sessions ended with a facilitated discussion of the sector's specific information needs.

The SINs identified by each CIKR sector will be integrated by DHS into the overarching HSEC SINs, and will enhance the ability of homeland security and IC partners to effectively collaborate with the private sector during every step of the intelligence cycle. Over the next year, DHS will continue to employ this new process for working with the other CIKR sectors to identify and address their information needs.

54 Homeland Security Community of Interest (HSEC COI) is defined as DHS and its federal, state, local, tribal, territorial, and private sector stakeholders and homeland security partners.

Building Beyond the Foundation

The ISE is building beyond the foundation set over the last several years and is making critical improvements in responsible information sharing. The foundation of the ISE was built through strategic coordination and mission partner investment. The 2007 National Strategy for Information Sharing provided specific goals, guidance, and performance assessment criteria by which progress is measured. As the ISE moves into the next phase of implementation, PM-ISE is focusing its attention on new priorities, while ISE mission partners continue to sustain and grow existing capabilities. The PM-ISE is refreshing the National Strategy for Information Sharing to bring a new performance framework, with identified goals, objectives, and metrics for monitoring progress, into action.

Governance has emerging as a critical enabler and guiding force for accelerating the implementation of the ISE and coordinating efforts among multiple agencies at all levels of government and with the private sector. The Information Sharing and Access Interagency Policy Committee (ISA IPC) and its subordinate Sub-Committees and Working Groups are at the forefront of achieving effective interagency governance, coordinated implementation, and results measurement. Sub-Committees and Working Groups, which are chaired by senior representatives from throughout the ISE, are achieving consensus on how to develop a unified ISE and are realizing whole of government results for new and improved sharing and protection capabilities for all ISE partners. The ISA-IPC has reached a strong operating state, with a quarterly battle rhythm that drives progress toward the ISE goals.

The National Security Staff and the Office of Management and Budget issue annual ISE programmatic and implementation guidance that leads to cohesion and focus across the ISE. This and other Federal Government-wide guidelines, rules, procedures and functional standards are creating further momentum to enable the ISE to be an effective and efficient environment to responsibly share critical national and homeland security information. In addition to this top-down governance construct, communities of interest have formed around many key information challenges and these communities are accelerating progress and implementation of the ISE.

An ISE roadmap, with important components such as standards adoption, industry engagement, and strategic sourcing, will help steer the ISE in the right direction. Shared functional capabilities like identity management, information security, and auditing are necessary to provide a secure and functional technical space for information sharing. Further, continuing to develop human capital through enhancing training, conducting exercises, and replicating best practices remains a critical success factor for all ISE mission partners.

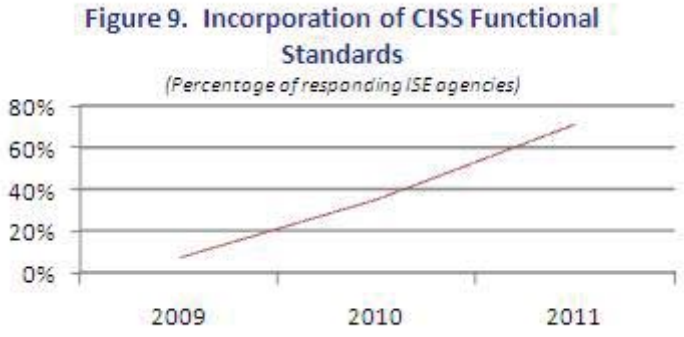
Increased interaction with all stakeholders, including industry and standards development organizations, is enabling standards-based procurement, strategic sourcing, and a deep collaboration that benefits all participants of the ISE. Ensuring that all mission partners are synchronizing efforts will ensure that the ISE continues to grow efficiently, and to enable analysts, investigators, and operators to prevent terrorist attacks and promote homeland security.

4 Establishing Standards for Responsible Information Sharing and Protection

The PM-ISE is working with mission partners and standards organizations to identify the best existing standards for reuse and implementation across the ISE. Following the Office of Management and Budget (OMB) direction on voluntary consensus standards in Circular No. A-119, the PM-ISE is leveraging and influencing industry standards to help make information transfer simpler and more predictable. Engagement with industry to build products based on standards both improves "off-the-shelf" interoperability of commercial solutions and ensures availability of technical solutions in shorter timeframes and at a lower incremental cost overall to mission partners.

4.1 Advancing Existing Standards for Information Sharing and Protection

To build the foundation of the ISE, the Common Information Sharing Standards (CISS) Program, was created to develop functional and technical standards to enable broader federal, state, local, tribal, and private sector access to, as well as the distribution and sharing of information. Functional standards set forth the rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas. There has been a steady increase in the number of departments and agencies that are incorporating functional standards into the management and implementation of ISE-related mission business processes; over the past year there has been a 36% increase to a total of 10 out of 14 departments and agencies (See Figure 9.)



The ISE Functional Standard for Suspicious Activity Reporting (ISE-SAR) is an excellent example of a functional standard now advanced by mission partner-specific efforts via the Nationwide Suspicious Activity Reporting Initiative (NSI). The ISE-SAR functional standard allows present and new participants in the NSI to use common terminology, data elements, and formats and also provides the necessary definitions, and outlines the behaviors, so that a police department in New Jersey, for example, can easily understand the details of a suspicious activity occurring in Los Angeles. Sixty-four percent of the ISE department and agencies indicate that functional standards such as ISE-SAR are helping to improve CT processes, interfaces to other ISE partners, and the structure of data/information for sharing in the ISE; this is a 21% improvement over the last year.

Similar functional standards currently being developed and implemented include:

- The NIEM AMBER Alert Specification, which improves the sharing of Amber Alerts between jurisdictions and across multiple communications networks and technologies.
- The Standard NIEM Prescription Monitoring Program Information Exchange, which assists law enforcement, health agencies, and prescribers in identifying potential abuse and diversion.
- NIEM-enabled Cyber Incident Information Sharing, which will bring cyber security specialists from around the world together to respond to cyber incidents as a collective force, to minimize loss and disruption.

CISS technical standards document the specific technical methodologies and practices used to design and implement information sharing capabilities into ISE systems. Many technical standards development efforts have evolved out of the growing needs of the Internet community, and are managed by industry consortia, often referred to as Standards Development Organizations (SDOs). These SDOs develop standards using robust methodologies and tools which are designed to simplify and unify the way in which applications communicate, interact and interface in order to handle their information exchange needs. At present, seven out of 14 responding ISE departments and agencies have incorporated CISS Technical Standards into their architectures, accounting for a 7% increase since 2010.

Technical standards also include a specific type of standard for securing information technology systems. Without commonly understood definitions for security controls and how they are implemented and maintained at the application, network, and enterprise levels, either costly retesting of security controls must be performed prior to interconnecting systems so they can share information, or significantly higher levels of risk must be accepted. In the federal space, several organizations have the authority, pursuant to the Federal Information Security Act of 2002 (FISMA; 44 USC §3541), to promulgate security standards, including: the National Institute for Standards and Technology (NIST) (the Special Publications 800 Series); the Intelligence Community (IC); the Department of Defense (DoD); and the Committee on National Security Systems (CNSS). This year the ISE has significantly increased coordination with these groups in order to adopt or establish common security standards. Increased standardization also enables industry partners to “bake in” common security controls in their products and services, thereby improving the overall security of such products and supporting downstream assured information sharing.

4.2 Coordination of Standards to Enable Interoperable Capabilities

Standards are critical enabling capabilities as they allow the ISE to deliver the decentralized, distributed, coordinated, and interoperable capabilities described in IRTPA. The way in which standards are identified, developed, adopted, and implemented requires significant cooperation and shared vision among interagency groups utilizing a rigorous governance structure that incorporates the values, expertise, and priorities of relevant partners.

Registry of USG Recommended Biometric Standards

The Registry of USG Recommended Biometric Standards (Registry), which was updated in February 2011, supplements the National Science and Technology Council (NSTC) Policy for Enabling the Development, Adoption and Use of Biometric Standards. This Registry lists recommended biometric standards for U.S. Government-wide use. It is based upon interagency consensus on biometric standards required to enable the interoperability of various federal biometric applications, and to guide federal agencies as they develop and implement related biometric programs. The NSTC Subcommittee on Biometrics & Identity Management will continuously review the content of this document, and release updated versions as required to assist agencies in the implementation and reinforcement process of biometric standards to meet agency-specific mission needs.

4.2.1 Standards Governance

Recognizing the critical role of standards in enabling the ISE and mission partner operations, in May 2011 the ISA IPC approved the creation of a Standards Working Group to coordinate efforts across departments, agencies, and levels of government. The Standards Working Group, which replaces interagency efforts previously under the Common Information Sharing Standards (CISS) Program, is developing a work plan focusing on standards and implementation profiles that should be coordinated and developed to ensure agreement, reduce duplication of effort, and influence existing standards efforts across the whole of government. The purpose of the interagency effort is to facilitate cross-domain, enterprise-wide interoperability and information sharing through standards. The initial goal of the group is to clearly define a process by which a standard is taken from need recognition to solution implementation, whether by adopting an existing standard, harmonizing or modifying a standard, or leading the creation of a new standard. To enable the government-wide approach, the Standards Working Group is also developing a shared lexicon, or term dictionary, wherein languages across many standards groups and domains can be aligned to prevent fragmentation or communication gaps. Another key to making standards work, is making them accessible, thus the working group is aiming to adopt a central repository so that government consumers will have a single location to locate and explore the available resources.

4.2.2 Industry Engagement

In 2011, PM-ISE joined both the Object Management Group (OMG) and the Organization for the Advancement of Structured Information Standards (OASIS). PM-ISE's aim in joining these organizations is to bring federal, state, local, and tribal government partners together to leverage existing work on specifying government standards and to harmonize those standards. Additionally, PM-ISE aims to work with OMG and OASIS to institutionalize those efforts as standards that industry can incorporate into their products and services.

In addition to engaging industry, PM-ISE is currently working with its ISE mission partners on a strategic sourcing approach based on industry standards and implementation profiles. Strategic approaches like

these will allow mission partners to procure products that are interoperable, cost-effective, and policy and standards-compliant. Mission partners can communicate these ISE-based requirements to industry in their requests for proposals (RFP) and realize targeted solutions which deliver the ISE. Industry reacts to customer demand (via RFPs, procurements, acquisitions) and this sourcing approach will encourage industry to create standards-based interoperable solutions for the ISE.

4.3 The National Information Exchange Model (NIEM)

NIEM is a "community-built" initiative that was born as a best practice developed by a handful of state and local practitioners. NIEM connects communities of people who share a common need to exchange information to advance their missions. The NIEM community is now a large partnership between federal agencies, state governments, the private sector and several international countries. NIEM is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. NIEM has become a well-tested and mature repeatable, reusable process for developing information exchange requirements that improves efficiency, saves time, reduces costs, and advances and fulfills organizational missions

Since its inception in 2005, NIEM has focused on data: understanding it, ensuring that it is discoverable, and standardizing it so that the data moves easily across departments and agencies. NIEM provides a commonly understood way to connect data to improve government decision-making for the greater good. This program has seen substantial mission area growth in the last several years, extending well beyond its original justice and homeland security roots. For example, this year saw the U.S. Department of Health and Human Services (HHS) joining the Federal Government's NIEM Steering Group with HHS's commitment to adopt NIEM into the health records data standardization process. NIEM has played a critical role in establishing a common vocabulary that has significantly enabled development of information exchanges, such as the SAR Information Exchange Package Documentation (IEPD), which defines the terms that would comprise a SAR anywhere a SAR is used if generated by participating partners at the federal, state, or local level, or by private-sector partners. These exchanges represent formal, machine executable models that ensure universal meaning even if the exchanging parties have no direct relationship with each other and do different jobs in different locations or agencies.

