INFORMATION SHARING ENVIRONMENT

ANNUAL REPORT TO THE CONGRESS

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

Prepared by the

Program Manager, Information Sharing Environment

30 June 2012


ISE.
Intelligence
Group
centers

INFORMATION SHARING ENVIRONMENT

ANNUAL REPORT TO THE CONGRESS

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

Prepared by the

Program Manager, Information Sharing Environment

30 June 2012

This page intentionally left blank

FOREWORD

As PM-ISE and our mission partners continue to implement responsible information sharing practices, we reflect on the tremendous progress made toward our goal, while recognizing that significant work still needs to be done. In January, Director of National Intelligence James R. Clapper spoke of the national responsibility to share information – "the right data, any time, any place, usable by any authorized recipient, preventable only by law or policy and not technology, and protected by a comprehensive regimen of accountability."[1] As the office responsible for organizing and implementing responsible information sharing practices nationwide, we are proud of the progress we have made strengthening national security while also honoring and protecting privacy, civil rights, and civil liberties.

We have become much better at using our inherent strengths to make the American people safer. Our federated democracy means that we have committed law enforcement, public safety, and intelligence professionals working at the federal, state, local, and tribal levels; they are also working closely with partners in the private sector to protect our nation's infrastructure. We have carved out a strong role for governance through our leadership role in the White House's Information Sharing and Access Interagency Policy Committee. Our robust and innovative private sector contributes significantly to the work of the ISE. And we are championing a standards-based approach to defining government requirements for responsible information sharing that will enable greater interoperability across our government's networks while offering a greater potential for cost savings.

September 2011 marked the tenth anniversary of the 9/11 terrorist attacks. The national security community has achieved numerous successes since 2001, including progress towards improving: interoperability of our sensitive but unclassified computer networks, capabilities of our fusion centers, and mission impact of our nationwide suspicious activity reporting practices. The PM-ISE has enhanced our national security by: advancing these initiatives, brokering solutions between organizations with different missions, convening partners from inside and outside the government, and leading improvements in responsible information sharing through policy, governance, and strategy.

The PM-ISE is committed to continuing to convene partners and lead efforts in innovation. We understand that this is a continuing journey. The evolution of the threats against us, the integration of our resources, and the efficient use of technology to move our responsible information sharing agendas forward requires constant vigilance and leadership.

[1] http://csis.org/files/attachments/120126_info_sharing_clapper_transcript.pdf

Three core ideas are the drivers of PM-ISE's mission. We are:

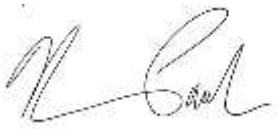
- Grounded by an enduring purpose to **advance responsible information sharing to further the counterterrorism and homeland security missions**. We must stay focused on the fact that we are sharing information in order to keep the American people safe.
- Leading a **transformation from information ownership to information stewardship** in order to improve nationwide decision making. We must treat information held by the government as a national asset: this means it must be used, and reused, to benefit the American people. Information must be protected and cultivated to ensure that we get the maximum value from it. At the same time, strong protections for the privacy, civil rights, and civil liberties of the American people must be safeguarded.
- Promoting **partnerships across federal, state, local, and tribal governments, and the private sector, as well as internationally**. By building organizational capacity at every level, we will share information more securely and effectively. The threats to our safety do not stop at jurisdictional borders; our information must not either.

We have also strengthened privacy, civil rights, and civil liberties protections by developing privacy guidelines, on behalf of the President, and supporting federal, state, and local agencies as they develop privacy policies that are at least as comprehensive as the ISE privacy guidelines.[2] This means that when citizens see something and say something, and when police officers submit reports to their local fusion centers, they all know that the information will be handled appropriately. It means that when analysts conduct their evaluations, they will proceed in a manner based on agreed-upon definitions of behaviors that are indicative of terrorist activity, and that their investigations will not be based on race or religion. It means that the American people can know that their government is committed to protecting their privacy, civil rights, and civil liberties, as well as their security.

While we focus on the accomplishments and the progress to date on numerous fronts, we maintain a sense of urgency about tackling the work that remains to be done. The biggest challenges facing the ISE are the continuously evolving threat environment, the tsunami of new data, and a constrained fiscal environment. As the ISE grows and its work deepens and expands, we need to continue to assess and adjust for current realities–allowing us to be well positioned for dealing with future threats and exploiting opportunities.

These challenges and opportunities present a framework within which to rethink the ISE and our approach to responsible information sharing. We see great potential in leveraging our advances and building from the terrorism-related mission to more broadly support information-led public sector transformation. Recognition of the enduring value of the ISE lies in the ceaseless needs of the mission and the variety of continued successes that have been spawned by our work. This Report showcases many of these accomplishments and lays out our way forward. While gaps, challenges, and opportunities for improvement are present and described, we have established traction, developed a clear and compelling value proposition, and identified a way forward.

We are fulfilling the mission set out before us, and we are enhancing our national security through responsible information sharing. We will continue to fulfill this mission and to identify and meet new challenges as they arise.



Kshemendra Paul, Program Manager, Information Sharing Environment

[2] *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* ("ISE Privacy Guidelines") (November 2006) available at http://ise.gov/sites/default/files/PrivacyGuidelines20061204_1.pdf

CONTENTS

This page intentionally left blank

EXECUTIVE SUMMARY

The ISE is a partnership for responsible sharing of terrorism-related information between the law enforcement, public safety, defense, intelligence, homeland security, and diplomatic communities. It extends to all levels of government – federal, state, local, tribal, and territorial; and incorporates private sector partners and international allies. This Sixth Annual Report to the Congress on the state of the Information Sharing Environment (ISE) examines the extent to which the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) terrorism information sharing mandate is being implemented by agencies that possess or use information about terrorism, operate a system in the ISE, or participate in the ISE.[3] This Report, which PM-ISE is submitting on behalf of the President,[i] incorporates input from our mission partners[4] and uses their initiatives and PM-ISE's management activities to provide a cohesive narrative on the state and progress of terrorism-related responsible information sharing,[5] including its impact on our collective ability to secure the nation and our national interests.

This Report describes how agencies have fared against established performance measures and highlights accomplishments, including illustrative examples of ISE progress toward the responsible information sharing goals derived from IRTPA, presidential guidelines in support of the ISE[6], and the National Strategy for Information Sharing. It covers PM-ISE's reporting responsibilities pertaining to the Interagency Threat Assessment and Coordination Group (ITACG).[7] PM-ISE also supports aspects of information sharing in other domains, such as maritime, primarily to promote cross-domain information integration in the pursuit of strengthening national security through responsible information sharing.

The activities and accomplishments of ISE departments and agencies are bringing us ever closer to achieving our vision of greater national security through more effective information sharing.

---

[3] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, P.L. 108-458 (December 17, 2004), Sec. 1016(h) and (i).
[4] IRTPA Section 1016 (i)(4).
[5] As defined in Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, P.L. 108-458 (December 17, 2004), Sec. 1016(a)(5).
[6] White House Memorandum for the Heads of Executive Departments and Agencies, Guidelines and Requirements in Support of the Information Sharing Environment (December 16, 2005).
[7] 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).

ORGANIZATION

The following sections of the 2012 Report detail ISE progress in:

- **Maturing Information Sharing Across the ISE -** *Adoption of and compliance with interoperable business processes and functional standards in ISE agencies, and their resulting mission impacts;*
- **Optimizing Mission Effectiveness -** *Implementation of identity controls and access management for government networks and data; progress toward interoperability among and between classified and unclassified networks; terrorism-related data aggregation efforts across ISE networks; and improvements in watchlisting and screening processes;*
- **Standards Development and Implementation -** *Development of, conformation with, and reuse of common technical standards that have resulted in mission benefits, improved acquisition practices, and strengthened partnerships between government and industry;*
- **Strengthening Safeguarding to Support Responsible Information Sharing -** *How maturing practices and technologies to safeguard terrorism information are creating a culture of trust, necessary for seamless and responsive sharing of terrorism-related information;*
- **Implementing Privacy, Civil Rights, and Civil Liberties (P/CR/CL) Protections -** *How ISE agencies are developing and implementing policies to enhance P/CR/CL protections*;
- **Managing and Fostering a Culture of Responsible Information Sharing -** *How PM-ISE and ISE agencies are driving the governance and performance- management processes necessary to move the ISE forward as a cohesive whole.*

MATURING INFORMATION SHARING ACROSS THE ISE

Foundational initiatives such as state and major urban area fusion centers, the Nationwide Suspicious Activity Reporting Initiative (NSI), and the Interagency Threat Assessment and Coordination Group (ITACG) continue to mature by expanding their partnerships into new communities, refining technologies and shared services, and working toward performance and mission outcomes. In the law enforcement and intelligence communities, the previous year's efforts are setting the stage for changes in the potential to move information sharing beyond previous expectations. The expansion of federal agency participation in Joint Terrorism Task Forces dramatically improves communication, coordination, and cooperation, leading to a more efficient and effective response to terrorist threats. Emerging ideas for transforming the public safety information sharing business model, coupled with the use of new technologies, such as facial recognition by frontline officers, are making the vision of eliminating administrative and jurisdictional obstacles to information sharing a reality. And the Intelligence Community's IT transformation effort will significantly enhance our ability to share and safeguard information, undoubtedly paving the way for shared services implementation by all communities in the ISE.

With respect to information sharing between the Federal Government and international partners, there have been notable improvements, such as the trilateral agreement between Canada, Mexico, and the United States to work toward interoperable information sharing solutions, and commitment to pilot projects to demonstrate capabilities in this area.

Private sector information sharing is lagging – particularly the communication of threat information from the government to the owners and operators of critical infrastructure, and the ability of the Federal Government to leverage the knowledge and analytic capabilities of these owners – as highlighted by the National Infrastructure

Advisory Council's recent report to the President. Federal, state, local, and private sector partners are taking steps to fill the "bi-directional" information sharing gaps through fusion center and private sector collaboration initiatives, analytic exchanges between the intelligence community and the private sector, and strategic partnerships such as the Domestic Security Alliance Council (DSAC).

Finally, multimodal information sharing initiatives such as the Maritime Information Broker are promoting maritime information sharing among federal, state, local, and tribal (FSLT) law enforcement agencies, but can also be leveraged by all ISE partners as a best practices model for cross-domain information sharing.

The following list highlights accomplishments over the past year. Further detail is provided in the body of the Report.

- DHS and fusion center stakeholders developed and conducted a repeatable annual assessment process, and DHS led gap-mitigation efforts to assist fusion centers in fully achieving critical operational capabilities and enabling capabilities;
- The NSI Program Management Office (PMO) expanded the NSI by implementing standards, policies, and processes across the National Network of Fusion Centers;
- The FBI and NSI PMO continued improvements for eGuardian and NSI Shared Space interoperability, and the ability to search SAR data;
- State, local, and federal agencies, as well as law enforcement associations, created a *unified approach* to the reporting and sharing of information related to suspicious activity;
- The ITACG initiated a multi-faceted Fire Service Intelligence Integration project aimed at increasing intelligence support to firefighters, and developed training to raise awareness of violent radical extremist recruitment in U.S. correctional facilities;
- Counterterrorism Data Layer (CTDL) now provides National Counterterrorism Center (NCTC) analysts with the ability to search, exploit, and correlate terrorism information in a single environment;
- Canada, Mexico, and the United States signed a trilateral Memorandum of Understanding (MOU) to formalize their collective intent on information sharing and interoperability, and are conducting two information sharing pilot projects; and
- Canada is establishing its own version of a PM-ISE; reporting to their Federal CIO, located in the Treasury Board, and with government-wide responsibility.

OPTIMIZING MISSION EFFECTIVENESS

This section of the Report addresses common mission dependencies, highlighting initiatives and progress in the fields of identity, credential, and access management (ICAM); network interoperability; data aggregation (correlation); watchlisting and screening; and Controlled Unclassified Information (CUI) implementation. As these capabilities mature and move toward common solutions, agencies can begin to overcome the barriers that exist between agencies and missions–both technological and policy-based–and open the door to achieving shared goals of ensuring consistent access to the right information across government-wide networks by authorized users who are uniquely and universally identified on networks.

- Sensitive But Unclassified/Controlled Unclassified Information (SBU/CUI) interoperability partners made measureable progress in the areas of Simplified Sign-On (SSO), Search and Discovery, and Standardized Security Controls;

- The CUI Executive Agent–the National Archives and Records Administration—completed major requirements of Executive Order 13556, "Controlled Unclassified Information";
- Interoperable ICAM solutions on federal Secret networks moved from strategic planning under the leadership of the Senior Information Sharing and Safeguarding Steering Committee to tactical implementation by the Committee on National Security Systems (CNSS), with continued oversight of the Steering Committee;
- The DNI, the Attorney General, and Director of NCTC signed updated guidelines designed to allow NCTC to obtain and more effectively analyze certain data to better address terrorism-related threats; and
- PM-ISE canvassed the Intelligence Community and other federal agencies to assess the state of technical collaboration and integration of data screening and data aggregation programs, and produced an interagency report of the findings.

STANDARDS DEVELOPMENT AND IMPLEMENTATION

Architecture, standards, and technology allow mission partners to automate activities, deliver information in a more timely fashion, and acquire and implement interoperable solutions. The end objective is to provide a flexible and scalable architecture on which all partners can participate by building and employing shared services and open standards—like the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—to gather, share, analyze, and disseminate information, and manage costs more effectively.

- The Information Sharing and Access Interagency Policy Committee (ISA IPC) Standards Working Group (SWG) hosted a Standards Repository Summit to identify best practices for creating and maintaining standards for registries and repositories;
- The Standards Way Ahead was created under the auspices of the SWG and the Standards Coordinating Council to capture the collective decisions from the December 2011 Workshop for Information Sharing & Safeguarding Standards (WIS3), sponsored by PM-ISE;
- The National Information Exchange Model (NIEM) Unified Modeling Language (UML) specification was developed, adopted as a standard by the Object Management Group, and implemented by industry;
- NIEM and Universal Core (UCore) council members began discussing NIEM-UCore convergence;
- Trident Warrior 2011 demonstrated the use of NIEM-Maritime for sharing vessel position reports;
- PM-ISE and Canadian government representatives met to discuss NIEM adoption for Canada's law enforcement and public safety communities; and
- The European Pool against Organised Crime (EPOC) is now focused on using NIEM as a method to increase interoperability and drive down costs.

STRENGTHENING SAFEGUARDING TO SUPPORT RESPONSIBLE INFORMATION SHARING

Over the past year, there has been considerable activity in the area of information safeguarding as it relates to advancing and enabling information sharing. The most prominent accomplishment has been the development of a new federal-wide approach to safeguarding and governance for classified information and systems. Catalyzed by the WikiLeaks breach, the creation of new governance structures to support information sharing and safeguarding has positioned the Federal Government to improve situational awareness and management for classified

networks, maintain interoperability, and increase classified safeguarding overall. E.O. 13587 affirmed the primary responsibility of agencies that handle classified information on computer systems to share and safeguard such information, consistent with appropriate protections for privacy and civil liberties. The Administration identified five near-term tactical priorities for improving the safeguarding of classified information on computer systems and instantiated these priorities through the budget process.

In addition to the activity around safeguarding classified networks and information, progress on other aspects of sharing and safeguarding has continued. Key safeguarding milestones were realized across all ISE stakeholder groups. Major accomplishments included the advancement of cyber-threat information sharing initiatives with foreign partners and the private sector, and progress toward the development and implementation of common security standards to support reciprocity and interoperability.

- The National Insider Threat Task Force developed a draft National Insider Threat Policy to deter, detect, and mitigate insider threats;
- The Intelligence Community (IC) CIO launched a plan to improve the efficiency of the IC Information Technology Enterprise that will significantly enhance the IC's ability to share and safeguard intelligence;
- The Department of Defense completed a successful pilot project for sharing cyber-threat information with private sector companies that comprise the Defense Industrial Base; and
- The United States and India signed an MOU to promote the timely sharing of cybersecurity information.

IMPLEMENTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTIONS

To ensure that information is shared in a manner consistent with privacy, civil rights, and civil liberties (P/CR/CL) protections, these protections must be well understood within the culture, and they must be reinforced in training as well as integrated into business processes and technologies. Actions taken include increased focus on the development and implementation of federal policies consistent with the ISE Privacy Guidelines; training for fusion centers and front-line law enforcement officers; and expanded membership to the ISA IPC's Privacy and Civil Liberties (P/CL) Subcommittee to include a state and local advisory representative. All federal partners reported having some kind of mechanism in place to allow for agency verification that personnel are in compliance with agency privacy and civil liberties policies. Sixteen state and major urban area fusion centers conducted the first round of peer-to-peer P/CR/CL compliance reviews, using a compliance verification template issued by the Global Justice Information Sharing Initiative (Global) and the Criminal Intelligence Coordinating Council (CICC), and all ISE departments and agencies reported that their respective training programs address the protection of privacy and civil liberties.

MANAGING AND FOSTERING A CULTURE OF RESPONSIBLE INFORMATION SHARING

Exercising government-wide authority over the sharing and safeguarding of information requires the PM-ISE and ISE agencies to foster a culture of responsible information sharing that is built upon mutual trust and shared responsibility. Integrated governance, ISE-wide performance management, budget-performance integration, training, incentives, tools, and sourcing of best practices are the means to mature the culture from a partially realized ISE to a tightly knit association of mission partners whose development, adoption, and implementation of common practices and standards comprises a coherent whole. For example, ISE agencies are increasingly assigning executives and dedicating staff to overseeing responsible information sharing functions, and have increased the nomination of candidates for information sharing and collaboration awards.

- The Department of Homeland Security and its federal partners hosted a series of workshops and seminars on countering violent extremism, analytic tradecraft, security, classified information sharing, and fusion center liaison programs;
- The NSI PMO developed and is now implementing Suspicious Activity Reporting (SAR) awareness training for other key non-law- enforcement constituencies, or "hometown security partners" that are important to the SAR effort; and
- The FBI developed three Web-based, information sharing-related training modules, and made them available to federal, state, local, and tribal law enforcement partners and fusion center personnel via their Unclassified Virtual Academy.

HOW THE 2012 REPORT DIFFERS FROM PAST REPORTS

In addition to reporting on ISE initiatives as they relate to IRTPA requirements, the 2012 Report also addresses the ISE's actions in response to PM-ISE's implementation guidance for the ISE, highlighting the extent to which the Program Manager has supported ISE agencies in their execution of responsible information sharing initiatives. This Report also includes a "way forward" for the ISE; this demonstrates leadership's commitment to responsible information sharing, describes an implementation roadmap, and updates PM-ISE's vision, mission, and objectives to deliver capabilities that enhance national security through responsible information sharing. The way forward addresses lingering concerns that have kept terrorism-related information sharing on the GAO High Risk List since 2005.

This Annual Report is an Executive-level document outlining progress and highlighting successes in the ISE. The information sharing initiatives and process improvements of both PM-ISE and our partners are briefly discussed throughout this Report. Detailed results are further discussed in our online presence at ISE.gov. Additional information will be provided through our "Building Blocks" knowledge management initiative, which will be deployed on ISE.gov later this year.

PM-ISE'S CONTRIBUTIONS OVER THE LAST YEAR

The Federal Government and its state, local, and tribal counterparts have achieved significant information sharing success over the last year. The Office of the PM-ISE provides an effective platform for those agency contributions. In particular, PM-ISE continues to contribute to national security by advancing responsible information sharing, brokering solutions between organizations with different missions, convening partners from inside and outside the government, and leading national information sharing through strategy, technology, interoperability, policy, and governance. Several key contributions are highlighted below.

TOOLS OF THE PM-ISE

- Standards Development
- Convening/Liaison Function
- Honest Broker of Requirements
- Pilots and Implementation Funding
- Programmatic and Implementation Guidance
- Training, Outreach, and Communication
- Governance, Policy, Guidance

To advance responsible information sharing to further the counterterrorism and homeland security missions, and to improve decision making at all levels of government, the PM-ISE has:

- Worked with the International Association of the Chiefs of Police, Global, and DoJ's Bureau of Justice Assistance to address critical law enforcement information sharing gaps, issues, and challenges, and as a result began a dialogue based on a white paper entitled "Reinventing the Public Safety Business Model;"

- Convened the National Fusion Liaison Officer Program Workshop, in partnership with DHS, to facilitate sharing of best practices and lessons learned across the National Network of Fusion Centers;
- Partnered with DHS's Domestic Nuclear Detection Office to demonstrate the ability to connect radiological/nuclear alarm data and detectors in the Global Nuclear Detection Architecture;
- Began to apply the ISE's proven information sharing techniques and processes to the cyber information sharing problem set;
- Initiated development of a new NIEM-based Information Exchange Package Documentation (IEPD) for Requests for Information;
- Sponsored, along with the National Maritime Intelligence-Integration Office (NMIO), a maritime port security information sharing initiative to facilitate the integration of maritime information and intelligence collection and analysis in support of national policy;
- Initiated, with DHS, a portfolio initiative to drive geospatial information sharing as a national asset;
- Sponsored the first "whole-of-government" Data Aggregation Summit for 160 individuals representing 25 ISE mission partners, and identified persistent data aggregation, data integration, and data management challenges; and
- Canvassed the Intelligence Community and other federal agencies to assess the state of technical collaboration and integration of the Federal Government's non-traditional terrorism-related data screening and data aggregation programs, and produced an interagency report of the findings and recommendations.

Grounded in the understanding that a standards-based approach will enable shared services, greater interoperability, and more efficient use of existing systems, PM-ISE has contributed in the following ways:

- Brought together five different federal or national identity federation efforts for the first time to discuss their identity management frameworks, future plans, and how they could better align their efforts;
- Convened more than 200 ISE mission partners, leading standards development organizations (SDO), and industry associations to debate, discuss, and agree on standards and frameworks to enable responsible information sharing;
- Developed, with DoJ/Bureau of Justice Assistance (BJA), training and toolkits for grant managers and grantees to implement standards-based requirements development;
- Promoted the development, ratification, and adoption of open standards for commercial products and services that can easily exchange information in partnership with industry-led consortia and SDOs;
- Provided dedicated subject matter expertise to interagency SBU/CUI interoperability efforts;
- Supported efforts to facilitate NIEM-UCore convergence, permitting multiple communities' information systems to exchange messages;
- Sponsored the American Council for Technology - Industry Advisory Council (ACT-IAC) to solicit industry input on data exchange technical standards, and to learn from industry what tools it needs to work more effectively with government on standards-based IT acquisitions;
- Provided dedicated subject matter expertise to advance coordinated identity, credential, and access management (ICAM) efforts across the whole of government;

- Teamed with the U.S. General Services Administration (GSA) to operationalize the Backend Attribute Exchange (BAE), in order to enable systems to securely access user attributes originating from multiple data sources, based on existing industry standards, while properly handling both security and privacy issues;
- Launched an initiative to re-evaluate the baseline set of standards needed for information exchange, working closely with the Standards Working Group and the Standards Coordinating Council;
- Sponsored, in partnership with DoJ, the development of an IEPD for federated search, and sought to increase the number of agencies that share sensitive law enforcement information;
- Sponsored the Integrated Justice Information Systems (IJIS) Institute Springboard effort to advance justice, public safety, and homeland security information sharing via an open standards implementation process; and
- Initiated a gap analysis to determine if Federal Identity, Credential, and Access Management (FICAM) can be implemented on the federal Secret Fabric, with CNSS as a partner.

Engagement, training, and management support are helping to create a culture shift that instills an enduring commitment to responsible information sharing. Exercising its responsibility to plan for, manage, and oversee the implementation of the ISE, PM-ISE has contributed in the following ways:

- Served on the National Security Staff's (NSS) post-WikiLeaks Structural Reforms IPC and helped draft E.O. 13587 to improve the sharing and safeguarding of classified information and systems;
- Established the Classified Information Sharing and Safeguarding Office (CISSO) in concert with E.O. 13587 structural reforms, affirming PM-ISE's cross-cutting leadership role in both information sharing and safeguarding;
- On behalf of the Senior Information Sharing and Safeguarding Steering Committee, led the development of the 90-day Report to the President on the status of information sharing and safeguarding of classified information on computer networks;
- Issued ISE Implementation Guidance that provides more specific direction for agency activities in order to achieve the priorities defined in joint Office of Management and Budget (OMB) and NSS programmatic guidance, and serve as the basis for objective system-wide performance goals for the following year;
- Hosted an international training event to help implement NIEM-conformant exchanges for North American pilots for public health and public safety information sharing;
- Partnered with Canadian government representatives to discuss NIEM adoption for Canada's law enforcement and public safety communities;
- Created a set of illustrative, mission-based scenarios to translate White House strategic goals and initiatives into mission-specific narratives, to assist agencies in planning for and executing goal-based initiatives;
- Supported, with DHS, the Centers of Analytical Excellence Workshop to identify fusion centers that have developed expertise in topical areas, and to benefit the National Network of Fusion Centers; and

- Partnered with the NSI PMO and relevant professional organizations to develop the Hometown Partners training materials aimed at 911 operators, fire and emergency medical service personnel, emergency management personnel, private sector security personnel, and probation, parole, and corrections personnel.