4.3.1 Advancing Use of NIEM Across All Levels of Government

NIEM creates a standardized way of doing business and as such, is a core process and framework for the ISE. In FY 2010, OMB provided guidance to all federal agencies to evaluate the adoption and use of NIEM as the basis for developing reference information exchanges. The initial results of the evaluation were very positive. To date, 12 federal agencies have committed to using NIEM. NIEM is also gaining significant adoption as a common framework for information sharing for a number of states, as well as local and tribal agencies. Seven more federal agencies and some international partners are evaluating the potential to use NIEM for their missions. Agencies that are not already using NIEM are required to exchange information with those that are, which will drive further adoption.

In April 2011, the Federal CIO Council released the NIEM adoption and use report. This Report indicates that:

- NIEM is gaining significant adoption as a common framework for information sharing. NIEM architecture allows the flexibility for different domains and agencies to leverage the common infrastructure and architecture offered by NIEM, while allowing them to maintain the information exchange requirements for their domains. This flexibility is a key contributing component for NIEM success and adoption.
- A growing number of federal, state, local, tribal and international mission partners are adopting NIEM for their information sharing needs
- Twelve federal agencies have committed to using NIEM. Seven more federal agencies and some international partners are evaluating the potential to use NIEM for their missions
- Recent additions to NIEM domains include Cyber security, Federal Health and Human Services, Youth and Family Services, and Agriculture

4.3.2 Advancing NIEM and UML Tools

To foster the evolution of the NIEM toolkit, the NIEM Program Management Office (PMO) and the PM-ISE, with support from SEARCH (the National Consortium for Justice Information and Statistics), are partnering with OMG to develop a Unified Modeling Language (UML) Profile for NIEM IEPD. A Request for Proposal (RFP) for developing this UML Profile was submitted to OMG by the Government Domain Task Force for consideration during the June 2011 OMG Technical Meetings in Salt Lake City. The RFP received a very strong response and OMG approved the issuance of the RFP to their community of U.S.-based and international government and private-sector industry membership. The next steps include submission and development of the UML profile, followed by the development of at least one commercial or open source product that will use the new NIEM UML profile.

The goal of this effort is that the standard, which mixes the best of NIEM with that of the UML standard is adopted by industry. Then government will be able to purchase commercial products with standardized information sharing “baked-in” from the start.

Advancing Industry Standards

In May 2011, PM-ISE engaged a multi-partner effort with the NIEM PMO and members of the OMG, a consortium of both industry and government members, to develop a UML profile for NIEM that will further NIEM success and adoption. This UML profile will be an industry standard that will enable NIEM developers to graphically develop models of information sharing across systems, agencies, and levels of government. NIEM’s success and adoption as a consensus standard has led to the recognition that we need better support and integration for NIEM in commercial products, enabling native support for NIEM throughout the Systems Development Life Cycle.

Recently, members of the NIEM community from outside the NIEM PMO—including both for-profit and non-profit organizations—have begun offering data standard development tools, signaling the maturity of NIEM and the formation of a robust market for like tools. The UML profile will specify a standard way of capturing IEPD content and structure in UML, the leading industry standard for modeling supported by dozens of tool vendors and open source projects. When the implementation profile is complete, and has been adopted as a standard by OMG, the NIEM UML Profile will be available for use in any number of UML tools available to the developer community today. NIEM support will be an extension of the existing tools and products, and IEPD developers will be able to use off-the-shelf UML tools to model exchanges and generate NIEM-conformant IEPDs from their models.

The resulting expansion of UML tools will encourage an ever-growing community of developers as they implement interoperable components for responsible information sharing across departments and agencies, across different levels of government, and between government and the private sector. All are welcome to join the efforts. The challenges and opportunities our modern world faces requires such interoperability, since they no longer exist in the domain of just one government department or jurisdiction.

4.4 Identity, Credential and Access Management (ICAM)

Responsible information sharing can occur when partners are able to share the identity of users requesting access to information in a form that is understandable to all partners. ICAM capabilities help with both tagging people in a form that can be recognized, and that can assist with the management of responsible information sharing across partners.

In November 2009, the Identity, Credential, and Access Management Subcommittee (ICAMSC) of the Information Security & Identity Management Committee (ISIMC) released the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Part A. This document provides common segment architecture and associated implementation guidance for use by federal agencies as they continue to invest in FICAM programs. The FICAM segment architecture will serve as an important tool for providing awareness to external mission partners and will drive the development and implementation of interoperable solutions. Part B of the FICAM Roadmap is scheduled for release in August 2011 and will include detailed implementation guidance for departments and agencies.

4.4.1 Implementing Federated Identity Standards into the ISE's Interoperability Efforts

Throughout the last year, ISE partners have participated in various forums addressing ICAM. In order to synchronize efforts, the PM-ISE convened the leaders associated with the multiple logical access related management activities of the Federal Government in May 2011. All leaders agreed to a broad vision of enabling these different identity frameworks to ultimately become aligned across all mission partners to provide the critical foundation for authenticating and appropriately authorizing access to information and systems.

There are at least five ICAM frameworks in use by federal agencies:

- The Federal CIO Council's FICAM Roadmap[55] and Personal Identity Verification - Interoperable (PIV-I) guidance for unclassified networks;
- The DOJ's and DHS's Global Federated Identity and Privilege Management (GFIPM) standards for unclassified networks and non-federal partners;
- The FBI's Criminal Justice Information Services (CJIS) Division Federated Identification and Management Service (FIMS) for unclassified networks and non-federal partners;
- The Committee on National Security Systems (CNSS) Public Key Infrastructure (PKI) for National Security Systems; and
- The IC's Identity and Access Management (IdAM) effort across all IC networks at all security domains.

Each ICAM framework covers separate communities and separate security domains. The goal in bringing all frameworks together is to achieve interoperability from both a horizontal – spanning all mission partners across a single security domain – and a vertical – spanning across security domains – perspective. Horizontal and vertical ICAM interoperability will eventually support key assured information sharing capabilities such as federated cross domain searching and discoverability, and insider threat detection and prevention. In the near term, the focus is on first achieving horizontal ICAM alignment to support assured information sharing across all mission partners within a security domain. For example, FICAM, GFIPM, FIMS, and IC IdAM at the unclassified level will need to be interoperable to achieve simplified sign-on (SSO) capability for the Assured SBU Interoperability Initiative. Similarly for federal Secret networks, CNSS PKI, IC IdAM at the Secret level, and other existing PKI solutions deployed on Secret networks will need to be aligned to preserve and expand assured intra-network access to mission critical information.

When fully implemented, the ISE's efforts at promoting federated identity, in concert with FICAM, will close identified security gaps in the areas of user identification and authentication, access control, and logging and auditing. These efforts support the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. The transformation of these business processes is vital to the security of the United States.

55 http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

National Strategy for Trusted Identities in Cyberspace (NSTIC)

The National Strategy for Trusted Identities in Cyberspace (NSTIC) charts a course for the public and private sectors to collaborate on raising the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions. The NSTIC focuses on ways to establish and maintain trusted digital identities, which are critical for improving the security of online transactions. Online transactions are electronic communications among two or more parties, connected via networks, systems, and computers. Individuals, organizations, hardware, networks, and software are all participants in an online transaction; therefore, each of these may be identified, authenticated, and authorized. Technology and processes for identification (establishing unique digital identities) and authentication (verifying the identity of a user, process, or device) are at the forefront of this Strategy. In addition, the Strategy focuses on ways of providing trusted and validated attributes to enable organizations to make decisions about authorization (approving or giving consent for access benefits). Identification, authentication, and authorization provide the information and assurances necessary for the parties within a given transaction to trust each other. The strategy as laid out in the NSTIC is based upon the FICAM Roadmap and is foundational to satisfying the needs of the ISE to provide assured information sharing.

4.4.2 Advancing Attribute Governance and Backend Attribute Exchange (BAE)

A challenge for acceptance and usage of both the PIV and PIV-I credentials is how to make authentication decisions based on attributes of an individual user to allow access to information that is not held within the home organization- essentially, how can an organization verify the that an individual from an outside entity meets the required criteria to access their information. Attributes can be an affiliation with an organization, a role within that organization, specific training or certification, as well as information about the operating environment.

The BAE standard and service is intended to satisfy the enterprise-wide need to verify attributes: providing for the exchange of information between an Attribute Authority (i.e., the information's authoritative source) and a Relying Party (RP) to make access decisions. The RP requests specific attributes of the individual who is trying to obtain information. The Attribute Authority responds, returning requested information as appropriate. The RP uses the returned information as necessary to make authorization decisions.

In partnership, PM-ISE and U. S. General Services Administration (GSA) are leading the effort to develop a business case and life-cycle sustainment analysis which will fully develop the need for the BAE and outreach to stakeholders to gauge their level of involvement and document their commitment of support. This analysis will also include the development of attribute governance and a sustainability plan for the BAE.

4.5 Security, Auditing and Cross-Domain Frameworks

World events–starting with 9/11, continuing through the WikiLeaks disclosures, and most recently culminating in the take down of Osama bin Laden–have generated a number of questions related to the appropriate relationship between information security and information sharing. Information security and assurance helps partners manage connections between what data people are allowed to access and share, in a way that promotes responsible information sharing across partners.

Some world events have been characterized as evidence of the limits of safe information sharing, while others have been highlighted as positive examples. These questions and the continuing tension between sharing and protection illustrate the complexity of the situation mission partners collectively face in developing the ISE. This complexity cannot be simply described as an inverse relationship between sharing and protection; rather, it is a more nuanced relationship of appropriate calibration between sharing and protection aimed at effectively managing the risks associated with both.

In March 2011, ISE leaders from the State Department, DoD, the Office of the Director of National Intelligence (ODNI) and PM-ISE, testified before the Senate Homeland Security and Governmental Affairs Committee hearing, "Information Sharing in the Era of WikiLeaks: Balancing Collaboration and Security." As the WikiLeaks story evolved over the past year, many voiced concerns that information sharing would suffer a setback. This hearing presented an opportunity to discuss the root causes as well as our efforts to accelerate and strengthen both information sharing and information security.

IRTPA recognized the complex relationship between information sharing and protection in its description of the characteristics associated with the ISE. Half of the fifteen characteristics identified as crucial for the ISE include elements of information protection – a clear recognition that protection and sharing are indivisible aspects of the ISE. Assured and responsible information sharing continues to be the overarching goal of the ISE.

4.5.1 Securely Sharing Classified Information with State, Local, Tribal, and Private-Sector (SLTPS) Partners

The need to share actionable and relevant classified information with SLTPS partners in support of homeland security is evident. Equally evident is the need for a unified, consistent program for the application of standardized security procedures for security clearance management and the safeguarding of classified information across the executive branch and in support of classified information sharing efforts with our partners in the SLTPS communities.