This page intentionally left blank

ANALYSIS OF LEGAL REQUIREMENTS, PERFORMANCE ASSESSMENT DATA, AND GAPS, CHALLENGES, AND OPPORTUNITIES FOR IMPROVEMENT

This Report does not provide an exhaustive chronology of ISE activities over the previous year. However it does illustrate the major areas of focus and ongoing investment as reported by ISE agencies, and provides a basis for analysis by PM-ISE. The following high-level analysis and findings provide:

- An assessment of the extent to which this Report conforms to the requirements as stated in the law;
- An assessment of the maturity of the ISE as measured by the PM-ISE Annual Performance Assessment; and
- Areas for improvement, and opportunities for future investment as identified by this analysis.

MEETING THE LEGAL REQUIREMENTS FOR ISE PERFORMANCE MANAGEMENT REPORTS

Section 1016(h) of the Intelligence Reform and Terrorism Prevention Act (IRTPA) specifies ten reporting categories that are required in the annual performance management report. In order to ensure compliance with these requirements, all content in this Report that corresponds to Section 1016(h) is cited using endnotes, and all reporting requirements are addressed. In addition, reporting which corresponds to the ISE attributes listed in Section 1016(b) is cited in order to show alignment between ISE activities and the mandatory attributes of the ISE.

HIGH-LEVEL ANALYSIS OF THE ANNUAL PM-ISE PERFORMANCE ASSESSMENT REPORT

The ISE Performance Framework uses three stages of maturity to communicate expected capabilities for the following year. Maturity Stage 1 describes the capabilities currently expected for ISE agencies; Maturity Stage 2 describes capabilities that are expected to be developed in two to three years; and Maturity Stage 3 describes capabilities that are expected in five to seven years.[8] 2012 is a baseline year for the ISE Performance Management Framework; we therefore are focusing analysis on the Maturity Stage 1 initiatives.

Currently, ISE agencies demonstrate progress at Maturity Stage 1, with the following exceptions:

- Consistent, government-wide application of privacy protections.[ii]
  - **Finding:** *Compliance with the requirements of the ISE Privacy Guidelines remains incomplete. Six years after the issuance of the ISE Privacy Guidelines, a small number of ISE agencies are still developing ISE privacy policies. Within the past 12 months, there has been a 30% increase in the number of completed ISE privacy policies. One positive development has been the direct engagement by the senior leadership of those agencies without ISE privacy policies, many of whom have committed to the completion of their agency's ISE privacy policy by the end of 2012.*[9]
- Assured network interoperability.
  - **Finding:** *Approximately one-half of ISE agencies have implemented interconnection plans for SBU/CUI networks supporting ISE-related missions. A constrained fiscal environment, fragmented*

[8] See Appendix A for more detail.
[9] Implementation Guidance for FY 2013 Programmatic Guidance for the Information Sharing Environment (ISE), PM-ISE memo dated August 8, 2011.

architectures, and policy challenges hinder agency efforts in this area. To help address these gaps, the SBU/CUI Interoperability Working Group is focusing on identity and access management (IdAM) solutions to provide a simplified sign-on capability between mission partners' SBU and CUI networks.

- ISE mission system acquisition processes.
  - **Finding:** *Only one-half of ISE agencies consider ISE functional and technical standards when issuing grants or RFPs for ISE-related systems. PM-ISE, in partnership with GSA, has begun several efforts to address the standards-based acquisition issue and to develop a baseline set of standards for information exchange. PM-ISE intends to leverage the output of these efforts and, in coordination with GSA and our partner organizations, will make recommendations to foster information sharing standards in acquisition and grant language.*

Looking ahead, ISE agencies are well positioned to meet Maturity Stage 2 goals in two to three years. However, the data from the annual ISE performance assessment suggest that the following Stage 2 issues require close management oversight:

- Privacy compliance.[iii]
  - **Finding:** *Of the agencies with privacy policies, 79% have made no progress in verifying that their ISE-enabling business processes are in compliance with their ISE privacy policy. Approximately one-third of agencies with ISE privacy policies completed those policies within the past 12 months and are still in the initial stages of implementing ISE privacy protections and policies. Agencies with established policies report consistent progress in implementing ISE policies, including the proactive integration of protections into the development of new systems and initiatives. The Privacy and Civil Liberties Subcommittee of the Information Sharing and Access Interagency Policy Committee (ISA IPC) is developing a compliance review self-assessment tool that will assist federal ISE mission partners in identifying gaps and will result in more detailed and measured performance reporting.*
- Federated Identity Management[iv]
  - **Finding:** *33% of ISE agencies do not accept IT security certification bodies of evidence from other federal agencies, nor do they make accreditation decisions without retesting. In collaboration with GSA and the Federal Chief Information Officers (CIO) Council, PM-ISE is attempting to bridge that capability gap through the Backend Attribute Exchange (BAE) pilot, which endeavors to securely access various credentials that may originate from multiple authoritative sources to make access control decisions.*
- Entity/Data Tagging.
  - **Finding:** *65% of ISE agencies report little or no progress in working towards metadata tagging solutions. This reduces their ability to automate access decisions based upon user and data attributes, and hinders their ability to discover and retrieve data, perform analysis, and maintain provenance and lineage on terrorism-related data.*

Additionally, the annual performance assessment responses indicated that the ISE has significant challenges in integrating non-traditional partners such as the smaller non-Title 10 (Defense) and non-Title 50 (Intelligence) entities into its operations, especially in efforts such as the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), and the National Network of Fusion Centers. To address this issue and to provide a mechanism for addressing non-traditional partner equities, coordination groups such as the Department of Homeland Security NT-10/50 Stakeholder Forum have been established in the ISE community.

OTHER GAPS, CHALLENGES, AND OPPORTUNITIES

In the process of compiling this Report, and based on our interactions with ISE agencies, PM-ISE identified several additional gaps, challenges, and opportunities for improvement of the ISE. Near-term actions to address these issues are reflected in the high-level roadmap included in the Way Forward section of this Report. The implementation roadmap includes three years of implementation guidance from the PM-ISE to the agencies, based upon the Administration's priorities. PM-ISE and the ISA IPC will monitor ISE agency efforts to implement this guidance through the governance and performance management actions outlined in Section 6 of this Report. Significant issues to address are as follows:

- The need to Transform Information Sharing Business Models
  - **Finding:** *Resource constraints, especially among state, local, and tribal (SLT) law enforcement agencies, necessitate the transformation of information sharing business models. A significant cost savings could be realized through consolidation, regionalization, and reuse of open standards and trusted IT platforms. In addition, as diverse resources are applied to particular justice and public safety problems (including terrorism), systems at all levels of government need to factor in case deconfliction. Development of common, agreed-upon, national deconfliction standards will help ensure common awareness in the operational environment.*
- Challenges with Data Aggregation
  - **Finding:** *Centralized data correlation and data storage introduces privacy and security challenges that limit mission effectiveness. The development of a data aggregation reference architecture could alleviate these challenges by establishing a roadmap for centralized correlation with decentralized data producers. In addition, unstructured data, such as free-form text documents, presents further technical and human resource challenges.*
- Public-Private Sector Information Sharing Gap[v]
  - **Finding:** *According to the National Infrastructure Advisory Council (NIAC), federal-private sector bi-directional information sharing is still relatively immature, leaving a large gap in public-private sector information sharing. In particular, intelligence sharing between the Federal Government and private sector owners and operators of critical infrastructure is lagging behind the "marked improvements" the NIAC observed in the sharing of federal intelligence with state, local, tribal, and territorial governments over the last several years.*
- Tribal Information Sharing Gaps[vi]
  - **Finding:** *There are opportunities to increase tribal information sharing through the National Network of Fusion Centers. PM-ISE and its federal partners are focused on addressing and improving some of the foundational policy, governance, relationship, and capacity issues related to tribal information sharing. SLT partners are expanding tribal participation through Fusion Liaison Officer (FLO) programs.*
- Classified Information Sharing and Safeguarding Governance Gaps
  - **Finding:** *With the collective progress in developing Federal Government-wide governance structures for Secret networks and in solidifying key priorities and milestones for implementation, the Federal Government is positioned for continued improvements in classified information sharing and safeguarding in the coming year.*
- Opportunity with Cybersecurity Information Sharing
  - **Finding:** *Given the increasing frequency, impact, and sophistication of attacks on information and information systems in the United States, cybersecurity is a national security priority. Cybersecurity can be improved if agencies more effectively share cyber-vulnerability and intrusion incident information. The application of the ISE's proven information sharing techniques and processes to the cyber*

information sharing problem set can enable this. As new legislation emerges in this area, information sharing related to cybersecurity functions will play an increasingly important role in the ISE.

- Opportunity to Strengthen Collaboration and Coordination Between Federal, State, Local, Tribal, and Private Sector Entities
  - **Finding:** *To further accomplish the goals of the ISE as stated in IRTPA and Presidential Guidelines,*[10] *PM-ISE and its mission partners are exploring new mechanisms for enhancing collaboration and coordination between federal, state, local, tribal, and private sector entities. Although significant information sharing relationships have been institutionalized between these organizations, it is anticipated that a dedicated forum is needed to fully bring the accountability, oversight, and governance capabilities of the ISE to bear on lingering information sharing gaps between federal agencies and non-federal partners by enhancing understanding of one another's missions, the respective policy and legal hurdles each faces, and the benefits each will realize through senior-level interaction.*

[10] Guideline 2 – *Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector*.

INTRODUCTION

This Report examines the extent to which IRTPA's terrorism information sharing mandate is being implemented by agencies that possess or use terrorism-related information, operate systems within the Information Sharing Environment (ISE), or otherwise participate in the ISE.[11] The Report describes how agencies have fared against established performance measures, and highlights accomplishments, including illustrative examples of ISE progress toward responsible information sharing goals derived from IRTPA, Presidential guidelines and requirements, and the National Strategy for Information Sharing. It also covers PM-ISE's reporting responsibilities pertaining to the Interagency Threat Assessment and Coordination Group (ITACG).[12] PM-ISE also supports aspects of information sharing in other domains, such as the maritime domain, primarily to promote cross-domain information integration in the pursuit of our vision of strengthening national security through responsible information sharing. The activities and accomplishments of ISE departments and agencies are bringing us ever closer to achieving this vision.

SCOPE

The ISE is a partnership for sharing and safeguarding terrorism-related information between the law enforcement, public safety, defense, intelligence, homeland security, and diplomatic communities. It extends to all levels of government – federal, state, local, tribal, and territorial; and incorporates private sector partners and international allies. This 2012 ISE Annual Report to the Congress incorporates input from mission partners[13], representing each of these communities, and uses their initiatives and PM-ISE's management activities to provide a cohesive narrative on the state of and progress of terrorism-related information[14] sharing and safeguarding, including its impact on our collective ability to secure the nation and our national interests.

Throughout the Report narratives, performance data, and success stories provide not only a progress report on the maturity and progress of our responsible information sharing initiatives, but also tell the story of how progress has impacted the ISE agencies' missions[vii]. All relevant activities over the past year are mapped to IRTPA requirements in the form of endnotes. This story is continued in the interludes found between sections that further demonstrate how agencies are implementing the ISE, or leveraging ISE technology standards and common processes to improve responsible information sharing outside of the counterterrorism domain.

To accurately inventory progress that encompasses terrorism-related information sharing, a classified supplement will be sent to the Congress under separate cover.

PRIMARY SOURCES

In order to provide the best and most comprehensive assessment of ISE initiatives, we source data both internally, from PM-ISE divisions and coordinators who are working daily with agencies in the pursuit of responsible information sharing goals, and directly from the agencies that are executing the initiatives. Our agency data comes from responses to the annual ISE Performance Assessment Questionnaire (ISE PAQ), other

[11] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, P.L. 108-458 (December 17, 2004), Sec. 1016(h) and (i).
[12] 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).
[13] IRTPA Section 1016 (i)(4).
[14] As defined in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, P.L. 108-458 (December 17, 2004), Sec. 1016(a)(5).

direct agency input[15], and from the Information Sharing and Access Interagency Policy Committee (ISA IPC) subcommittees and working groups.

[15] IRPTA Section 1016(i)(4).

SECTION 1:
MATURING INFORMATION SHARING ACROSS THE ISE

This section of the Report highlights important initiatives for accessing, retaining, using, sharing, and safeguarding timely and actionable information across the five communities: homeland security, law enforcement, intelligence, defense, and international. It surveys the extent to which FSLT agencies are participating in the ISE; the extent to which private sector data, including information from owners and operators of critical infrastructure, is being incorporated into the ISE; and the extent to which individuals and entities outside the government are receiving information through the ISE.[viii]

The following list is a summary of specific actions taken over the past year to mature information sharing across the ISE. These activities are discussed in further detail below:

- DHS and fusion center stakeholders developed and conducted a repeatable annual assessment process, and DHS led gap-mitigation efforts to assist fusion centers in fully achieving critical operational capabilities and enabling capabilities;
- DHS and fusion center stakeholders completed an assessment of the total cost incurred in operating the National Network of Fusion Centers (National Network);
- NSI Program Management Office (PMO) expanded the NSI by implementing standards, policies, and processes across the National Network;
- The FBI and NSI PMO continued improvements for eGuardian and NSI Shared Space interoperability, as well as the ability to search SAR data;
- State, local, and federal agencies, as well as law enforcement associations, created a *unified approach* to the reporting and sharing of information related to suspicious activity;
- The ITACG reviewed 191 intelligence products, a 50% increase over the previous year;
- The ITACG initiated a multi-faceted Fire Service Intelligence Integration project aimed at increasing intelligence support to firefighters, and developed training to raise awareness of violent radical extremist recruitment in U.S. correctional facilities;

- The FBI deployed a Repository for Individuals of Special Concern (RISC) Rapid Search, and a Facial Recognition Pilot to help quickly assess threats associated with law enforcement encounters;
- The State of Indiana launched the Indiana Data Exchange (IDEx), a 21-agency effort that includes federal, state, and local law enforcement information sharing;
- Counterterrorism Data Layer (CTDL) now provides NCTC analysts with the ability to search, exploit, and correlate terrorism information in a single environment;
- DHS initiated HSpace, a networking and collaboration tool designed to connect members of the homeland security intelligence community operating at the SECRET classification;
- The United States and the European Union took a vital step forward in fighting terrorism and transnational threats, while protecting privacy and civil rights, through a new Passenger Name Record (PNR) agreement;
- Canada, Mexico, and the United States signed a trilateral MOU to formalize their collective intent on information sharing and interoperability, and agreed to conduct two information sharing pilot projects;
- Fusion centers in the Delmarva (Delaware, Maryland, Virginia) Peninsula region collaborated on their first public-private partnership forum to improve information sharing with the private sector;
- PM-ISE worked with the International Association of the Chiefs of Police, Global, and DoJ's Bureau of Justice Assistance (BJA) to help address critical law enforcement information sharing gaps, issues, and challenges , and as a result began a dialogue based on a white paper entitled "Reinventing the Public Safety Business Model";
- PM-ISE and the National Maritime Intelligence-Integration Office sponsored a maritime port security information sharing initiative to facilitate the integration of maritime information and intelligence collection and analysis in support of national policy; and
- PM-ISE developed, with DHS, the Centers of Analytical Excellence workshop to identify fusion centers that have developed expertise in topical areas and that benefit the National Network.

FOUNDATIONAL ISE INITIATIVES

NATIONAL NETWORK OF FUSION CENTERS

As of February 2012, 77 designated state and major urban area fusion centers comprise the National Network. State and major urban area fusion centers serve as the focal points for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and SLTT entities as well as private sector partners Agency responses to the 2012 ISE Performance Assessment Questionnaire (ISE PAQ) indicate that two-thirds of federal agencies are participating in this vital initiative; and an equal number of agencies report that they are incorporating fusion center information into their own products and services.

To date, DHS's Office of Intelligence and Analysis (I&A) has deployed nine Regional Directors, 65 Intelligence Officers, 18 Reports Officers, and two Intelligence Analysts to fusion centers, as well as the classified Homeland Secure Data Network (HSDN) to 63 fusion centers. The Federal Bureau of Investigation (FBI) has approximately 100 personnel (Special Agents and Intelligence Analysts) assigned to 55 fusion centers nationwide, 16 of which are co-located within the FBI's Joint Terrorism Task Forces (JTTF), described below, or Field Intelligence Groups (FIG). The FBI's classified computer network (FBINet) is installed in 47 fusion centers.[ix]

FUSION CENTER ASSESSMENT AND GAP MITIGATION

In 2011, DHS and fusion center stakeholders developed and conducted a repeatable annual assessment process using lessons learned from the 2010 Baseline Capabilities Assessment. The Fusion Center Assessment Program (FCAP) evaluates the maturity of the National Network, providing objective data to inform federal investments in fusion centers. The assessment program measures fusion center capabilities in four Critical Operational Capabilities (COC)—Receive; Analyze; Disseminate; and Gather—and four Enabling Capabilities (EC)—Privacy, Civil Rights, and Civil Liberties Protections; Sustainment Strategy; Communications and Outreach; and Security. In October 2011, DHS, in collaboration with interagency partners, concluded the 2011 assessment of the National Network. All 72 fusion centers that comprised the National Network as of August 2011 participated in this assessment. The results of the 2011 Assessment are captured in the 2011 National Network of Fusion Centers Final Report (Final Report). Beyond serving as the vehicle for summarizing the National Network's aggregate capabilities, the Final Report also encompasses a number of recommendations to mature and sustain National Network capabilities. The 2011 Final Report explains that the National Network has demonstrated significant progress in achieving the Critical Operational Capabilities and Enabling Capabilities.[16] Findings from the 2011 assessment include:

- 79% of fusion centers have approved plans, policies, or standard operating procedures (SOPs) for receiving federally-generated threat information, representing an 84% increase in the number of fusion centers with this capability from September 2010 to August 2011;
- 76% of fusion centers have approved plans, policies, or SOPs for assessing the local implications of time-sensitive and emerging threat information, representing a 175% increase in the number of fusion centers with this capability from September 2010 to August 2011;
- 79% of fusion centers have approved plans, policies, or SOPs governing the timely dissemination of products to customers within their area of responsibility, representing a 97% increase in the number of fusion centers with this capability from September 2010 to August 2011;
- 81% of fusion centers have documented plans, policies, or SOPs for gathering locally-generated information, or have a Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) site plan, representing a 45% increase in the number of fusion centers with this capability from September 2010 to August 2011; and
- 100% of fusion centers have a privacy policy that has been determined to be at least as comprehensive as the ISE Privacy Guidelines, representing a 260% increase in the number of fusion centers with this capability from September 2010 to August 2011.

DHS is also leading interagency gap-mitigation efforts to assist fusion centers in fully achieving and maintaining COCs, ECs, and additional priority areas. Informed by the results of the 2011 Assessment, DHS, in coordination with fusion center directors and federal interagency partners, identified some of the resources that can most effectively mitigate fusion center capability gaps, including more than 40 new or existing activities to support gap-mitigation

[16] *2011 National Network of Fusion Centers Final Report*, May 2012.

efforts in 2012. For example, DHS developed a standard mechanism for fusion centers to request access to SECRET information that might not be currently available to them on HSDN, or resident on the Secure Internet Protocol Router Network (SIPRNet).[x]

DHS will incorporate lessons learned and feedback garnered from the 2011 Assessment to continue to refine the assessment process. Future assessments will also measure the performance of the National Network to ensure that fusion center capabilities are delivering the outcome intended from collective federal and SLTT investments.

2011 FEDERAL COST INVENTORY

ISE Implementation Guidance required DHS to provide the Office of Management and Budget (OMB) and PM-ISE with an inventory of all federal funding and personnel dedicated to the National Network. In the fall of 2011, DHS and interagency partners worked through the Fusion Center Sub-Committee of the ISA IPC to complete an assessment of the total cost incurred by federal partners in support of the National Network. This activity contributes to efforts to build a long-term sustainment strategy that provides meaningful justification for resource expenditures.[xi]

The 2011 Federal Cost Inventory provided an opportunity for the Federal Government—for the first time—to capture federal departments' and agencies' investments in fusion centers in a common and consistent manner. The 2011 Federal Cost Inventory illustrates that there is a significant level of federal investment, particularly in terms of personnel and information technology that is essential to maintaining and supporting the National Network. Further, the 2011 Federal Cost Inventory provides valuable data for evaluating the compliance of departments and agencies with the Federal Resource Allocation Criteria (RAC) policy. The objective criteria and coordinated approach established by the Federal RAC policy provides guidance for ensuring that interagency partners are providing appropriate support to fusion centers, particularly in a fiscally constrained environment. Going forward, a standard annual federal cost inventory process will allow the Federal Government to analyze investments in fusion centers over time and further comply with Section 1016(h)(2)(C) of the IRTPA.[xii]

Together with data collected through the Fusion Center Assessment Program, the Federal Government will have a comprehensive picture of the national investment in fusion centers and the resulting capabilities. This will provide valuable insight into the value and impact of fusion centers and the level of investment that is necessary to fully achieve and maintain their Critical Operational Capabilities and Enabling Capabilities. This combined dataset will help federal, state, and local government partners make informed investments as they continue to mature the National Network, and to measure the return on those investments. This assessment provides a baseline against which we can measure federal investment in the future.

FUSION CENTER PARTNERSHIPS

In 2011, DHS worked with a variety of federal partners to increase awareness of fusion centers and their missions, capabilities, and resources while exploring opportunities for mutual collaboration. These efforts are highlighted below.

High Intensity Drug Trafficking Area (HIDTA) Investigative Support Centers (ISC) - DHS and the Office of National Drug Control Policy (ONDCP) continue to support national security efforts through an enhanced partnership between fusion centers and HIDTA ISCs. In 2011, DHS, ONDCP, and PM-ISE fostered dialogue and collaboration at the National Fusion Center Training Event, the Northeast Regional Intelligence Group Meeting, the annual ISC Managers/Domestic Highway Enforcement (DHE) meeting, the HIDTA/Fusion Center Coordination Strategy Session, and quarterly meetings established between DHS and ONDCP. DHS and ONDCP have also developed a series of case studies and best practices as well as a guidebook to familiarize fusion center, HIDTA, and other key

stakeholders with the core missions, functions, and distinctions between fusion centers and HIDTA ISCs. Finally, DHS provided ISC analysts with access to the Homeland Security Information Network (HSIN) and State and Local Intelligence Community of Interest (SLIC).[xiii]

Drug Enforcement Administration (DEA) - In 2011, DHS and DEA worked closely to facilitate fusion centers' access to two important DEA resources–the National Virtual Pointer System (NVPS) and the DEA Internet Connectivity Endeavor (DICE). NVPS provides access to active investigative target information through a single point of entry using an SBU network such as the Regional Information Sharing System Network (RISSNET). DICE supports queries for phone numbers, e-mail addresses, vehicle identification numbers, and other types of data, including license plate information. Additionally, DHS and DEA coordinated to provide fusion centers with access to the intelligence products posted on DEA's classified portal, which significantly expands the amount of counternarcotics intelligence information available to fusion centers.[xiv]

U.S. Attorneys' Offices - In July 2011, DHS met with the Executive Office for the United States Attorneys and United States Attorney Offices (USAO) to identify partnership opportunities between fusion centers and USAOs located across the country. In November 2011, DHS I&A issued a Memorandum to Fusion Center Directors outlining opportunities for fusion centers to forge relationships with the local Anti-terrorism Advisory Council Coordinator and local Intelligence specialists to help foster a formal mechanism for mutual collaboration.

TRIBAL INTEGRATION[xv]

Tribal law enforcement agencies are vital participants in fusion centers. Through federal government support, and in cooperation with state and local partners, tribal law enforcement personnel are integrated into several fusion centers; and tribal participation is realized through liaison programs and embedded analysts. These efforts allow fusion centers to more fully address threats and vulnerabilities in lands under complete control of Indian Country.

There continue to be some recognized gaps in tribal information sharing. PM-ISE's efforts are focused on addressing and improving some of the foundational policy, governance, relationship, and capacity issues related to tribal information sharing. While not all fusion centers allow tribal representation at this point in time, progress in this area continues.

The Washington State Fusion Center's (WSFC) Fusion Liaison Officer (FLO) program was started in December 2010 with 19 candidates from around the state. They now have 634 FLOs comprising law enforcement, fire, critical infrastructure/key resources, military, and tribal personnel. The FLO program is continuing to grow, and they expect to have more than 800 officers by the end of the year. WSFC's goal is 100% tribal representation.

JOINT PRODUCT DEVELOPMENT ASSISTANCE PROGRAM

Through its Joint Product Development Assistance Program, DHS is facilitating the development of joint intelligence products with and between fusion centers that address cross-jurisdictional security issues such as border-related crime, transnational organized crime, critical infrastructure assessments, and other strategic issues of mutual concern. In addition to fostering increased collaboration between federal partners and fusion center analysts, the program promotes the incorporation of SAR into jointly-produced intelligence products.[xvi]

FUSION CENTERS OF ANALYTICAL EXCELLENCE

While it remains important for fusion centers to achieve and maintain a baseline level of capabilities, there is also interest at the National Fusion Center Association (NFCA), which represents all state, local, and tribal personnel working within fusion centers, in acknowledging the value that individual fusion centers can provide, based on their unique areas of expertise and specialization. The NFCA recognizes specialization among fusion centers and

seeks to leverage that specialized expertise to strengthen the larger network and acknowledge qualified centers as "Centers of Analytical Excellence." This concept has been the subject of significant research over the last 12 months by the NFCA, in coordination with its federal partners, and is currently in the planning phase. The concept of acknowledging a fusion center as a Center of Analytical Excellence will result in the certification of centers demonstrating excellence in a particular subject area of analytical methodology or expertise in a defined area. These centers will then share their analytical competencies across the National Network for the purpose of strengthening the collective enterprise of fusion centers.