In August 2010, the President issued Executive Order (EO) 13549 to all federal departments and agencies, establishing the Classified National Security Information Program designed to safeguard and govern access to classified national security information shared by the Federal Government with SLTPS entities.

In August 2010, the President released EO 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," designed to safeguard and govern access to classified national security information shared by the Federal Government with SLTPS entities.

This EO establishes a governance and oversight structure that will serve to ensure the uniform application of security standards within the executive branch and SLTPS communities while maintaining consistency with existing national policy and standards.[56] The EO also called for the establishment of the SLTPS Policy Advisory Committee (PAC) to discuss the program-related policy issues in dispute in order to facilitate their resolution. They will also recommend changes to policies and procedures that are designed to remove undue impediments to the sharing of information under the Program. The SLTPS PAC conducted its initial meeting on 11 January 2011.

The EO designated the Secretary of Homeland Security as the Executive Agent (EA) for the program. The Secretary subsequently assigned responsibility for the execution of the EO and the implementation, management, and oversight of the program to the DHS Office of the Chief Security Officer (OCSO). The OCSO is completing work with interagency and STLPS partners to develop the implementing directive that will establish a governance and oversight structure to instill and promote the uniform application of security standards within the executive branch and SLTPS communities consistent with existing policies and standards.

In the coming months, the EA, in collaboration with other federal agencies and the SLTPS PAC, will work to fully implement the requirements of the EO. Among the efforts that will be addressed are the development of systems that are able to document and track the final status of security clearances and to maintain security implementation profiles of SLT facilities that have access to classified information and the development of an SLTPS Security Awareness and Training for program.

4.5.2 Policy and Procedural Framework for Security Reciprocity

Security reciprocity is an important means for developing a consistent, transparent approach to security that minimizes administrative burdens and cost for all mission partners. Through harmonizing the standards and processes used for security clearances for personnel, facilities security, and information technology systems security, mission partners can better understand the security measures used by one another, make well-informed risk management decisions, and achieve predictable security outcomes. Consistency and transparency in turn generate the trust that enables mission partners to accept the security determinations of one another and to minimize the administrative burden of re-examining security measures taken by others.

Significant progress in the area of security reciprocity continued over the past year as evidenced by continued promulgation of harmonized National Institute for Standards and Technology (NIST)-Committee on National Security Systems (CNSS)-Intelligence Community Directive (ICD) standards. These improvements are laying the foundation for an assured information sharing ecosystem among federal departments and agencies; state, local and tribal mission partners; private-sector owners of critical infrastructure; and international partners. At present, 9 out of 14 ISE departments and agencies responding to the 2011 ISE Performance Assessment have documented policies and/or implementation

56 Executive Order (EO) 13526, “Classified National Security Information;” EO 12968, “Access to Classified Information;” EO 13467, “Reforming Processes Related to Suitability for Government, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information;” and EO 12829, as amended, “National Industrial Security Program.”

guidelines on IT security reciprocity, stating the conditions under which they will accept the security certification and/or accreditation of another organization.

Progress has also continued with regard to developing the policy and procedural framework for reciprocity for information systems security. Building on the key milestone achieved in 2009, the harmonization of security standards between national security and non-national systems security standards represented by the publication of the NIST Special Publication 800-53 Revision 3 and the CNSS Policy 1253 – NIST's Joint Task Force Transformation Initiative continued its groundbreaking work to publish a suite of jointly-coordinated security standards. The suite of five IT systems security standards, shown in Table 4, will form a de facto common security standards baseline for all federal information systems.

NIST Special Publication	Date	Title
SP-800-30	July 2002	Risk Management Guide for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)
SP 800-53 Rev. 3	August 2009	Recommended Security Controls for Federal Information Systems and Organizations (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)
SP 800-37 Rev. 1	February 2010	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)
SP 800-53 A Rev. 1	June 2010	Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans (http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf)
SP 800-39	March 2011	Managing Information Security Risk: Organization, Mission, and Information System View (http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf)

Table *4. Key Publications Supporting Reciprocity, by Date of Release*

Although individual organizations must tailor these standards to their specific operational environment, the harmonization among standards issued by NIST, DoD, and the IC lays a common foundation that will enable all federal agencies to reciprocally accept one another's security testing results. This alignment will in turn enable state, local, and tribal mission partners to meet a common set of security requirements for interconnecting with federal systems, and significantly reduce the time and cost associated with practicing assured information sharing. Alignment of IT systems security standards across all federal communities will also facilitate responsible information sharing capabilities that operate horizontally across networks and vertically across security domains.

NIST Leads Effort to Harmonize Security Standards

The National Institute of Standards and Technology (NIST), an agency under the Department of Commerce (DOC), continued to lead the interagency effort to harmonize security standards among federal civilian agencies, DoD, and the IC, and published two additional security standards in the past 12 months. These harmonized standards represent the beginning of a single coordinated federal baseline for information systems security that will enable security reciprocity among federal mission partners, and will also enable reciprocity to be extended to non-federal partners such as fusion centers.

NIST also created the program management office for the National Strategy for Trusted Identities in Cyberspace (NSTIC) in April 2011. This strategy, which is aligned with key existing federal identity management efforts, will provide an important framework to enable interoperable identity management solutions among federal and non-federal mission partners, including state, local, and tribal governments and private-sector partners.

4.5.3 Information Assurance and Auditing

Generating records of individual activities on networks and in handling information provides an important part of the overall function that is information assurance. When individual users understand that their actions are being monitored, they are more likely to be vigilant in avoiding mistakes; they are also more likely to think twice about committing acts of deliberate malfeasance. Audit data and the analysis of patterns of use also constitute the means of predicting and detecting security problems as they occur.

However, to be useful in its role in information assurance, audit data must be shared effectively both vertically and horizontally. To assemble a comprehensive picture of date use, audit data covering activities on different networks and systems must be shared among mission partners. But audit data must also be shared or aggregated vertically across security domains to achieve a complete picture of use. Consequently, audit data present a uniquely broad challenge for information sharing.

Through the use of common standards for capturing audit data, and interoperable processes for aggregating it across networks and security domains, the complete picture of use becomes an achievable goal. The ISE, and the tools it employs to enable assured information sharing, is the optimal ecosystem for supporting an effective audit function.

In the past year, the IC has made progress in harmonizing audit data and procedures. Recently promulgated IC standards implement uniform information security requirements and procedures concerning audit information in the IC information environment, and address the use of collected audit

data for insider threat detection. These standards enable the capture and analysis of user activities to protect sensitive information, promote interoperability and efficiency, support identification of threats, and promote effective information sharing. The IC's experience in audit functions presents an opportunity for leveraging best practices for other federal, state, and local networks to improve the overall assurance of the ISE.

4.5.4 Information Sharing Across Security Domains

Security reciprocity and the use of common security standards and implementation profiles also support key ISE capabilities such as federated searching and the aggregation of audit data. In the future, security reciprocity and common standards will support capabilities that span horizontally across different networks at the same classification level, as well as capabilities that operate vertically across security classification domains, where appropriate. The ability to provide capabilities that cross security domains is necessary for certain functions, such as auditing (as previously noted), and it enables significant efficiencies for users in functions such as federated searching.

For example, an authorized individual operating on a classified domain should be able to search across both classified networks and unclassified networks. Inversely an individual operating only an unclassified domain may not see the classified results of a search; nevertheless, the search and discovery processes can trigger a notification to authorized individuals at the classified domain regarding interest from the unclassified domain for information. In the future, such a notification may then trigger actions to make some form of the classified information available to the unclassified domain. By achieving cross-domain federated search and information discovery, the ISE empowers members to find information actively and to have timely, relevant, and accurate information to find them. In both cases, use of interoperable security standards, privacy standards, and identity standards are a necessary condition to enable cross-domain functions.

4.5.5 Guiding Departments and Agencies

As part of previous efforts to establish the ISE through structural standardization, an Enterprise Architecture Framework was released in 2008 and continues to be utilized by many agencies. Sharing information in an electronic world requires agreement on the structures, policies, processes, and protocols under which sharing takes place. This is especially important in a distributed, decentralized environment like the ISE, where sharing takes place across a vast array of information technology systems and networks. This framework provided specific guidance to ensure that information technology investments are driven by the need for interconnectedness, interoperability, and seamless information sharing and collaboration. Its concepts and principles have been incorporated into OMB's Federal Segment Architecture Methodology (FSAM) as a best practice and are being adopted by other government-wide information sharing initiatives, such as the Next Generation Aviation Transportation System, the Maritime Domain Awareness Initiative, and the Federal Health ISE.

Adherence to ISE concepts has proven beneficial to members of the ISE community, to include ISE's broad guidance and recommendations to departments and agencies resulting in:

- Seven of 14 responding ISE departments and agencies applying Enterprise Architecture transition plans at key decision points in the investment cycle;
- Eleven of 14 responding ISE departments and agencies mapping at least one IT investment to its information sharing segment architecture, a 14% increase from 2010;
- Eight of 14 responding ISE departments and agencies representing all major ISE IT investments in their enterprise transition plans, a 7% increase from 2010; and,
- Five of 14 responding ISE departments and agencies including at least one information sharing measurement indicator for FY 2010 in Section E Performance Information table (Table I.E.1) of their annual OMB Exhibit 300s for ISE investments.

As the ISE continues to develop and move forward, a roadmap will continue to accelerate the provision of guidance and recommendations to departments and agencies, to focusing on standards adoption, industry engagement, and strategic sourcing across all levels of government.

Information Sharing and Protection Challenges and Opportunities

As the WikiLeaks story emerged, concerns were voiced that information sharing would suffer a setback. The guidance throughout the Executive Branch has been consistent: we need to accelerate our information sharing in a responsible and secure way. While complex and challenging, the imperatives to share and protect are not in conflict. In fact, as our information protection measures mature, are accepted by more and more mission partners, and become more and more transparent – our trust of one another's practices and security controls will result in increased reciprocal acceptance of information systems certification and accreditation, Identity, Credential, and Access Management, and audit procedures. In this new trusted environment, information sharing is facilitated by the very protections put in place to prevent another WikiLeaks-type incident.

We do not yet enjoy the benefits of the trusted environment described above and the challenges highlighted by the WikiLeaks breach are complex and go to deeply rooted issues:

- Our legacy of agency-based, bi-lateral, and fragmented rather than common, consistent, transparent, and comprehensive solutions for trusted, assured information sharing and protection;
- Our inconsistent and uneven counterintelligence posture against the insider threat and related technical considerations;
- Our inclination to fix the surface-level problem, namely our focus on securing the specific classified network involved, while ignoring the fact that the challenge of sharing information in a secure manner applies to and spans all security domains.

A *whole of government approach* is necessary to effectively address these issues in a robust way. We cannot hope to build a truly trusted ISE without addressing the concerns and mitigating the risks of all ISE mission partners.

In addition, the ISE is mandated to address terrorism, homeland security, and weapons of mass destruction information regardless of classification. Fundamental policies and solutions must be framed to address all types of protected information, *classified and unclassified*, held by the Federal Government and by our state, local, and tribal partners, as our critical national and homeland security issues cut across security domains.

Finally, a strong and broadly applied *governance, strategy, and policy framework* is foundational to improving information sharing and protection. We can achieve the trusted environment that we want, but every entity that has an ISE equity must have a seat at the table and be incorporated into the strategic vision from the outset.