FUSION CENTERS IN ACTION

The value of fusion centers is best communicated by sharing the successes they have had in protecting their state, local, tribal, and territorial communities, informing decision making, and enhancing information sharing activities between and amongst law enforcement and homeland security officials at all levels of government. These successes cover a broad range of efforts, spanning the all-crimes and all-hazards mission areas.

Fusion Center and Terrorism Liaison Officers Instrumental in the Arrest of an Attempted Bombing Suspect - In June 2011, the Lakewood (Colorado) Police Department received information that an individual had placed two improvised explosive devices at a bookstore in a local mall. The JTTF and Alcohol, Tobacco, and Firearms Agents responding to the alert began collecting information, which they passed on to the Colorado Information Analysis Center (CIAC), which in turn relayed the information to its statewide Terrorism Liaison Officer (TLO) network. Within minutes, the CIAC received vital information from two TLOs linking a suspect to the attempted bombing. The CIAC passed this information to the JTTF, and the suspect is being held on charges stemming from the incident.[xvii]

The FBI, a Fusion Center, and the Public Partner to Apprehend Armed and Dangerous Fugitives - On August 9, 2011, after the sighting of three dangerous fugitives, the FBI Denver Division sought assistance from the CIAC to issue a "Be On the Look-Out" alert for immediate distribution to Colorado law enforcement and the National Network. The FBI also released photographs of the fugitives along with a description of their vehicle, and asked the public to call 911 if anyone spotted the trio. On August 10, a citizen's tip to local law enforcement led to the pursuit and apprehension of these fugitives by the Colorado State Patrol and local law enforcement authorities.[xviii]

Fusion Center Provides Critical Information to International and Federal Partners, Contributing to the Arrest of Armed Suspects - In October 2011 the Alaska Information and Analysis Center (AKIAC), in coordination with the Alaska JTTF, issued an Officer Safety Bulletin on two potentially violent individuals believed to be illegally armed and departing for Canada. The AKIAC used liaisons with the Royal Canadian Mounted Police and U.S. Customs and Border Protection (CBP) to ensure that the Canadian Border Security Agency (CBSA) received this information and was on alert. As a result, CBSA conducted a high-risk inspection at a port of entry, and discovered a weapon. The suspect was denied entry into Canada, turned around, and was then stopped at the CBP checkpoint, where he was arrested by Alaska State Troopers.[xix]

NATIONWIDE SUSPICIOUS ACTIVITY REPORTING (SAR) INITIATIVE (NSI)

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a collaborative effort led by the DoJ Bureau of Justice Assistance (BJA) in partnership with DHS, the FBI, and SLTT law enforcement partners. NSI provides another tool to help prevent terrorism and other related criminal activity by creating a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. NSI is an important component of DHS's "If You See Something, Say Something™" campaign, a simple and effective program to raise public awareness of the indicators

of terrorism and terrorism-related crime that emphasizes the importance of reporting suspicious activity to the proper local law enforcement authorities.

IMPLEMENTING THE NSI

Over the past 12 months, the NSI Program Management Office (PMO) has implemented the standards, policies, and processes of the NSI across the National Network.[xx] As of March 2012, 68 fusion centers have the capability to contribute and share SAR information using the Shared Space, and all 77 fusion centers have the capability to contribute to SAR through the Shared Space and/or eGuardian platforms. The NSI, through the National Network, now reaches more than 14,000 law enforcement agencies in 46 states and the District of Columbia. Outreach efforts are underway to implement the final participating sites into the NSI process, with an expected completion date of September 2012.

In addition, the SAR Subcommittee of the ISA IPC met six times in 2011 to focus on expanding support to SAR at the federal level, and to recommend priorities for evolving the NSI. At the federal level, 72% of respondents to the 2012 ISE PAQ reported some level of participation in the NSI, and 83% of agencies reported forwarding validated SARs to the NSI.

As the NSI expands to more sites, there has been a commensurate increase in users, in the use of NSI Federated Search,[17] and in the number of SARs that are available to users. Over the last 12 months, the number of SARs available to Federated Search users increased to more than 17,000 – a 36% increase over the previous year. Users have conducted more than 43,000 searches against these SARs, which are available in the shared spaces.

A UNIFIED MESSAGE FOR SAR

The Unified Message document, issued in April 2012, was created to help clarify a unified approach to the process of reporting and sharing information related to suspicious activity.

Every agency connected to the NSI mission, from the Federal Government to local law enforcement, must work together to share information that may help prevent the next attack, while continuing to ensure the protection of privacy and civil rights and civil liberties. To help enhance existing partnerships and information sharing, the International Association of Chiefs of Police (IACP) hosted a series of meetings in the summer of 2011, with representatives from state, local, and federal agencies, as well as law enforcement associations, to create a unified approach to the reporting and sharing of information related to suspicious activity. As a result of these meetings, federal, state, and local partners created "A Call to Action: A Unified Message Regarding the Need to Support Suspicious Activity Reporting and Training," a document which: 1) emphasizes the importance of reporting suspicious activities; 2) stresses the importance of SAR training and tells agencies where they can receive it; 3) discusses the role of fusion centers, FBI FIGs, and JTTFs in analyzing and investigating SAR; and 4) encourages agencies at all levels – SLTT – to work with the DHS on its "If You See Something Say Something™" campaign.[18]

ANALYSIS OF SAR DATA

Providing analytical context to SAR data is an essential element of the NSI's overall mission.[xxi] As the NSI and fusion centers mature, analysts are beginning to create relevant products that provide situational awareness for their mutual stakeholders.

[17] NSI Federated Search permits users to search across a federated environment, using a standardized data format.
[18] http://nsi.ncirc.gov/documents/A_Call_to_Action.pdf

For example, DHS has begun to integrate SAR information into the Roll Call Release (RCR) product. Early in 2012, DHS started a series of RCRs that address the NSI-defined indicators and behaviors of potential terrorist preoperational attack planning. These products are focused on the national level and provide actual examples of SARs that illustrate these indicators and behaviors.

Additionally, state and major urban area fusion centers are developing and distributing products that integrate SAR information specific to their jurisdictions. The Northern California Regional Intelligence Center has a bulletin—disseminated weekly to law enforcement in the area—that highlights current SAR information. The New Jersey Regional Operations Intelligence Center is distributing a series of quarterly reports designed to identify SAR trends in the state. This report includes a summary of SAR information received during the quarter, breaks out the information into graphs identifying the most current trends, and offers suggestions for the areas of concern on which law enforcement may want to focus their resources. And the Nevada Threat Analysis Center (NTAC) has developed a monthly bulletin that contains current regional and local information intended for Nevada's TLO network. This bulletin includes a list of priority SAR information areas that help TLOs better identify information that may help supplement the analytical products developed and distributed by the NTAC.

EGUARDIAN AND NSI SHARED SPACE INTEROPERABILITY

The FBI's eGuardian system was developed to help meet the challenges of collecting and sharing terrorism-related activities, e.g. tips and leads, amongst law enforcement agencies across various jurisdictions. eGuardian allows law enforcement agencies to combine new SARs with existing (legacy) SAR reporting systems to form a single information repository accessible to thousands of law enforcement personnel. The information captured in eGuardian is migrated to the FBI's internal Guardian system, where it is assigned to the appropriate JTTF for any further investigative action.

The FBI and NSI PMO have also worked closely together to ensure eGuardian and NSI Shared Space interoperability. Today, users can enter a SAR into eGuardian or the Shared Space, and the SAR is accessible by users of either system. Continued improvements over the past year have addressed system compatibility, record retention policies, data collection synchronization, and unified outreach to fusion centers regarding SAR reporting. Of note, 82% of respondents to the 2012 ISE PAQ reported using eGuardian.[xxii]

The FBI's classified Guardian system has implemented record retention time frames that closely mirror those of 28 CFR Part 23,[19] the policy that governs the retention policies for state and major urban area fusion centers. In addition, the NSI has taken steps to facilitate the automated migration of SAR entries from the Shared Space to eGuardian to ensure receipt by JTTFs. The value of JTTFs receiving SAR data is clear: as of April 2012, more than 700 investigations have been initiated by the FBI, based on information received from eGuardian.[xxiii]

NSI TECHNOLOGY IMPROVEMENTS

The NSI PMO made several improvements to the NSI Federated Search over the past year, as highlighted below, and has also provided resources for users to turn to for assistance if needed. The State Department is also upgrading its Security Incident Management and Analysis System (SIMAS) to help integrate with the NSI. SIMAS is scheduled for completion by the end of FY2012.

Single Line Search - Similar to a "Google" search, the NSI Federated Search tool provides users with the ability to enter search parameters in an unstructured entry called the Single Line Search. In addition, the Single Line Search

[19] 28 Code of Federal Regulations Part 23 (28 CFR Part 23) is a federal guideline for law enforcement agencies that operate federally funded, multijurisdictional criminal intelligence systems.

provides broader search parameters than previously available on the Advanced NSI Search tool. This will help analysts find the information they need in a more efficient, expedient manner.[xxiv]

Subscription Service - NSI Federated Search users can now create and save queries, also known as a subscription service. These queries can be saved to run on a recurring basis, identify other users searching the same criteria, and identify when a new SAR is submitted that contains the information saved in the data query.[xxv]

NSI Analytics – To assist analysts in linking behaviors and activities together with current threat information, the NSI PMO developed the NSI Analytical Tool, which will be released in 2012. This tool will allow users to review, search, and compare SAR information for individual fusion centers, or across multiple fusion centers, using user-defined search.[xxvi]

Shared Space - eGuardian Web Service – The NSI PMO and FBI eGuardian staff implemented a capability to allow fusion centers to electronically push SAR from fusion centers' local NSI common box to the eGuardian system. This migration utilizes the eGuardian Web service, which not only enables the push but also provides an eGuardian ID number for future reference.[xxvii]

Help Desk - The NSI help desk and knowledge base is a secure site that allows users to: find information regarding Frequently Asked Questions (FAQs); submit additional FAQs to the database; find helpful links and points of contact; view training documents and podcasts; and request additional assistance from the help desk.[xxviii]

EGUARDIAN TECHNOLOGY IMPROVEMENTS

To date, 53 federal agencies have active eGuardian accounts, and use the FBI's eGuardian system to share terrorism-related information. The FBI has made the following improvements to eGuardian over the past year:

Web Services Interface – Agencies can now use their own incident management systems to electronically submit terrorism-related incidents to eGuardian.

Enhanced Tools to Share ISE SAR Function Standard-Compliant Incident Information - When entering an incident in e-Guardian, the author can now indicate whether it is compliant with the ISE SAR standard. Indicating "No" means that the incident will be shared with the FBI, but not with the ISE Shared Space. Selecting "Yes" means the incident will be shared with both the FBI and the ISE Shared Space.

Geospatial Referencing - The eGuardian home page now displays a dynamic map that shows the locations of incidents. This is a first geospatial release, which sets a baseline. Future releases will provide more world-wide map coverage and reference tools.

Enhanced Tools to Share Incident Information between Fusion Centers and FBI JTTF - Fusion Center approvers now have a new workflow button labeled "Report." "Report" moves an incident into the FBI JTTF, but does not publish the incident to all of eGuardian; nor does it publish the incident to the ISE Shared Space. This function allows incident information that does not yet meet the ISE SAR Functional Standard to be shared with a limited audience for the purposes of further analysis and/or investigation.