The ISE has, since its inception, focused on information sharing in a responsible and assured manner. The risk of future WikiLeaks-like incidents can be reduced; but, fixing these government-wide challenges is complex, difficult, and requires sustained commitment. To share and protect information effectively, we must work to find what the DNI has termed the "sweet spot" between these critical imperatives.

5 Enabling Assured Interoperability Across Networks

The Information Integration Sub-Committee (IISC) of the Information Sharing and Access Interagency Policy Committee (ISA IPC) coordinates high-priority interagency efforts to accelerate the delivery of the ISE, including interoperability among Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI) and Secret networks, identification of best practices in support of data aggregation[57] activities, and advancement of industry-based standards in support of all ISE activities, as discussed in Chapter 4. The IISC also ensures that both federal and non-federal partners (e.g., fusion centers, state and local law enforcement activities, and public safety endeavors) have appropriate input in guiding and implementing shared information integration capabilities, policies, and processes that satisfy their mission needs. The 2011 Annual Performance Assessment indicates there are opportunities for improving information integration across the interagency. For example, only five of 14 responding ISE departments and agencies have a plan for implementing interconnection capability for sharing terrorism and homeland security information across SBU/CUI networks.

The IISC accomplishes this mission through its Working Groups by coordinating functional and technical standards, interoperability, data methods, and other responsible information sharing efforts harmonizing governance, policy, and investments across agencies and departments. These efforts are further discussed in the sub-sections below.

5.1 Data Aggregation

The mission to disrupt terrorist acts before they occur is enabled by finding, sharing and collaborating on data that comes from trusted and reliable mission partners. Mission partners are continually producing and consuming data from a wide variety of sources. The goals of data aggregation in the ISE are achieved through an established governance process that enables mission partners to obtain the data, through shared ISE enterprise services, that is necessary to perform their missions while protecting the privacy of persons for whom no nexus to terrorism exists. Key to enabling the access and dissemination of aggregated data within the ISE will be the capability to authenticate users across the environment. Through positive user authentication, logging of data access, and auditing of data trails, the risks associated with the sharing of aggregated data are mitigated.

Under the joint leadership of Department of Homeland Security (DHS) and Office of the Director of National Intelligence (ODNI), the Data Aggregation Working Group (DAWG) was formally approved and chartered by the IISC to focus on capabilities that are entity (identity)-focused, and to employ automated data discovery, data characterization, data correlation, and disambiguation algorithms to

57 Data aggregation refers to the collection of processes, policies, procedures, and technologies that allows for the detection of relationships between people, places, things and characteristics, linking information across organizations and helping analysts to identify the connections between data that are not obviously related.

aggregate information from multiple domains into a mission-specific enterprise-level analytic service. The objectives of the DAWG are to:

1. Provide a forum for sharing best practices, developing enterprise solutions, reviewing architectures, and resolving interagency issues related to data aggregation.
2. Explore options and provide recommendations to the IISC for implementing data aggregation approaches as part of the broader ISE.
3. Provide a forum for linking National Security-related matters with federal information technology, information systems, and architectural guidance as they relate to the data aggregation.
4. Evaluate options and provide recommendations to the IISC for enabling cross security domain search, discovery, and retrieval in aggregated data sets.
5. Serve as a technical forum of federal-wide engagement for assessing and providing recommendations to the IISC on the optimization of data-related processes, standards, and architectures that lead to data aggregation capabilities in support of non-traditional screening for terrorism.
6. Remain in synchronization with the Privacy and Civil Liberties Sub-Committee of the ISA IPC so that technical, policy, standards, and privacy issues related to data aggregation are consistent across multiple security domains.

The mission of the ISE is to improve the management, discovery, fusing, sharing, delivery of, and collaboration around terrorism-related information to enhance national security and to help keep our people and our institutions safe. Under the joint leadership of DHS and ODNI, the Data Aggregation Working Group is identifying and characterizing systems and programs that aggregate ISE data.

The Working Group envisions the ISE as an enterprise and applies enterprise data management principles to precisely define, easily integrate, and effectively retrieve data for both internal applications and external communications and sharing. This approach supports a more flexible ISE with lower costs by leveraging partner systems and applications and data for re-use and re-purposing through aggregation.

Since its creation, the DAWG has completed a review of the U.S. Government oversight and governance structures that provide strategic policy, technical and mission guidance for terrorism-related data aggregation, data integration, and data management efforts. To complete its tasking from the IISC, the Working Group has created questionnaires and survey tools to:

- Develop an accurate inventory of programs that perform counterterrorism data aggregation across the U.S. Government. The goal of the inventory is to increase efficiencies by sharing best practices, lessons learned, and architectures for data aggregation programs with interagency partners;
- Increase information sharing by cataloging data sources (highly valued/consumed data) in a way that highlights technical and policy issues related to data sharing; and

- Identify best practices and architectures and make recommendations on moving forward and to set the standards by which next generation data aggregation systems are built across the U.S. Government.

As the DAWG identifies best practices and lessons learned, it is expected that mature technical solutions will be identified that can be shared across the ISE. The DAWG is collaborating with the Privacy and Civil Liberties sub-committee of the ISA IPC to identify legal and/or policy protection constraints over data discovery, access, ingestion, use, and retention for person-centric data. The group is also working with other joint agency teams and the working groups under the Watchlisting and Screening sub-committee of the ISA IPC to ensure that business processes and best practices can be leveraged.

Finally, as a complete picture of data aggregation efforts across the U.S. Government is completed, overlaps and/or gaps in analytic responsibilities and information sharing among the ISE agencies will be identified, and business practices that bridge or close the gaps in the counterterrorism (CT) mission will be proposed and implemented.

5.2 Assured Secret Network Interoperability

The ability to effectively and responsibly share classified information among federal and non-federal mission partners is a key capability needed to support the CT mission and overall homeland security. However, federal Secret networks were not built with information sharing capabilities in mind, and the cross-departmental governance structures to coordinate functions that would support assured sharing across all federal Secret networks–that is, to manage federal Secret networks as an enterprise–have not previously existed. This coordination is necessary to ensure that classified information can be shared consistently and predictably with the appropriate level of assurance – not only among federal departments and agencies, but also between the Federal Government and key mission partners, such as fusion centers.

In April 2010, PM-ISE completed a study of the current state of federal Secret network connectivity and accessibility by non-federal partners. The study identified the need for consistent processes for planning and coordinating implementation of assured information sharing capabilities across the Federal Secret Fabric, and the need for a cross-federal governance body in which to hold such discussions. Based on these recommendations, in 2010 the ISA IPC chartered the Assured Secret Network Interoperability Working Group (ASNI WG) to serve as a forum for federal agencies operating Secret networks to work together to develop enterprise governance for the Federal Secret Fabric, to resolve interoperability issues, and to support assured information sharing among federal Secret networks. A particular focus of the ASNI WG is to develop efficient and assured information sharing between Federal mission partners and fusion centers.

The goal of the ASNI WG is to coordinate and facilitate interoperability between Secret systems–through establishing effective governance and harmonizing standards, policy, and technology–in order to ensure effective and efficient enablement of national security missions. In doing so, the ASNI WG partners with other existing working groups and advises the ISA IPC on all issues that require, or would be most effectively addressed by, coordination across multiple departments and agencies related to the secure sharing of information through the interconnection of federal Secret-level computing environments. DHS currently chairs the ASNI WG.

Over the past nine months, the interagency ASNI WG has delivered a number of key incremental accomplishments towards increasing interoperability and information sharing among federal Secret networks and between federal Secret networks and fusion centers.

In 2011, the Assured Secret Network Interoperability Working Group partnered with the Fusion Center Sub-Committee of the ISA IPC to document, validate, and prioritize information requirements. This establishes the foundational requirements needed to inform the development of technical connectivity and access to sensitive information for fusion centers.

In 2010, the ASNI WG identified a requirement to better understand fusion center information needs in order to ensure an appropriate basis for coordinated network connectivity and access. A joint interagency team, representing a partnership between the Fusion Center Sub-Committee and the ASNI WG, conducted a study in the spring of 2011 that drew upon data gathered from existing fusion center reports as well as discussions with key analytic personnel. These information needs were aligned to the Homeland Security Standing Information Needs (HSEC SINs), further supporting the ability of federal, state, local and tribal partners to use a common lexicon as they engage in information sharing activities.

Documenting fusion center information needs will help in communicating these needs to federal mission partners and application owners and will inform the technical access and connectivity solutions that are being developed by the Federal Government in order to securely share information with fusion centers. The results of this study were also shared with the DAWG and the Assured SBU/CUI Interoperability Working Group.

The ASNI WG also supported demonstrated progress on mission capabilities on Secret networks for fusion centers, which were announced at the 2011 Fusion Center Conference. These capabilities included: improved access to white-listed sites on DoD's Secret network (SIPRNet) via DHS's Homeland Secure Data Network (HSDN); preserved and expanded fusion center access via HSDN to *NCTC CURRENT* during its relocation to SIPRNet; expanded Secret-level video-conferencing capabilities as a shared service between the FBI's Secret network and HSDN for fusion centers; and new access to the FBI's white pages and email directories through HSDN.

The ASNI WG also made progress toward several goals related to interoperability and governance of the Federal Secret Fabric. ASNI WG completed an initial study of DHS's authorities related to Secret network access provisioning and coordination for non-Title 10 and non-Title-50 organizations. The Working Group developed and began administering a survey to federal Secret networks to develop a body of information around network characteristics that impact information sharing. Finally, the Working Group began a study of the impacts on information sharing resulting from new security controls implemented after the WikiLeaks disclosures, raising awareness among the information sharing community of potential mission impacts.

Over the coming year, the ASNI WG will continue its work to improve coordinated classified connectivity and access, and to improve information sharing with fusion centers. It will also continue to develop governance among all Secret network stakeholders toward the overall goal of coordinating the Federal Secret Fabric to support assured information sharing. Key activities that will support this goal include completing work on developing a current picture of Secret network characteristics that support

information sharing; developing an end-state vision for protected sharing; and prioritizing gaps between the two, based on fusion center mission-based requirements for information and other use cases. The ASNI WG will also continue to strengthen linkages and to leverage activities between other coordination bodies related to Secret networks, such as the Committee on National Security Systems. Finally, the ANSI WG will monitor the impact of new WikiLeaks-related security measures on information sharing and will coordinate among member agencies to ensure that information security and information sharing on the Federal Secret Fabric increase in tandem.

Multi-Agency Collaboration Environment (MACE)

The Multi-Agency Collaboration Environment (MACE) develops interagency alliances of partners to demonstrate the power of data sharing within a common enterprise architecture. MACE and PM-ISE, in coordination with federal, state, local, and tribal entities, are sponsoring a pilot effort to demonstrate the value of interagency data sharing to disrupt the financial networks used to support threats to our national security, our economic interests, and our allies. Participating organizations will work together to facilitate information discovery, planning, and the execution of operations across departmental and agency boundaries. The impact of integrating architectures, data, and technology on operations, tactics, techniques, and procedures will also be analyzed. This pilot will act as a catalyst to accelerate the interoperability, policy, and security advancements needed to meet the challenges that will be encountered by our nation in the coming years.