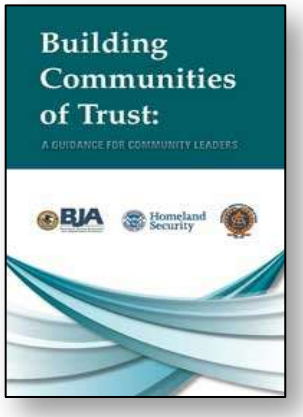
DEPARTMENT OF TRANSPORTATION ESTABLISHES DEPARTMENT-WIDE SAR PROCESS

In support of the NSI, the Department of Transportation (DoT) recently established a department-wide SAR entry, vetting, and cataloging process. DoT employees in Washington, DC and across the country can now access a convenient online form to report suspicious activity, and trained DoT analysts can vet SARs for inclusion in the NSI Federated Search. By aiding in the detection of terrorism-related suspicious activities and sharing SARs with NSI

partners, DoT can contribute to a unified approach to national security while also enhancing the safety and security of the national transportation system, a core DoT mission.[xxix]

BUILDING COMMUNITIES OF TRUST: A GUIDANCE FOR COMMUNITY LEADERS

Law enforcement agencies have long recognized the need to develop trusting relationships with the communities they serve. NSI's Building Communities of Trust (BCOT) initiative is designed to help develop these relationships by bringing together local law enforcement leaders, U.S. Attorney's Offices, fusion centers, and community representatives to engage in open dialogue about how these groups can work together. In 2012, *Building Communities of Trust: A Guidance for Community Leaders*[20] was developed in partnership with BJA and DHS to help law enforcement empower local partners to help keep communities safe from threats of crime and terrorism. The guide includes:



- Information about the Nationwide Suspicious Activity Reporting Initiative;
- Tips to help community leaders be more proactive in working with law enforcement; and
- Links to helpful resources for both law enforcement and community leaders.

This guide is intended as a companion to the *Guidance for Building Communities of Trust,* which was released in the fall of 2010. The strategies discussed in the new guide also complement national strategic goals for empowering local partners to keep their communities safe from threats of violent extremism. The BCOT initiative has been highlighted as a best practice in the President's strategy for preventing violent extremism, and was also featured in DHS's 2011 Countering Violent Extremism Workshop.[xxx]

The White House Community Partnerships Interagency Policy Committee (IPC) has reached out to PM-ISE in order to leverage the ISE's tools and techniques for engaging the private sector, and state and local communities. The Community Partnerships IPC is particularly interested in the possibility of leveraging the BCOT initiative and the ISE "Building Blocks," discussed in Section 6 of this Report, to assist them with their vital efforts.

INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP (ITACG)

The Interagency Threat Assessment and Coordination Group (ITACG) integrates, analyzes, and assists in the dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction (WMD) information. By working closely with the National Counterterrorim Center (NCTC), DHS, and FBI analysts, the ITACG ensures that shared information is both timely and relevant, and that it is transformed into situational awareness products for public safety officials, thereby enhancing their capabilities for quickly assessing and effectively responding to suspected terrorist activities.[xxxi]

[20] http://nsi.ncirc.gov/documents/BCOT_Final.pdf

In the five years since the establishment of the ITACG, the maturity, trust, and integrity of the program have grown. The ITACG continues to play an important role in institutionalizing the process of information sharing between the Federal Government and SLTT partners by assisting federal partners in interpreting and analyzing intelligence intended for dissemination to frontline law enforcement, public safety, and homeland security personnel. Analysis of the 2011 NCTC-led Counterterrorism Customer Satisfaction Survey of Intelligence Community Products and Services data provided by SLTT on ITACG products revealed that 91% of SLTT customers rate their satisfaction with the usefulness, timeliness, and responsiveness of ITACG Roll Call Release products as "Very Useful" to "Somewhat Useful." ITACG uses feedback provided by SLTTPS customers to adjust its products to better meet their needs; the ITACG has made significant headway in the production arena, as well as through the implementation of numerous projects and key initiatives that promote and help sustain a strong information sharing effort. While the ITACG has been rated effective in enhancing the sharing of intelligence with SLTTPS partners through established mechanisms within DHS and the FBI, a mechanism to fully assess the ITACG's impact beyond customer surveys does not exist. The primary source of feedback on ITACG performance is customer satisfaction data collected by DHS and NCTC, which provides only an indirect measure of performance. PM-ISE acknowledges that work has been done over the last year to further develop an ITACG performance framework. However, without the development of a comprehensive performance framework, including specific performance measures associated with the ITACG's mission; a repeatable process to collect data against these performance measures; and a dedicated effort to analyze this data, PM-ISE cannot determine if ITACG has achieved its desired end state.[21]

A DAY IN THE LIFE OF THE ITACG

Daily, ITACG detailees review reporting on classified information systems and work with the embedded analysts to nominate topics for inclusion in NCTC's daily Terrorism Summary, which is available to State, local, and tribal homeland security and law enforcement partners on the Secret network.

Detailees review a wide range of IC products, including IC component production, with a keen eye toward products with potential implications for first responders. They propose topics for production, conduct research, and write products, including the Roll Call Release.

They also nominate the downgrading of intelligence reports in their entirety, or request that separate, tailored products be produced for their mission partners.

Detailees also attend the morning secure video teleconference SVTC, attended by both White House and interagency personnel; the daily National Joint Terrorism Task Force briefing; and shift turnovers for personnel on watch in the NCTC Operations Center.

They routinely coordinate on draft intelligence products, produced by DHS's Office of Intelligence Analysis and the FBI's National Security Branch, which are sent to the ITACG detail as part of the regular production cycle.

Finally, detailees are assigned projects that contribute to federal, state, local, and tribal information that best leverage their expertise in law enforcement, fire safety, public health, and intelligence professionals.

THE ITACG DETAIL'S ACCESS TO INFORMATION

In April 2012, PM-ISE staff interviewed several members of the ITACG Detail and determined that the Detailees continue to have appropriate access to relevant information at the NCTC. The primary sources of this information include direct access to classified and unclassified information systems; secure video teleconferences; briefings; "shift" turnovers; and embedded federal analysts who are assigned to support the Detail. For example, detailees have access to NCTC CURRENT, the premier classified resource for counterterrorism (CT) reporting and analysis throughout the Intelligence Community (IC), as well as the CIA's Trident system, the primary research and analysis environment for CIA Analysts. One detailee noted that his access to information at NCTC "exceeded every expectation," and that the positioning of the Detail at NCTC "opens doors throughout the IC." The ability of the detailees to conduct face-to-face meetings with federal analysts

[21] 6 USC 124K(c) requires PM-ISE to monitor the ITACG and report annually on progress, including an assessment of the detailees' access to information at NCTC. The law requires DHS to provide ITACG performance data to PM-ISE for inclusion in its annual report to Congress.

enhances the IC's ability to prepare versions of intelligence products that are unclassified, or classified at the lowest possible level, for dissemination to the state, local, and tribal homeland security and law enforcement partners who are helping keep Americans safe from terrorist attacks.[xxxii]

ITACG DETAIL PERFORMANCE

The ITACG Detail facilitates information sharing to SLTTPS partners through the review and coordination of federally-coordinated intelligence products. *Since June 2011, the Detail has reviewed 191 intelligence products, representing a 50% increase over the previous year*. During this same period, the ITACG Detail nominated 1,380 articles for inclusion in NCTC's daily Terrorism Summary, over half of which were accepted. The Detail originated 12 Roll Call Releases (fewer than half from the previous year), and submitted 30 requests for product classification downgrade. Seven of these requests were approved; six were denied due to source sensitivity; and seventeen are pending.[xxxiii]

ITACG Detailees spend several days a week, on a rotational basis, working with DHS I&A analysts. This direct interaction helps bring a state or local first-responder perspective into the initial phases of intelligence product development. The Detail is also currently assisting DHS I&A in its endeavor to improve the flow of timely and relevant intelligence information to and from fusion centers, JTTFs, and FBI field offices nationwide. One important aspect of this effort is to create meaningful dialogue with SLTTPS partners, aimed at providing better, more timely, and useful information to the field. The Detail's role in this endeavor is to serve as first-responder subject matter experts to DHS I&A analysts.

DHS has leveraged information collected by I&A and NCTC customer assurance components to provide customer feedback on products the ITACG Detail is involved in producing. DHS I&A produces an annual report to Congress that documents voluntary consumer feedback on DHS intelligence and other information products, as required by the Implementing Recommendations of the 9/11 Commission Act of 2007.[22]

ITACG PROJECTS

Over the course of the past year, the ITACG Detail has worked on several key initiatives to help increase information sharing across the FSLT enterprise, and to fill known information sharing gaps. In support of the National Preparedness Goal of Presidential Policy Directive 8, the Detail is participating in the development of the National Prevention Framework, which will describe roles and responsibilities, define coordinating structures and other key operational planning considerations, and provide information that SLTT governments and private sector partners can use to develop, inform, or revise prevention efforts.

The Detail initiated a multi-faceted Fire Service Intelligence Integration project aimed at increasing intelligence support to firefighters. The Detail developed terrorism awareness and fire service training for the National Fire Academy; conducted a nationwide Fire Service survey to determine the extent to which intelligence is reaching fire departments; based on the results of the Fire Service survey, promoted familiarity among firefighters with the ITACG Roll Call Release; and developed a new product, Fireline, specifically intended to meet the unique intelligence needs of the Fire Service. The Detail is supporting existing DHS I&A State and Local Program Office (SLPO) efforts to increase fire service engagement with fusion centers.[xxxiv]

To address awareness of violent radical extremist recruitment in U.S. correctional facilities, the Detail developed a training course titled *Violent Radical Extremism in the Correctional Environment,* with the support of and input from various members of the IC and state and local subject matter experts. The course was piloted in March 2012

[22] *2011 Report to Congress Feedback from State, Local, Tribal, and Private Sector Consumers*, March 14, 2012.

at the Maryland Public Safety and Corrections Training Facility. The Detail incorporated feedback from this pilot to revise the course, and has submitted the course for DHS review.

Finally, in collaboration with NCTC, DHS, and the FBI, the Detail is piloting a proposal to create an unclassified "For Official Use Only" product that aggregates terrorism-related reporting from across the IC, as well as the Homeland Security Intelligence Enterprise.

LAW ENFORCEMENT INFORMATION SHARING

JOINT TERRORISM TASK FORCES (JTTF)

In order to maximize the dissemination of the right information to the right people in a timely and responsible manner, regardless of organizational or physical boundaries, ISE partners adopt a whole-of-government approach. Joint Terrorism Task Forces (JTTF) are dedicated to sharing information among trusted partners to investigate terrorism and coordinate counterterrorism (CT) efforts across the United States. JTTFs consist of squads of highly-trained investigators, analysts, operators, linguists, and other specialists from FSLT law enforcement organizations and federal intelligence agencies. The FBI has increased the number of JTTFs from 35 in 2001 to 103 today—one in each of the 56 Field Offices, and 47 more in Resident Agencies across the country. FBI and other federal partners—including the Office of the Director of National Intelligence (ODNI), the Department of Defense (DoD), and the Department of Homeland Security (DHS)—also share threat information through the JTTFs.

According to the 2012 ISE PAQ, 83% of respondents reported participating with JTTFs. For example, the Internal Revenue Service has more than 62 Special Agents embedded in JTTFs across the country, and DoD has approximately 90 detailees that support 56 FBI JTTFs throughout the United States. In August 2011, DoD and DoJ adopted an overarching MOU to promote standardized and controlled information sharing. This collaboration plays an important role in protecting U.S. military communities.[23] The interagency make-up of the JTTFs expands both the volume and the nature of collection capabilities.

Having personnel from multiple agencies co-located at the JTTF dramatically improves communication, coordination, and cooperation among agencies, which leads to a more efficient and effective response to terrorist threats. Task Force Officers provide instant access to government agencies' investigative databases, which ensures timely and efficient vetting of investigative leads. A single National Joint Terrorism Task Force (NJTTF) manages JTTFs around the country and provides a venue for collaboration with IC personnel to exchange information, analyze data, and plan CT strategies. The 80 officers, agents, and analysts who make up the NJTTF come from 45 different agencies from the law enforcement, intelligence, homeland security, defense, diplomatic, and public safety sectors.[xxxv]

The 2011 FBI Information Sharing Report details the role of JTTFs in optimizing information sharing among ISE partners to enable decision advantage and discusses other key FBI initiatives aimed at maximizing and integrating information sharing capabilities while safeguarding this information against malicious insiders.[24]

[23] DHS FEMA National Preparedness Report, March 30, 2012.
[24] http://www.fbi.gov/stats-services/publications/national-information sharing-strategy-1/information sharing-report-2011/view

NEXT GENERATION IDENTIFICATION SYSTEM

The Next Generation Identification System (NGI) is incrementally replacing the FBI's existing Integrated Automated Fingerprint Identification System, in service since July 1999. 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. NGI's Repository for Individuals of Special Concern (RISC) Rapid Search, deployed in August 2011, allows officers on the street to use a mobile identification device to rapidly search a national repository of 1.2 million fingerprint records to quickly assess the threat level of any subject encountered during their normal law enforcement activities, receiving a response within seconds. Currently more than 500 agencies in eight states use the RISC service on their mobile identification devices to securely transmit "live" fingerprints from the field to the RISC for a rapid search.[xxxvi]

NGI has also recently deployed the Facial Recognition Pilot, affording participating law enforcement agencies access to a national gallery of more than 12 million legally collected mug-shot photos to be searched in aid of investigations. This enhancement to NGI was initially assessed for privacy purposes in a privacy impact assessment that was published in 2008, and is on the FBI's website.[25] Currently, participation is limited to agencies with existing facial recognition systems, but later this summer the FBI will deploy the Universal Face Workstation software, a free-of-charge client application that will provide users with the tools for conducting and managing facial/photo searches with a minimal resource investment. The full deployment of the NGI face capability is scheduled for the summer of 2014, but the pilot will provide valuable operational information and feedback to ensure that the full deployment provides our contributors with the best service possible. The privacy implications of the pilot have been evaluated in a privacy threshold analysis, and full deployment of the NGI face capability will be preceded by the publication of a privacy impact assessment addressing the privacy risks and mitigations of this technology. Like the RISC pilot before it, the FBI anticipates that many success stories will be captured from the use of this new investigative service.[xxxvii]

THE INTERNATIONAL ASSOCIATION OF THE CHIEFS OF POLICE AND THE ISE

The International Association of Chiefs of Police (IACP) has established itself as the preeminent voice for over 20,000 law enforcement executives in over 100 different countries. Since its inception in 1893, the IACP has assumed a leadership role on a vast array of issues facing law enforcement, but its impact on the disciplines of criminal intelligence and information sharing is unsurpassed.

The landmark IACP 2002 Criminal Intelligence Sharing Summit of law enforcement executives and intelligence experts from across the country produced a roadmap for the future of law enforcement information sharing. A decade ago they formally engaged the issues of capacity building, technology, standards, guidelines, intelligence-sharing barriers and training that addressed important legal and civil rights that guide all criminal intelligence gathering and sharing processes.

The IACP leadership in information sharing has continued in earnest over the years, with their involvement in the creation of virtually every major committee, policy, strategy, and initiative undertaken in our country. This past year proved no different as IACP partnered with numerous federal agencies to ensure that programs such as the Unified Messaging for the NSI, Suspicious Activity Reporting Training for Front Line Officers, Fusion Center support, N-DEx, Building Communities of Trust (BCOT) and the Reinventing the Public Safety Business Model Concept Paper were efficiently and professionally delivered to police agencies of all sizes.

TRANSFORMING OUR NATION'S JUSTICE AND PUBLIC SAFETY INFORMATION SHARING BUSINESS MODEL

In 2011, the PM-ISE undertook an initiative to assist the law enforcement community in addressing their information sharing challenges by drafting a white paper titled, "Reinventing the Public Safety Business Model." This paper examines the justice system as a whole and suggests strategic ways to fundamentally improve how the enterprise collects, shares, and uses information to support, transform, and enhance public safety information-sharing capabilities. It surmises that significant cost savings could be

[25] See http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

realized through consolidation, regionalization, and reuse of open standards and trusted IT platforms. A key message in the paper was that SLT law enforcement should not expect continued funding at current levels from the Federal Government. Therefore, significant changes to their business models are needed.

PM-ISE facilitated meetings with key stakeholders, including the IACP, specifically through their Criminal Justice Information Systems (CJIS) Committee at its mid-year meeting. With the Committee's support for the undertaking (including recommendations for how to strengthen the effort), at their 2011 annual conference, in an unprecedented resolution, the IACP adopted the concepts set forth in the paper and joined the PM-ISE in an effort to turn the ideas set forth in the paper into a reality.

PM-ISE also reached out to the Bureau of Justice Assistance (BJA), a component of DoJ's Office of Justice Programs, which has the statutory responsibility of supporting the needs of SLT law enforcement agencies and improving local justice systems. Together, PM-ISE and BJA relied on the solid input and critical partnership of all of the major national SLT justice organizations involved in Global to further develop the "Reinventing Paper." As a result of PM-ISE's partnership with BJA, and drawing on the prior recommendations and the input of Global, a major review and expansion of the paper was completed, resulting in a new paper titled "Transforming Our Nation's Justice and Public Safety Information Sharing Business Model." It is anticipated that BJA, with the broad input of the justice community, may consider the specific issues identified in the paper that are ripe for solutions that may aid BJA in meeting its responsibilities for improving state, local, and tribal justice systems.[xxxviii]

INTERNATIONAL JUSTICE INFORMATION SHARING

The International Justice and Public Safety Network (Nlets) and the International Criminal Police Organization (INTERPOL), leveraging Global-supported solutions, have devised a secure means for electronically exchanging critical information between U.S. and INTERPOL databases. The Nlets/INTERPOL justice-sharing capability, which uses standard data models, including NIEM, now connects more than 18,000 domestic law enforcement agencies to the INTERPOL database in Lyon, France, and is available to all states – with 33 states having implemented direct data exchange as of June 2012. Using NIEM and other standard data models to automate this capability results in near real-time queries of rich databases and mitigates potentially suboptimal manual searches. The Nlets/INTERPOL exchange immediately enhances officer safety and allows them to be more effective on the roadside or in an investigation.

INDIANA DATA EXCHANGE

The Indiana Data Exchange (IDEx), a 21-agency effort that includes federal, state, and local association participation, launched as a proof-of-concept in August 2011 under the Indiana Department of Homeland Security's leadership. This initiative seeks to connect data from disparate justice and public safety systems for the purpose of enhanced decision making and increased public safety, leveraging prior investments. IDEx is an example of how states can leverage federal grant funding to initiate projects that will result in both immediate and long-term cost savings and efficiencies.

INTELLIGENCE INFORMATION SHARING

INTELLIGENCE COMMUNITY (IC) IT ENTERPRISE TRANSFORMATION

The 9/11 Commission recommended that the IC solve the legal, policy, and technical issues across agencies to create a "trusted information network." The ODNI is taking significant strides to enhance intelligence information sharing and interagency collaboration throughout the IC. Working closely with the "Big Five" intelligence

agencies[26], the IC Chief Information Officer (CIO) is working to implement a plan that will integrate the separate networks and IT services into a single IC IT Enterprise. While conceived out of the need to save money, the integrated IT enterprise will also significantly enhance the IC's ability to share and safeguard intelligence, including terrorism information.[xxxix]

To improve information discovery, as well as access to and retrieval of intelligence products, the IC CIO continues implementation of Intelligence Community Directive (ICD) 501-based initiatives. ICD-501 addresses mandates in IRTPA to strengthen the sharing, integration, and management of information within the IC and establishes policies for the discovery and dissemination or retrieval of intelligence and intelligence-related information produced by the IC.[27] According to the 2012 ISE PAQ, each intelligence component reported that ICD 501 implementation is proceeding as planned. For example, the Marine Corps reported that ICD 501 has been fully implemented for all service-level production activities.

COUNTERTERRORISM DATA LAYER

Intelligence analysts from more than 30 agencies work inside the ODNI-led National Counterterrorism Center (NCTC), which facilitates information sharing between the IC and state, local, tribal, and private sector partners in coordination with DHS, the FBI, and other interagency partners. NCTC serves as the Federal Government's central and shared knowledge repository on known and suspected terrorists and international terror groups.

Prior to December 2009, NCTC analysts had to search for and integrate information from multiple homeland security and intelligence networks manually. Today, the Counterterrorism Data Layer (CTDL) ingests CT-related data gathered from multiple data sets and provides NCTC analysts with the ability to search, exploit, and correlate terrorism information in a single environment. Sophisticated analytical tools are in place to permit analysts to conduct advanced searches, conduct link analysis and data visualization, and triage information. These efforts are being pursued with careful consideration of legal, policy, and technical issues to protect privacy and civil liberties.[28] [xl]

HOMELAND SPACE (HSPACE)

DHS is adapting IC tools to facilitate information sharing among its diverse elements. In March 2012, DHS I&A initiated HSpace (Homeland Space), a networking and collaboration tool designed to connect members of the homeland security intelligence community operating at the SECRET classification level. HSpace is a technical replication of the ODNI's "A-Space," the social networking and collaborative environment for analysts in the Top Secret/Sensitive Compartmented Information domain. The initial HSpace pilot is limited to counterterrorism (CT) mission support. Once the pilot is completed and DHS's Office of Privacy successfully completes a Privacy Compliance Review, HSpace will be expanded to encompass the full statutory mission of DHS.[xli]

INTERNATIONAL INFORMATION SHARING

AGREEMENTS FOR THE EXCHANGE OF TERRORISM SCREENING INFORMATION WITH FOREIGN PARTNERS

Since June 2011, the State Department, with the Terrorist Screening Center (TSC) has negotiated and signed 10 agreements or arrangements to exchange terrorism screening information with select foreign partners, bringing

[26] The Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Security Agency (NSA), and the National Reconnaissance Office (NRO).

[27] http://www.dni.gov/electronic_reading_room/ICD_501.pdf

[28] Testimony of Matthew G. Olsen, Director, NCTC, before the Permanent Select Committee on Intelligence, U.S. House of Representatives, October 6, 2011.

the total number of such arrangements to 34. Through these 34 agreements, DOS and the TSC have strengthened international cooperation on the identification of Known or Suspected Terrorists (KST). These agreements have enhanced current information already contained in the TSC Terrorist Screening Database (TSDB) as well as added new identities to the Terrorist Identities Datamart Environment (TIDE) and the information provided downstream to our domestic and international screening partners. Similarly, agreements on Preventing and Combating Serious Crime, negotiated by DHS, DOJ, and the State Department have provided an important platform for sharing criminal biometric and biographic information with foreign governments.

INTERNATIONAL PASSENGER NAME RECORD (PNR) AGREEMENT

Sharing Passenger Name Record (PNR) information is essential for terrorism prevention efforts. PNR information has assisted CT officials in nearly every high-profile U.S. terrorist investigation in recent years. The European Parliament gave its consent for a new PNR agreement, and the European Council concluded the agreement with the United States in April 2012, demonstrating that the United States and the European Union are continuing to take vital steps to work together to fight terrorism. The new PNR agreement, which replaces the one that has been provisionally applied since 2007, requires airlines flying from Europe to the United States to share PNR information about all their passengers with the DHS for the purposes of "prevention, detection, investigation, and prosecution" of terrorism or other transnational crimes.[29] It also establishes a “robust data protection regime” by including strong information-safeguarding requirements.

According to the 2012 ISE PAQ, 89% of ISE agencies are integrating information from international partners into their watchlisting and screening process.

INTERNATIONAL SOURCING OF BEST PRACTICES AND INNOVATIONS

A core component of terrorism information sharing is the sourcing of ISE best practices and innovations. Over the past several years, the United States has engaged with Canada on a variety of information sharing topics, such as the National Information Exchange Model (NIEM), SAR, standards, privacy policies, and governance. This relationship has resulted in a robust information sharing framework with Canada, in which both countries benefit from the mutual exchange of information.

Recently, Canada established a Canadian version of PM-ISE, with government-wide responsibility, to oversee and facilitate the development of a Canadian ISE and to liaise and engage with ISE partners internationally. The Canadian PM-ISE reports to Canada’s Federal CIO and is housed in the Treasury Board, a Cabinet committee of the Queen's Privy Council of Canada. As Canada builds their ISE framework, they will look to U.S. ISE mission partners for lessons learned, best practices, and models for core ISE concepts, and to further joint information sharing initiatives.

NORTH AMERICAN DAY PILOT PROGRAMS

The United States, Canada, and Mexico annually participate in the North American Day conference to exchange ideas about and approaches for improving information technology, including information sharing programs, interoperability, standards, investments, and partnerships between the private and public sector.

[29] http://consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf

During the July 2011 North American Day, Canada, Mexico, and the United States signed a trilateral MOU to formalize the collective intent of the three countries to carry out cooperative activities in the area of information sharing, interoperability and exchange.

To demonstrate these capabilities, the Canadian, Mexican, and U.S. delegations agreed to conduct two pilot projects, in the areas of public safety and public health. The Public Safety pilot focuses on trilateral exchanges of information about stolen vehicles that cross borders among the three countries. The Public Health pilot focuses on exchanging aggregated health alerts concerning food-borne illness outbreaks. Although some information exchange on these topics already occurs between the three countries, it has been primarily ad-hoc and based on point-to-point interfaces. The purpose of the pilots is to demonstrate that information can be shared among the three countries in a consistent and repeatable manner, based on the NIEM processes and framework.

To enable and support similar efforts in the global health community, the Public Health team documented their processes and mapped the content of the health alert NIEM IEPD to the World Health Organization (WHO) Public Health Event of International Concern (PHEIC). The team is also planning to share their IEPD, which provides a mechanism for sharing of best practices and lessons learned that can be used for future international information exchanges with the WHO. Moving forward, the working group will continue to progress towards using this capability for real health alerts shared across borders. The working group is also documenting their process in order to provide a mechanism for the sharing of best practices and lessons learned to be used for future trilateral information exchanges.