5.3 Assured Sensitive But Unclassified (SBU) Network Interoperability

In the spring of 2010, PM-ISE conducted a user requirements survey with thousands of SBU system users. Those users identified that there are multiple SBU/CUI networks, portals, and systems currently in existence containing a rich variety of data and services that they regard as essential for doing their jobs. However, differences in policy and technology prevent authorized users from gaining access to many of those resources without having to individually log on to multiple systems using separate sets of credentials. System users stated that the ability to reduce the number of credentials needed to access SBU/CUI systems was their most desired requirement. Specifically, the overarching requirement is to provide federal, state, local and tribal law enforcement officers and analysts with the ability to log in just once to an approved system that would grant users access to an interoperable and protected SBU/CUI environment. Commonly referred to as Simplified Sign On (SSO) and branded by the SBU partnership as the “no wrong door” concept, achieving this capability has been identified by operators and analysts a top priority.

The SBU/CUI interoperability initiative has been in existence since 2007. To formalize this effort, the group was renamed the Assured SBU Network Interoperability Working Group, and it was brought under the Information Integration Sub-Committee of the ISA IPC. The Working Group (aka “SBU Partners”) is composed of representatives of four systems listed in Table 5. The goal of the Working Group is to coordinate and facilitate interoperability between SBU/CUI systems through efficient governance and establishment of standards. Reaching consensus on the standards and architecture

needed to achieve interoperability between these four key SBU/CUI systems will lead the way for interoperability between a broader set of SBU/CUI systems.

In February 2011, an ISA IPC meeting was held with senior interagency leaders to gather support to move quickly in addressing the SBU challenge. One recommendation was to have an SBU partner lead the SBU Working Group. Given the RISS program's long standing efforts to expand information sharing among federal, state, local, and tribal partners, it was decided that RISS would be the first partner to lead the group to ensure that the SBU effort continues its forward progress. PM-ISE will continue to support RISS in facilitating the agenda, objectives and meetings for the Working Group.

Law Enforcement Online (LEO)	Law Enforcement Online (LEO) is a state-of-the-art Internet system that is accredited and approved by the FBI's Criminal Justice Information Services (CJIS) for SBU/CUI information. LEO is used to support investigative operations, send notifications and alerts, and provide an avenue for remotely accessing other law enforcement and intelligence systems and resources. LEO provides all levels of the law enforcement, criminal justice, and public safety communities virtual private network access to its "anytime and anywhere" system for secure electronic communications, online training, and information sharing.
Intelink-U	Intelink-U and related services provide robust information sharing and collaboration capabilities for the IC and its national defense (U.S., allied, and coalition partners), homeland security, foreign relations, and law enforcement partners. The Intelink Enterprise Collaboration Center provides, in all three security domains, the operational means to deliver enabling services supporting the objectives of the National Intelligence Strategy. These community level services include: search, discovery, and delivery services (e.g., web-based content search, content indexing, personalized and group subscriptions, customer support); collaboration tools and services (e.g., email, chat, instant messaging, forums, wikis, blogs); web-based content and hosting in Community Shared Spaces; analytical support in the use Intelink resources; infrastructure services (e.g., mail relay, directory services , cross-domain platforms, public key infrastructure (PKI) certificates) and network management, monitoring and control. In the SBU/CUI realm Intelink services are accessible to more than two million users through existing interconnections and partnerships.
Homeland Security Information Network (HSIN)	HSIN, hosted by DHS, is a secure, web-based platform that enables SBU/CUI information sharing and collaboration capabilities among state, local, territorial, tribal, private sector, and international partners, and the Federal Government. HSIN supports several Communities of Interest in Law Enforcement, Intelligence, Emergency Management, Defense, and Critical Sectors.
Regional Information Sharing System Secure Intranet (RISSNET)	Regional Information Sharing Systems (RISS) is a nationwide information sharing and investigative support program that provides secure communications and investigative services to thousands of local, state, federal, and tribal law enforcement, criminal justice, and public safety agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, England, and New Zealand. RISS consists of six regional centers that serve the needs of their individual regions while working together on nationwide efforts. It offers diverse and unique services, facilitates rapid exchange of information, and provides secure, nationwide information and intelligence sharing capabilities through its secure Intranet, known as RISSNET. RISSNET has more than 60 partner agencies that leverage RISSNET through node connections to provide secure remote access to resources within their agencies.

Table 5. The Four SBU/CUI Partner Systems

5.3.1 Simplified Sign On (SSO)

Over the past year, the Assured SBU Network Interoperability Working Group has made significant progress towards achieving SSO. In December 2010, FBI's CJIS Trusted Broker Version Two became operational, providing SSO capabilities by allowing LEO users to access Intelink-U, RISSNET, and many other systems that are not yet part of the SBU partnership. In addition, the CJIS Trusted Broker allows RISSNET users to access the Joint Automated Booking System (JABS) and Intelink-U without having to obtain separate accounts. In March 2011, RISSNET achieved interoperability with the Pennsylvania Justice Network via the National Information Exchange Federation (NIEF) mechanism, enabling SSO for users of those two systems. Also, as a prerequisite for SSO, HSIN successfully tested Identity Provider (IP) and Service Provider (SP) capabilities, with RISSNET complying with the Global Federated Identity and Privilege Management (GFIPM) reference federation. In order to illustrate SSO capabilities and communicate these accomplishments to leadership and the SBU user base, the partnership produced a series of demonstration videos illustrating specific SSO use-cases. Over the next year, the partnership will continue to release additional videos that will demonstrate the services that are made available through the SBU/CUI effort.

PM-ISE hosted a Simplified Sign On (SSO) Technical Forum allowing SBU partners and experts to define the technical plan for federated SSO. Three SBU partners (Federal Bureau of Investigation's [FBI] Law Enforcement Online, RISS Secure Intranet [RISSNET], and Director of National Intelligence's [DNI] Intelink-U) have enabled simplified sign-on using the FBI's Criminal Justice Information Services' Trusted Broker.

5.3.2 Measuring SBU Progress

The Assured SBU Network Interoperability Working Group tracks the effectiveness of their efforts by monitoring a set of user metrics that are consistently collected from all partners on a monthly basis. These metrics have been designed by the SBU partnership to indicate progress towards the group's interoperability goals and to assist in fine-tuning particular interoperability efforts. Specifically, all partners report metrics on the total and external usage of their top services, such as web portals, document repositories, or instant messaging systems. External usage indicates user activity originating from one of the other three partners. Additionally, partners report the number of unique registered users each quarter (see Figure 11). This metrics collection effort has proven a valuable tool for fine-tuning SBU interoperability efforts and will continue to evolve as the SBU partnership adds additional participants in the future.

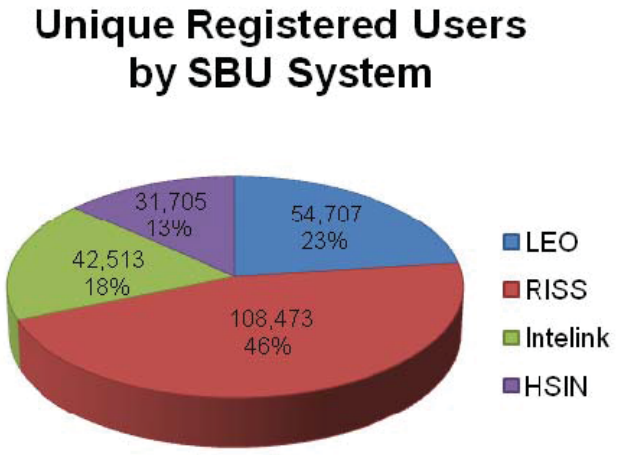


Figure 11. Unique Registered Users by SBU System

5.3.3 Future Plans

The SBU partnership has set goals for the coming fiscal year that are designed to further enhance interoperability among the partner systems. The group will continue to add IPs and SPs and to expand the user base that has access to an SSO capability. The group will also be focusing on other key capabilities, such as cross-partner federated search, discovery, and retrieval. In the 2010 SBU User Requirements Survey, the search capability was the second-most requested requirement, after SSO. The Working Group plans to demonstrate cross-partner federated search, discovery, and retrieval through a pilot before the end of fiscal year 2011. Finally, the SBU partnership intends to work to standardize system security practices to include user account vetting, user account de-provisioning, and system certification and accreditation reciprocity.

New HSIN COI Goes Operational on New Year's Eve in Times Square

Every year on New Year's Eve, approximately one million people gather in New York City's Times Square. Keeping them safe is the job of thousands of police officers, emergency service squads, drug and bomb-sniffing canine units, and counterterrorism personnel. As 2011 approached, New York's Mayor Bloomberg ordered the implementation of an information sharing program to connect the metropolis's 44 agencies, including six federal, 10 New York/New Jersey state, and 28 local agencies. In response, HSIN stood up the New York City Office of Emergency Management Community of Interest (COI) to connect the various citywide command posts of the New York City Office of Emergency Management and the Fire Department of New York. The COI went operational for the first time on New Year's Eve 2010, merging all the various emergency, law enforcement, and federal personnel, and feeding them up-to-the-minute information. It marked the first time an information sharing operation of this size and breadth has been conducted in the nation's largest metropolitan area.

HSIN Storms the Hill

The Legislative Branch Emergency Planners Group, composed of such elements as the United States House of Representatives, the United States Senate, the Capitol Police, the Architect of the Capitol, the Library of Congress, and many others, has adopted HSIN as their new command, control, and communications platform. They did so in order to increase situational awareness across three primary areas: exercises, general events (daily member movements) and special events (Presidential inaugurations, State dinners, State of the Union addresses, etc.). The site sponsor, the Office of the United States Senate Sergeant at Arms, was also interested in a centralized platform capable of coordinating information and manpower during emergencies such as the Capitol has faced in the past—gunmen on the grounds, anthrax mailings, etc. HSIN is now being used to compliment the emergency operations for 50 core users at the United States Capitol complex.

LEO Performance

- Approximately 54,700 active vetted users
- Approximately 41,700 unique users log in per quarter
- More than 960 Virtual Command Centers (VCC)
- More than 1,100 Special Interest Groups created
- An average of 28 new VCCs per user request activated monthly

5.3.4 Controlled Unclassified Information (CUI)

While interoperability between networks, systems, and data is critical to enabling information sharing among different partners, the imperative to achieve interoperability also applies to the rules by which information is marked. Historically, executive departments and agencies have employed ad-hoc, agency-specific policies, procedures, and markings to safeguard and control the dissemination of SBU information. As a result, there are more than 100 different policies and markings for handling such information across the Executive Branch. This inefficient, confusing patchwork system has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing.

On 4 November 2010, President Obama signed Executive Order (EO) 13556 "Controlled Unclassified Information,"[58] establishing a CUI program to manage all unclassified information that requires safeguarding and/or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. The Order identifies the National Archives and Records Administration (NARA) as the Executive Agent to implement the EO and to oversee department and agency actions to ensure compliance; and NARA established the CUI Office to manage the program. The Order also rescinded the May 2008 terrorism-related memorandum.

In November 2010, the President released Executive Order 13556 "Controlled Unclassified Information," establishing a CUI program to manage all unclassified information that requires safeguarding and/or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies

The designated bottom-up approach of EO 13556 prescribes an ongoing conversation between the CUI Office, departments and agencies, the private sector, representatives of the public, and state, local and tribal stakeholders to consolidate and standardize an Executive Branch-wide taxonomy and policy for CUI.

58 Executive Order 13556 "Controlled Unclassified Information," 4 November 2010.

5.3.5 Progress on CUI

Per EO 13556, departments and agencies have reviewed all categories, subcategories, and markings used to designate unclassified information for safeguarding and dissemination controls, and in May 2011, they submitted their proposed categories, subcategories, and markings to the EA for review and approval. All approved CUI terms will be published in the CUI Registry, discussed below.

On 9 June 2011, the CUI Office issued the "Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556."[1] This guidance applies to agencies that create or handle unclassified information requiring safeguarding or dissemination controls pursuant to and consistent with applicable law, regulation, or government-wide policy. During the directive development process, the CUI Office hosted multiple working group meetings and consulted with affected agencies and representatives of the public and private sector, as well as state, local, and tribal partners.

In conjunction with the issuance of Executive Order 13556, the CUI Office comprehensively updated its website to reflect the background, current status, and anticipated future direction of the CUI program. This website can be accessed at http://www.archives.gov/cui/. CUI Office staff represented the program at conferences, symposiums, and meetings for various audiences, including federal, state, local, and tribal governments, the private sector, law enforcement, military, academic, and public interest entities.

The CUI Office also produced CUI Awareness and Executive Order 13556 training modules. These computer-based tools are designed for stakeholders at all levels, and are publicly available at http://www.archives.gov/cui/ for either direct access or download.

5.3.6 The Way Ahead

In the coming months, the CUI Office will lead an interagency process to establish an Executive Branch-wide definition and taxonomy of categories for CUI. After consultation with additional stakeholders and representatives of the public, the EA will create a public registry of all approved CUI terms. This Registry will consist of categories, subcategories, and markings of CUI and their definitions, along with applicable safeguarding, dissemination, and decontrol procedures to increase transparency and ensure consistent application. The CUI Registry will be available on the CUI website beginning November 2011.

Departments and agencies will submit CUI compliance plans to the CUI Office by 6 December 2011. The CUI Office will review and, in consultation with affected agencies and the OMB, will establish deadlines for phased implementation by agencies. Follow-on guidance will be issued as the CUI program and schedule is developed.

Federal agencies are expected to initiate efforts to develop CUI guidance specific to their agency and unique mission requirements. The CUI Office will serve as a resource for departments and agencies to ensure coordination of CUI policy government-wide. Outreach efforts will continue, with increased attention to stakeholder groups that are new to the CUI effort. Additional future progress may include the development of attribute-based rules for CUI information sharing, allowing the integration of the Assured SBU Network Interoperability efforts.

Senior Privacy and Civil Liberties Officers

As technology has changed, Congress has identified the need for empowered leaders to protect privacy, civil rights, and civil liberties (P/CR/CL) around federal agency collection, maintenance, use, sharing, and dissemination of personally identifiable information (PII). DHS was the first department to have both a statutorily-created Chief Privacy Officer and Office for Civil Rights and Civil Liberties under the Homeland Security Act of 2002, as amended (6 U.S.C. 552). In 2005, Congress, through the Violence Against Women and Department of Justice Reauthorization Act of 2005, established the position of Chief Privacy Officer in the Department of Justice. In 2007, amendments to IRTPA through the Implementing the Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53) firmly established the Congress' expectation that "each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer." As directed by the 9/11 Act, senior privacy and civil liberties officers were appointed at ODNI, DOJ, State, Treasury, DoD and the CIA. In addition, the authorities of existing privacy officers, to include DHS, were enhanced.[59]

Senior privacy and civil liberties officers work across their departments and agencies to ensure compliance with P/CR/CL requirements. P/CR/CL issues do not have "one size fits all" solutions, so these officers must rely upon policy, guidance, and compliance tools to fashion mission-appropriate protections. Using tools such as a Privacy Impact Assessment (PIA)[60] or a Civil Rights and Civil Liberties Impact Assessment,[61] privacy and civil liberties officers work with program and system managers, developers and administrators to identify data needs and to mitigate risks associated with the collection, use, and maintenance of PII and protected activities. Tools such as a PIA help to ensure that the use of technology does not erode individuals' P/CR/CL. Privacy and civil liberties officers provide training to department and agency personnel on the importance of P/CR/CL protections in day-to-day operations. They also conduct outreach to their mission communities and to the P/CR/CL advocacy community. The ISE has leveraged these relationships with external groups to develop strong protections that are appropriately tailored to activities of the NSI and of fusion centers.

Over the past year, DOJ and DHS have worked to assist state, local, and tribal information partners in building a community of privacy and civil liberties officers within fusion centers. In 2010, the DHS Privacy Office and Office for Civil Rights and Civil Liberties provided core P/CR/CL "Train the Trainer" sessions to 68 fusion center privacy and civil liberties officers. DHS has hosted NSI supervisor training for fusion center analysts, which includes an extensive P/CR/CL protection component.

Going forward, the ISE is working to bridge the federal and state, local, and tribal communities to ensure that privacy and civil liberties officers at all levels of government can identify and address P/CR/CL issues impacting cross-cutting priorities and areas of focus. The ISA IPC Privacy and Civil Liberties Sub-Committee and other ISA IPC governance bodies will be venues for developing strong P/CR/CL protections necessary for cross-government efforts.

---

59 Most of these officers have extensive experience and hold professional certifications for P/CR/CL.

60 A PIA is a risk management tool for privacy required by the E-government Act of 2002 (Public Law 107-347).

61 DHS's Office for Civil Rights and Civil Liberties conduct Civil Rights and Civil Liberties Impact Assessments to determine whether a DHS program, policy, or activity has an impact on the civil rights or civil liberties of individuals.

6 Enhancing Privacy, Civil Rights, and Civil Liberties Protections

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) aims at the broadest possible sharing of information for counterterrorism purposes, while also explicitly recognizing that such sharing must respect privacy, civil rights, and civil liberties (P/CR/CL). Only by zealously protecting these rights and liberties will we continue to secure the confidence and support of the American people for critical information sharing efforts.[62] The ISE-based community of federal, state, local, and tribal privacy and civil liberties officers works diligently to ensure that privacy protections are identified and addressed with regard to terrorism information sharing activities. A critical factor in the success of the ISE lies in maintaining the trust of the American people that P/CR/CL is protected as information is shared. Accordingly, the Executive Branch is also working with interested privacy advocacy groups to ensure P/CR/CL are appropriately addressed as part of the WikiLeaks mitigation efforts.

The ISE Privacy Guidelines, approved by the White House in 2006, requires agencies to implement policies and processes to protect P/CR/CL.[63] The Guidelines also require federal departments and agencies, as well as non-federal partners, to implement protections that are "at least as comprehensive" as the Guidelines. The Privacy and Civil Liberties Sub-Committee of the Information Sharing and Access Interagency Policy Committee (ISA IPC), the successor of the ISE Privacy Guidelines Committee, serves as a resource for information sharing partners for best practices and tools to implement this protection framework. Over the last several years, additional implementation guidance, which provides detailed direction on ISE privacy policy development and white papers on privacy-related topics, has been developed to support the development of P/CR/CL protection policies.

6.1 Privacy, Civil Rights, and Civil Liberties Protection Policies

A critical step in the safeguarding of P/CR/CL during information sharing activities is the development and adoption of a written P/CR/CL policy that meets the standards of the ISE Privacy Guidelines.

As federal mission partners, PM-ISE, the Department of Justice (DOJ), and the Department of Homeland Security (DHS) have supported the development of ISE privacy protection policies by issuing guidance and providing technical assistance to assist ISE participants in implementing their agency or departmental ISE privacy protection policies. These efforts have helped ISE mission partners achieve consistent and uniform implementation of ISE Privacy Guidelines.

---

62 See page 27 of the 2007 National Strategy for Information Sharing for the Core Privacy Principles for Protecting Privacy and Other Legal Rights in the Sharing of Information: http://www.ise.gov/sites/default/files/nsis_book_0.pdf

63 Section 1016(d)(2)(A) of IRTPA requires the President to issue guidelines to "protect privacy and civil liberties in the development and use of the ISE." Presidential Guideline 5, 'Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment," implemented this requirement: http://www.ise.gov/sites/default/files/guideline%205%20-%20privacy%20rights%20and%20legal%20protections.pdf

Currently, nine out of 14 ISE departments and agencies have reported that they have developed ISE P/CR/CL protection policies. Federal agencies have also made measurable progress toward implementing these policies by modifying business processes and updating sharing agreements to align with the new policies. For example, the DOJ Deputy Attorney General issued a notification memo to all DOJ component heads outlining their responsibilities under the DOJ ISE Privacy Policy. In addition, eight out of 14 departments and agencies report that they have implemented mechanisms to assist senior privacy and civil liberties officers in verifying compliance with P/CR/CL protection policies, including the department or agency's ISE policy. For example, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and the DHS Office of the General Counsel now review all DHS agreements for sharing information with external partners to identify P/CR/CL equities, and to ensure that provisions addressing compliance measures and reviews are included.

As of 31 March 2011, all operational fusion centers have adopted ISE-consistent privacy policies. These privacy policies will ensure strong privacy protections for state and local partners and the public, and address the protection requirements for participation in the Nationwide SAR Initiative.

State, local, and tribal partners have worked to develop ISE P/CR/CL protection policies that are "at least as comprehensive as" the ISE Privacy Guidelines, a standard prescribed by the Guidelines as a prerequisite for receiving terrorism information from federal entitites. For example, all operational fusion centers were determined to have privacy policies that are "at least as comprehensive as" the ISE Privacy Guidelines. All fusion centers have designated privacy and civil liberties officers who have received core training in P/CR/CL protections from the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office. Additionally, from late 2010 to early 2011, 14 fusion centers conducted the first round of peer-to-peer P/CR/CL compliance reviews using a P/CR/CL compliance verification template issued by GLOBAL and the Criminal Intelligence Coordinating Council (CICC).

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Program Management Office is working diligently with NSI participants to implement all of the elements of the NSI Privacy Framework[64], including alignment with the privacy protections of the most current ISE-SAR Functional Standard. As part of the NSI expansion to federal agencies, the Department of the Interior (DOI) SAR Policy Working Group met with FBI personnel and with the DOI Chief Privacy Officer for two days in 2010 to develop the DOI policy for SAR.

64 The protection of P/CR/CL is paramount to the success of the NSI. Given this importance, the NSI has worked with key partners—including the American Civil Liberties Union and other advocacy groups—to develop protections that, when consolidated, make up the NSI Privacy Framework, which is derived from the protection requirements of the ISE Privacy Guidelines and has elements specific to NSI operations.

6.2 Privacy Training and Outreach

ISE mission partners have expanded training efforts to re-enforce and institutionalize P/CR/CL protections. All federal agencies reported that personnel receive training with a specialized privacy and civil liberties protection component at least annually. For example, the DOI trained members at all of their bureaus on P/CR/CL protection responsibilities during three sessions in late 2010.

As departments and agencies move forward with adopting P/CR/CL protections, agencies report an increase in P/CR/CL training for personnel with information sharing responsibilities. Currently, half of all responding ISE departments and agencies reported providing this training to ISE personnel on P/CR/CL protection policies, which is a seven percent improvement from 2010.

Under the auspices of the NSI, over 800,000 law enforcement officers nationwide are being provided the NSI Front Line Officer Training, a critical portion of which emphasizes the relevance of P/CR/CL protections in identifying and documenting suspicious activity. Through the full-day NSI Analytic training course, analysts and supervisory analysts receive extensive training in P/CR/CL protections applicable to the specialized SAR vetting process.

Outreach is central to achieving ISE privacy protections. ISE participants at all levels of government engage with external advocacy groups to demonstrate current protections and to solicit input for enhanced protections. Federal ISE participants are engaged in internal outreach among department and agency personnel. For example, the State Department distributed several cables about commercial data privacy to personnel at overseas posts, providing these posts with relevant background about privacy considerations specific to the host country, and increasing consular awareness and understanding of disparate regional approaches to P/CR/CL protection.

The State Department recently announced a mandatory distance learning course for employees. The purpose of this course is to provide employees with the skills and knowledge necessary to comply with laws and regulations by identifying and protecting personally identifiable information.

In addition, all DHS personnel must take the annual "Culture of Privacy" training, which incorporates the elements of the DHS ISE Privacy and Civil Liberties Protection Policy.

6.3 Privacy & Civil Liberties (P/CL) Sub-Committee

The P/CL Sub-Committee was established under the ISA IPC in September 2010. The P/CL Sub-Committee is the successor to the ISE Privacy Guidelines Committee and serves to advise and support the ISA IPC by addressing national security issues (including homeland security issues) that are necessary to facilitate the sharing of information to enhance the national security of the United States while protecting P/CR/CL. The P/CL Sub-Committee consists of senior privacy and civil liberties officials from all departments and agencies who are represented on the ISA IPC and is governed by an Executive Committee consisting of the senior privacy and civil liberties officials of the ODNI, the DHS, and the DOJ.

Over the past year, the P/CL Sub-Committee has established three working groups: the Privacy and Civil Liberties Legal Issues Working Group, the Privacy and Information Technology Working Group, and the Compliance Review Working Group. The Sub-Committee and its working groups are working on the following projects over the next year, including:

- Examining the ISE Privacy Guidelines and the Key Issues Guidance to identify areas in which P/CR/CL protections should be strengthened, clarified, or supplemented as a result of the implementation experience of ISE mission partners.
- Developing tools and processes for automated P/CR/CL practices within federal ISE departments and agencies, to achieve a more standardized application of principles across federal ISE departments and agencies. This effort will include an assessment of automated compliance review solutions currently in use by federal ISE mission partners to identify effective tools for standardizing and strengthening audit, accountability, and oversight capabilities.
- Developing a compliance review and best practices tool to ensure consistency and standardization as federal ISE participants implement the ISE Privacy Guidelines. Through the compliance review process, each federal ISE agency will evaluate its internal operating policies, processes, and procedures to assess its compliance with all applicable constitutional provisions and laws protecting P/CR/CL in the gathering and collection, use, analysis, retention, destruction, sharing, and disclosure of information.
- Developing and delivering P/CR/CL training for ISE mission partners as needed.

These projects reflect the P/CL Sub-Committee's strategic focus on strengthening and regularizing protections for P/CR/CL via compliance or enforcement mechanisms; harmonizing processes, tools, and terms of agreement; and leveraging capabilities. These efforts will support the work of privacy and civil liberties officers going forward.

7 APPENDIX A — Performance Assessment Data

The tables in this appendix contain selected results from the 2011 ISE Performance Assessment as self-reported by the ISE departments and agencies. The 2011 ISE Performance Assessment represents progress against the 2007 National Strategy for Information Sharing and the results are aligned according to the focus areas of this strategy. The "Highlight" box is used to describe successes relative to 2010 to help demonstrate the progress that continues to be made across the ISE. Please note that the Department of Defense (DoD)/Joint Chiefs of Staff (JCS) represents the responses of two ISE members, thus a "yes" response on this line counts as two yeses.

Personnel Appraisals

Measurement Question	Do all employees that support ISE-related priorities have "information sharing and collaboration" as a component of their performance appraisals?			
2011 Metric	14 out of 14 responding ISE departments and agencies have included "information sharing and collaboration" as a component in performance appraisals of employees supporting ISE-related priorities.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	Yes
ODNI	Yes		DOT	Yes
DOC	Yes		FBI	Yes
DoD/JCS	Yes		HHS	Yes
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	Yes
2011 Highlight	All departments and agencies report having accomplished this activity—up 14% from 2010.			

Measurement Question	How often do personnel *without* direct ISE responsibilities have "information sharing and collaboration" as a performance objective?			
2011 Metric	10 out of 14 responding ISE departments and agencies have included "information sharing and collaboration" as a component in performance appraisals of employees without direct ISE responsibilities.			
Agency	2011 Response		Agency	2011 Response
CIA	Always		DOJ	Never
DHS	Often		DoS	Always
ODNI	Always		DOT	Never
DOC	Sometimes		FBI	Never
DoD/JCS	Sometimes		HHS	Sometimes
DOE	No Response		NCTC	Always
DOI	Often		Treasury	NA
2011 Highlight	71% of responding ISE departments and agencies are carrying out this activity; 30% have shown improvement since 2010.			

ISE Awareness Training

Measurement Question	Have you implemented any mission-specific training that supports information sharing and collaboration?			
2011 Metric	10 out of 14 responding ISE departments and agencies implemented mission-specific training that supports information sharing and collaboration.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	Yes
DOC	No		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	Over the past year, there has been a 7% increase among responding departments and agencies in the development of ISE mission-specific training.			

Incentives for Information Sharing

Measurement Question	Does your agency offer an award that includes information sharing and collaboration directly or indirectly as criteria?			
2011 Metric	12 out of 14 responding ISE departments and agencies offer (or intend to offer) an award that includes information sharing and collaboration directly or indirectly as criteria.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	Under Development
ODNI	Yes		DOT	Yes
DOC	No		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	Yes
2011 Highlight	No change from 2010; 86% of responding departments and agencies offer (or intend to offer) an award that includes information sharing and collaboration directly or indirectly as criteria.			

Measurement Question	Has nomination of candidates for information sharing and collaboration awards increased since it was first offered?			
2011 Metric	6 out of 14 responding ISE departments and agencies indicated an increase in the number of nominations for information sharing and collaboration awards.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	NA		DoS	No
ODNI	Yes		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	No		HHS	No
DOE	No Response		NCTC	Yes
DOI	NA		Treasury	NA
2011 Highlight	43% of responding ISE departments and agencies identified an increase in nominations—doubling the number from 2010.			

Systems Security Practices

Measurement Question	Does your agency have documented policies and/or implementing guidelines on IT security reciprocity stating the conditions under which you will accept the security certification and/or accreditation/authorization of another organization?			
2011 Metric	9 out of 14 responding ISE departments and agencies have documented policies and/or implementation guidelines on IT security reciprocity stating the conditions under which they will accept the security certification and/or accreditation of another organization.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	No
DHS	Yes		DoS	No
ODNI	Yes		DOT	Yes
DOC	No		FBI	No
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	Yes
2011 Highlight	No change from 2010; 64% report having documented policies and/or implementation guidelines on IT security reciprocity stating the conditions under which they will accept the security certification and/or accreditation of another organization.			

ISE Shared Spaces

Measurement Question	Has your agency incorporated Common Information Sharing Technical Standards into your architectures?			
2011 Metric	9 out of 14 responding ISE departments and agencies have incorporated CISS Technical Standards into their architectures.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	No
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	No
2011 Highlight	There has been a 7% increase in the number of departments and agencies indicating that they are including CISS standards.			

Measurement Question	Does your agency reference mission segment architectures (e.g. SAR) in implementing ISE mission business processes?			
2011 Metric	9 out of 14 responding ISE departments and agencies reference mission segment architectures (e.g. SAR) in implementing ISE mission business processes.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	No
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	Over the past year, 7% more of the responding ISE departments and agencies are referencing mission segment architectures.			

Measurement Question	Is your agency able to share terrorism and homeland security information following the ISE Shared Spaces concept?			
2011 Metric	11 out of 14 responding ISE departments and agencies are able to share terrorism and homeland security information following the ISE Shared Spaces concept.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	Yes
ODNI	Yes		DOT	Yes
DOC	No		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	No
2011 Highlight	No change from 2010; 79% report the capability to share terrorism and homeland security information through ISE Shared Spaces.			

Measurement Question	Do you see an improvement in your terrorism information sharing processes with other ISE partners by implementing an ISE Shared Space in your organization?			
2011 Metric	11 out of 14 responding ISE departments and agencies see an improvement.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	Yes
ODNI	Yes		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	NA
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	No change from 2010.			

Measurement Question	Has access to terrorism information from ISE partners been improved by utilizing their designated ISE Shared Space?			
2011 Metric	9 out of 14 responding ISE departments and agencies are reporting improvement through use of designated ISE Shared Spaces.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	No
DHS	Yes		DoS	Yes
ODNI	Yes		DOT	Yes
DOC	NA		FBI	No
DoD/JCS	Yes		HHS	NA
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	No change from 2010.			

Privacy Policies

Measurement Question	Has your agency submitted an ISE privacy policy to the Privacy and Civil Liberties Sub-Committee?			
2011 Metric	9 out of 14 responding ISE departments and agencies have developed and implemented an ISE Privacy Policy and submitted it to the Privacy and Civil Liberties Sub-Committee.			
Agency	2011 Response		Agency	2011 Response
CIA	Under Development		DOJ	Yes
DHS	Yes		DoS	Yes
ODNI	Yes		DOT	Under Development
DOC	Under Development		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	Under Development
2011 Highlight	No change from 2010 - 64% of responding ISE departments and agencies have developed and implemented an ISE Privacy Policy and submitted it to the Privacy and Civil Liberties Sub-Committee			

Measurement Question	Have personnel with information sharing responsibilities received training on your agency's privacy and civil liberties policies, to include your agency's ISE Privacy Policy?			
2011 Metric	8 out of 14 responding ISE departments and agencies have provided training on privacy and civil liberties policies to personnel with information sharing responsibilities.			
Agency	2011 Response		Agency	2011 Response
CIA	NA		DOJ	Yes
DHS	Yes		DoS	Yes
ODNI	No		DOT	NA
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	No
2011 Highlight	There has been a 13% increase in the past year in the number of responding ISE departments and agencies who have provided this training.			

Enterprise Architecture – Investments

Measurement Question	Has your agency mapped at least one IT investment to its information sharing segment architectures?			
2011 Metric	11 out of 14 responding ISE departments and agencies have mapped at least one IT investment to its information sharing segment architectures.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	Yes
ODNI	Yes		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	No
2011 Highlight	There has been a 14% increase in the past year in the number of responding ISE departments and agencies who have mapped at least one investment—now at 79%.			

Measurement Question	Has your agency represented all major ISE IT investments in its enterprise transition plans?			
2011 Metric	8 out of 14 responding ISE departments and agencies have represented all major ISE IT investments in its enterprise transition plans.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	Yes
2011 Highlight	There has been a 7% increase in the past year in the number of responding ISE departments and agencies representing all major IT investments—now at 57%.			

Measurement Question	Does your agency have interconnection plans for SBU/CUI networks supporting the ISE?			
2011 Metric	8 out of 14 responding ISE departments and agencies have developed (or are developing) interconnection plans for SBU/CUI networks supporting the ISE.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	No		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	Under Development
2011 Highlight	There has been a 14% increase in the past year in the number of responding ISE departments and agencies who have interconnection plans for SBU/CUI networks supporting the ISE—now standing at 57%.			

Measurement Question	Does your agency have a plan for implementing interconnection capability for sharing terrorism and homeland security information across SBU/ CUI networks?			
2011 Metric	5 out of 14 responding ISE departments and agencies have a plan for implementing interconnection capability for sharing terrorism and homeland security information across SBU/ CUI networks.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	NA		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	Under Development
2011 Highlight	With the IC responding in the negative this year, there is a 21% decrease in positive responses for this question; now standing at 36%.			

Enterprise Architecture - Common Information Sharing Standards (CISS)

Measurement Question	Does your agency have a completed, approved information sharing segment architecture?			
2011 Metric	7 out of 14 responding ISE departments and agencies have a completed, approved information sharing segment architecture.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	NA
2011 Highlight	There has been a 7% increase in the past year in the number of responding ISE departments and agencies completing these architectures.			

Measurement Question	Does your agency reference the Information Sharing Environment section of the Federal Transition Framework (FTF) Catalog in building its segment architectures?			
2011 Metric	7 out of 14 responding ISE departments and agencies reference the Information Sharing Environment section of the Federal Transition Framework (FTF) Catalog in building its segment architectures.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	NA
2011 Highlight	With the IC responding in the negative this year, there is a 21% decrease in positive responses for this question; now at 50%.			

Measurement Question	Has your agency incorporated Common Information Sharing Functional Standards into the management and implementation of its ISE-related mission business processes?			
2011 Metric	10 out of 14 responding ISE departments and agencies have incorporated Common Information Sharing Functional Standards into the management and implementation of its ISE-related mission business processes.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	71% of responding ISE departments and agencies are incorporating the standards, representing a 36% increase over the past year.			

Measurement Question	Has your agency incorporated Common Information Sharing Technical Standards into enterprise architectures and IT capability?			
2011 Metric	7 out of 14 responding ISE departments and agencies have incorporated Common Information Sharing Technical Standards into enterprise architectures and IT capability.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	NA
2011 Highlight	50% of responding ISE departments and agencies are incorporating these standards—a 7% increase in the past year in this area.			

Measurement Question	Do you find the Common Information Sharing Functional Standards, such as ISE-SAR, helping your department/agency improve your counterterrorism processes, interfaces to other ISE partners, and structure of your data/information for sharing in the ISE?			
2011 Metric	9 out of 14 responding ISE departments and agencies have noticed improvement over the past year.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	No
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	There has been a 21% increase in the past year in this area with 64% of responding ISE departments and agencies showing improvement over the past year.			

8 APPENDIX B — Acronyms

ADA	Aviation Security and the Air Domain Awareness
ASCIA	Association of State Criminal Investigative Agencies
ASNI WG	Assured Secret Network Interoperability Working Group
AWW	America's Waterway Watch
BAE	Backend Attribute Exchange
BCA	Baseline Capabilities Assessment
BCOT	Building Communities of Trust
BIA	Bureau of Indian Affairs (DOI)
BJA	Bureau of Justice Assistance (DOJ)
CAIAC	Civil Aviation Intelligence Analysis Center (DoD)
CBP	U.S. Customs and Border Protection (DHS)
CIA	Central Intelligence Agency
CICC	Criminal Intelligence Coordinating Council
CIKR	Critical Infrastructure and Key Resources
CIKR ISE	Critical Infrastructure and Key Resources Information Sharing Environment
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Advisory Council (DHS)
CISO	Chief Information Sharing Officer
CISS	Common Information Sharing Standards
CJIS	Criminal Justice Information Services (FBI)
CNSS	Committee on National Security Systems
COC	Critical Operational Capabilities
COI	Community of Interest
CONOPS	Concept of Operations
CT	Counterterrorism
CUI	Controlled Unclassified Information
CUI Office	Controlled Unclassified Information Office (NARA)
CVE	Countering Violent Extremism
DAWG	Data Aggregation Working Group

DD/OS	Deputy Director for Operations Support (NCTC)
DEA	Drug Enforcement Administration (DOJ)
DHE	Domestic Highway Enforcement
DHS	Department of Homeland Security
DI	Directorate of Intelligence (FBI)
DIAP	Drug Interdiction Assistance Program (ONDCP)
DNDO	Domestic Nuclear Detection Office (DHS)
DNI	Director of National Intelligence
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DoS	Department of State
DOT	Department of Transportation
DSAC	Domestic Security Alliance Council (FBI)
DSI MG	DHS SAR Initiative Management Group
DTRA	Defense Threat Reduction Agency (DoD)
EA	Enterprise Architecture or Executive Agent
EO	Executive Order
EOP	Executive Office of the President
EU	European Union
FAA	Federal Aviation Administration (DOT)
FBI	Federal Bureau of Investigation
FBINet	Federal Bureau of Investigation Secret Domain Network
FEA BRM	Federal Enterprise Architecture Business Reference Model
FEMA	Federal Emergency Management Agency (DHS)
FICAM	Federal Identity, Credential, and Access Management
FIGs	Field Intelligence Groups
FIMS	Federated Identity and Management Service
FMCSA	Federal Motor Carrier Safety Administration (DOT)
FSAM	Federal Segment Architecture Methodology

FTF	Federal Transition Framework
FY	Fiscal Year
GAO	Government Accountability Office
GeoCONOPS	Geospatial Concept of Operations
GFIPM	Global Federated Identity and Privilege Management
GLOBAL	Global Justice Information Sharing Initiative
GSA	General Services Administration
HHS	Department of Health and Human Services
HIDTA	High Intensity Drug Trafficking Area
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center (DHS)
HSDN	Homeland Security Data Network (DHS)
HSEC SINs	Homeland Security Standing Information Needs (DHS)
HSIN	Homeland Security Information Network (DHS)
HSIN-CS	Homeland Security Information Network-Critical Sectors (DHS)
HSIN-EM	Homeland Security Information Network-Emergency Management (DHS)
HSIN-LE	Homeland Security Information Network-Law Enforcement (DHS)
HSPD	Homeland Security Presidential Directive
I&A	Office of Intelligence and Analysis (DHS)
IA	Intelligence Analyst
IACP	International Association of Chiefs of Police
IC	Intelligence Community
IC ISE	Intelligence Community Information Sharing Executive (ODNI)
ICAM	Identity, Credential, and Access Management
ICAMSC	Identity Credential and Access Management Subcommittee
ICD	Intelligence Community Directive
ICE	Immigration and Customs Enforcement (DHS)
IdAM	Identity and Access Management
IED	Improvised Explosive Device
IEPD	Information Exchange Package Description
IIB	Intelligence Integration Branch (FBI)
IISC	Information Integration Subcommittee
IJIS	Integrated Justice Information System

InCop	Information Collection on Patrol
INTERPOL	International Criminal Police Organization
IO	Intelligence Officer
IP	Office of Infrastructure Protection (DHS) or Identity Provider
IPC	Interagency Policy Committee
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA	Information Sharing and Access
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISC	Information Sharing Council
ISE	Information Sharing Environment
ISGB	Information Sharing Governance Board (DHS)
ISPE	Information Sharing and Partner Engagement (DoD)
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
JABS	Joint Automated Booking System
JCS	Joint Chiefs of Staff (DoD)
JPDO	Joint Planning and Development Office
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
LAPD	Los Angeles Police Department
LEISI	Law Enforcement Information Sharing Initiative
LEO	Law Enforcement Online (FBI)
LOB	Lines of Business
MACE	Multi-Agency Collaboration Environment
MCCA	Major Cities Chiefs Association
MCSA	Major County Sheriffs' Association
MDA	Maritime Domain Awareness
MIST	Multimodal Information Sharing Taskforce
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCIX	National Counterintelligence Executive (ODNI)
NCTC	National Counterterrorism Center (ODNI)

N-DEx	Law Enforcement National Data Exchange (FBI)
NDIC	National Drug Intelligence Center (DOJ)
NextGen	Next Generation Air Transportation System
NFCC	National Fusion Center Conference
NGA	National Geospatial-Intelligence Agency
NGI	Next Generation Identification
NICC	National Infrastructure Coordination Center (DHS)
NIEF	National Information Exchange Federation
NIEM	National Information Exchange Model
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NLE	National Level Exercises
Nlets	National Law Enforcement Telecommunications System
NMIC	National Maritime Intelligence Center
NOC	National Operations Center (DHS)
NPPD	Directorate for National Protection and Programs (DHS)
NSA	National Sheriff's Association or National Security Agency
NSI	Nationwide Suspicious Activity Reporting (SAR) Initiative
NSIS	National Strategy for Information Sharing
NSS	National Security Staff
NSTC	National Science and Technology Council
NSTIC	National Strategy for Trusted Identities in Cyberspace
NTAS	National Terrorism Advisory System
NYC	New York City
NYPD	New York Police Department
NYSIC	New York State Intelligence Center
OASIS	Organization for the Advancement of Structured Information Standards
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OMG	Object Management Group
ONDCP	Office of National Drug Control Policy
OPM	Office of Personnel Management

OSD	Office of the Secretary of Defense (DoD)
P/CL	Privacy and Civil Liberties
P/CR/CL	Privacy, Civil Rights, and Civil Liberties
PAC	Policy Advisory Committee
PCSC	Preventing and Combating Serious Crime
PDA	Portable Digital Assistant
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV-I	Personal Identity Verification – Interoperable
PKI	Public Key Infrastructure
PM-ISE	Program Manager, Information Sharing Environment
PMO	Program Management Office
PRND	Preventive Radiological Nuclear Detection
RAC	Resource Allocation Criteria
RFP	Request for Proposal
RIGs	Regional Intelligence Groups (FBI)
RISC	Repository for Individuals of Special Concern
RISS	Regional Information Sharing System
RISSNET	Regional Information Sharing System Network
SA	Special Agent
SAR	Suspicious Activity Report(ing)
SBU	Sensitive But Unclassified
SDOs	Standards Development Organizations
SIPRNet	Secret Internet Protocol Router Network
SLT	State, Local, and Tribal
SLTPS	State, Local, Tribal and Private Sector
SLTT	State, Local, Tribal and Territorial
SLTTPS	State, Local, Tribal, Territorial, and Private Sector
SNCTC	Southern Nevada Counter Terrorism Center
SP	Service Provider or Special Publication
SSO	Simplified Sign On
STC	Securing the Cities

TLOA	Tribal Law & Order Act
TON	Tohono O'odham Nation
TRIPWire	Technical Resource for Incident Prevention (DHS)
TSA	Transportation Security Administration (DHS)
TSC	Terrorist Screening Center (FBI)
TtT	Train the Trainer
TWCG	TRIPWire Community Gateway
UML	Unified Modeling Language
US-VISIT	United States Visitor and Immigration Status Indicator Technology
USCG	U.S. Coast Guard (DHS)
USD(I)	Under Secretary of Defense for Intelligence (DoD)
USIA	Under Secretary for Intelligence and Analysis (DHS)
USSS	U.S. Secret Service (DHS)
VCC	Virtual Command Centers
WITS	Worldwide Incidents Tracking System
WMD	Weapons of Mass Destruction
WSP	Washington State Police
XML	Extensible Markup Language

PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT
WASHINGTON, D.C. 20511

202.331.2490

WWW.ISE.GOV