The initial phase of the pilots will use test data, exclusive of personally identifiable information (PII), and will focus on providing a technical demonstration of the capabilities associated with adoption and use of NIEM as a basis for information exchange. The initial phase is on track to be completed by the summer of 2012, and will be discussed at the next North American Day conference in August 2012. The next phase of the pilots will aim to operationalize the exchanges, demonstrating mission value to the law enforcement and health care communities.

PRIVATE SECTOR INFORMATION SHARING[xlii]

Since the private sector owns and protects 85% of the nation's critical infrastructure, sharing threat information with private sector partners is of vital importance. In January 2012, the National Infrastructure Advisory Council (NIAC)[30] produced an intelligence information sharing report that addresses the current state of information sharing with private sector owners and operators of critical infrastructure. Based on more than 200 interviews and extensive open-source research, the NIAC uncovered a wealth of insights on this complex information sharing problem.

This bi-directional sharing is still relatively immature, leaving a large gap in public-private sector information sharing. The NIAC observed that establishing trust is essential to making public-private sector information sharing work, and that trust results when partner capabilities are understood, valued, and appropriately leveraged. To mitigate this information sharing shortfall, the NIAC made seven recommendations:

- Assert the priority of infrastructure protection and resilience in national security;
- Improve the implementation and accountability of existing authorities;
- Improve information content by leveraging partner capabilities to reduce risk;
- Improve the value of information products to industry risk-management practices;

[30] The NIAC provides the President of the United States with advice on the security and resilience of the 18 Critical Infrastructure and Key Resources (CIKR) sectors and their supporting information systems.

- Build accepted practices for timely information delivery;
- Capitalize on private sector capabilities for counterterrorism solutions; and
- Enhance fusion center capabilities as one mechanism for sharing.[31]

FUSION CENTERS AND PUBLIC-PRIVATE COLLABORATION

In line with the NIAC's recommendation, five fusion centers in the Delmarva (Delaware, Maryland, Virginia) Peninsula region collaborated on their first public-private partnership forum. Operation Delmarva is a collaborative regional effort between the Delaware Information and Analysis Center, the Virginia Fusion Center, the Maryland Coordination and Analysis Center, the New Jersey Regional Information and Operations Center (ROIC), and the Pennsylvania Criminal Intelligence Center. These fusion centers met with their private sector partners to share key information about criminal trends and methods of operation, to educate each other about the nuances of each of their disciplines or sectors, and to share best practices.

Fusion center and private-security partnerships are critical to preventing terrorism and terror-related acts. These partnerships put relevant information into the hands of people that need it, and drive operational success within public safety agencies. The ROIC relies upon its public and private sector partners to enhance its overall perspective of both hometown and homeland security. ROIC's non-law-enforcement constituents are uniquely situated to provide Critical Infrastructure and Key Resources (CIKR) perspectives that allow the ROIC to act as a force multiplier.[xliii]

IC ANALYST/PRIVATE SECTOR PARTNERS PROGRAM

The IC Analyst/Private Sector Partners Program seeks to establish collaborative partnerships among subject matter experts in the private sector and the IC to address complex issues surrounding some of our nation's most pressing challenges. In October 2011, ODNI held a summit at which joint private sector-IC analyst teams presented their findings on topics such as telecommunications, emerging technology, Southwest border security, supply chain security, and biodefense. Robert Cardillo, DDNI for Intelligence Integration (ODNI) and Caryn Wagner, Under Secretary for Intelligence & Analysis (DHS) provided opening and closing remarks, each highlighting the importance of responsible information sharing with the private sector. Beginning in 2012, DHS will serve as the executive agent for the IC Analysts/Private Sector Partners program. The IC Analyst/Private Sector Partners program is an important step toward filling the "bi-directional" information sharing gap identified by the NIAC.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION: THE DOMESTIC SECURITY ALLIANCE COUNCIL (DSAC)

The Domestic Security Alliance Council (DSAC) is a strategic partnership between the FBI, DHS, and the private sector that enhances communication and promotes the timely and effective exchange of information. Its goal is to keep the nation's critical infrastructure (such as interstate commerce and proprietary industrial information) secure and resilient. At the DSAC Annual Meeting in February 2012, FBI Director Mueller discussed current threats to the U.S. private sector and the importance of increased collaboration between the public and private sectors. Director Mueller also said that cybersecurity could replace terrorism as the FBI's number-one priority within the next couple of years, and emphasized the need for innovative approaches to case management, because issues related to cybersecurity cut across all investigative disciplines. Importantly, Director Mueller also stated that strong information sharing partnerships are a

[31] http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information sharing-final-report-01102012.pdf

critical tool, citing the National Cyber Investigative Joint Task Force as an example of a successful collaboration between the FBI, other federal agencies, state and local governments, international partners, and the private sector.[xliv]

INFORMATION SHARING AND ANALYSIS CENTERS

Information Sharing and Analysis Centers (ISAC) are trusted entities established by CIKR owners and operators to provide comprehensive sector analysis that is shared within the sector, with other sectors, with fusion centers, and with the government. ISACs take an all-hazards approach and have strong reach into their respective sectors, with many reaching over 90% penetration.

Services provided by ISACs include risk mitigation, incident response, and alert and information sharing. The goal is to provide users with accurate, actionable, and relevant information. In September 2011, the Multi-State ISAC published a Cyber Toolkit featuring educational material designed to raise cybersecurity awareness through a variety of informative and practical means. The Toolkit has been distributed to all 50 states, with customizable material that can be widely shared across government, as well as with businesses, schools, and citizens. The Toolkit is available for download at: http://www.isaccouncil.org/.

VIRTUAL BIOSECURITY CENTER[xlv]

The release of a dangerous biological agent, whether intentional, accidental, or caused by a natural outbreak, could cause millions of casualties and result in far-reaching economic impacts. Now more than ever, biosecurity awareness, public health preparedness, and education about the responsible use of science and technology are crucial components for dealing with these threats.

The Virtual Biosecurity Center (VBC) was developed in 2011 with a grant from the ODNI-led National Counter Proliferation Center and the Carnegie Corporation of New York as a "one-stop shop" for biosecurity information, education, best practices, and collaboration. VBC resources include:

- Comprehensive biosecurity news and events, and an education center and library that is updated on a continuous basis with the most current information;
- The Global Forum on Bio-risks, a collaborative online forum and tool for informing policy and empowering partnerships among professional biosecurity communities around the world;
- A calendar of global conferences to raise awareness and develop plans to address both current and future biosecurity issues;
- Education and partnership to help bridge the gap between the scientific, public health, intelligence, and law enforcement communities; and
- Translations into more than 50 languages.[32]

MULTIMODAL INFORMATION SHARING

Every year, more than 250 million tons of cargo crosses our nation's land borders or arrives at our airports and seaports, where it is then conveyed across complex maritime, air, rail, and roadway infrastructures. At the federal level, this vast and diverse environment requires authorities to share a common operating picture to enable tracking of domestic chemical, biological, radiological, and nuclear material conveyance across land, sea, and air, providing situational awareness for federal, state, local, and tribal agencies.

[32] http://virtualbiosecuritycenter.org

MARITIME SAFETY AND SECURITY INFORMATION SYSTEM

The Maritime Safety and Security Information System (MSSIS) has proven successful in building international situational-awareness partnerships by incorporating 69 sovereign nations worldwide (up from 60 in 2011) into the global maritime unclassified common operating picture. Building upon tribal integration with the NSI and the National Network, PM-ISE, the National Maritime Intelligence-Integration Office (NMIO), and departmental MDA Executive Agents of DoD, DHS, and DoT are exploring an opportunity to pilot enhanced MDA and maritime information sharing with the Great Lakes Tribal Nations community through MSSIS. This initiative could promote maritime information sharing among federal, state, local, and tribal law enforcement agencies within the Great Lakes region by receiving and sharing non-classified Automatic Identification System reports to enhance their maritime common operating picture.[xlvi]

MULTI-AGENCY MARITIME INFORMATION SHARING

NMIO and PM-ISE are sponsoring the sharing of information on maritime vessels arriving at U.S. ports between FSLT government agencies that have responsibilities for maintaining maritime security in those ports. At present these agencies do not have access to common situational-awareness information on maritime traffic in the port areas. The goal of this project is to provide the information that will enable all the agencies to see the same "picture" of traffic moving in the port, and to be aware of traffic that may have been identified as potentially dangerous or threatening.[xlvii]

MARITIME IDENTITY INTELLIGENCE ENVIRONMENT

NMIO and the Office of Naval Intelligence have partnered to extend the capability developed in the Single Integrated Look-Out (SILO) List[33] to include information on people moving in and around the maritime environment. Maritime Identity Intelligence (MI2) Environment will provide an environment for maintaining identity information on persons of interest as they move around the world. The primary focus is the maritime environment: however, the MI2 environment can be applied to persons of interest in multiple domains (land/air/maritime). This effort will support the analysis of activities that may be regarded as threatening or suspicious.

GLOBAL SUPPLY CHAIN SECURITY SUPPORT

NMIO is supporting the implementation phase of the Global Supply Chain Security work led by the National Security Staff. NMIO is leading the Situational Awareness Working Group, which supports outreach to maritime industry and international partners. The Working Group is fostering improved collaboration, information sharing, and analytic cooperation between U.S. government agencies that are focused upon cargo arriving in and departing from U.S. ports, and agencies that are focused upon cargo moving between foreign ports. The goal is to maximize the sharing of analytic methods between those two kinds of activities, and to minimize information gaps on any cargo moving around the world that eventually arrives at U.S. ports. The implementation phase is expected to be complete by the end of FY2012.[xlviii]

[33] Single Integrated Look-Out (SILO) List is a list of all vessels of domestic and international intelligence interest.

U.S. Department of Justice's Global Advisory Committee Member Agencies

- Administrative Office of the United States Courts
- American Association of Motor Vehicle Administrators
- American Correctional Association
- American Probation and Parole Association
- Association of State Correctional Administrators
- Conference of State Court Administrators
- Criminal Intelligence Coordinating Council
- Criminal Justice Information Services (CJIS) Advisory Policy Board
- Executive Office for United States Attorneys
- Federal Bureau of Investigation, CJIS Division
- International Association of Chiefs of Police (IACP)
- IACP—Division of State and Provincial Police
- IACP—Indian Country Law Enforcement Section
- INTERPOL Washington
- Major Cities Chiefs Association
- National Association for Court Management
- National Association of Attorneys General
- National Association of Counties
- National Association of State Chief Information Officers
- National Center for State Courts
- National Conference of State Legislatures
- National Council of Juvenile and Family Court Judges
- National Criminal Justice Association
- National District Attorneys Association
- National Governors Association
- Nlets—the International Justice and Public Safety Network
- National Legal Aid & Defender Association
- National Sheriffs' Association
- SEARCH, the National Consortium for Justice Information and Statistics
- U.S. Department of Homeland Security
- U.S. Department of Justice

INTERLUDE: LOCAL, STATE, TRIBAL, AND FEDERAL PARTNER IMPLEMENTATION OF THE ISE – "FROM THE BOTTOM UP"

The U.S. Department of Justice's (DoJ) Global Justice Information Sharing Initiative (Global) is an exemplar for implementing the ISE "from the bottom up." Global serves as an advisory body to the Federal Government—specifically through the U.S. Attorney General and the Assistant Attorney General Office of Justice Programs—to recommend standards-based electronic information exchange throughout the justice and public safety communities. The Global Advisory Committee (GAC) includes key personnel from local, state, tribal, federal, and international justice and public safety entities, as well as agency executives and policymakers, managers, information practitioners, and end users. GAC membership reflects the involvement of the entire justice community in information sharing.

Under the Global umbrella, the Criminal Intelligence Coordinating Council (CICC), which is made up of members representing the law enforcement and homeland security communities, is an advocate for local, state, and tribal law enforcement. The CICC supports their efforts to develop and share criminal intelligence for the purpose of promoting public safety and securing the nation, and assists DoJ in ensuring that every chief, sheriff, and local law enforcement executive understands his or her agency's role in developing and sharing information and intelligence.

While the main focus of the ISE is on terrorism and homeland-security exchanges, the need for collaboration and data sharing extends beyond terrorism-related issues to encompass all information relevant to national security and the safety of the American people. Consider the results of a study[34] by the New York State Intelligence Center, assessing major terrorist activities that have taken place against the United States since September 11, 2001. More than half of the 77 individuals involved had had contact with law enforcement prior to their participation in an attempted terrorist plot or planned attack—arrests related to drugs, weapons charges, assault and battery, robbery, and traffic violations—the types of "all crimes" incidents that drive development of many of the DoJ's Office of Justice Programs, BJA and Global-supported information sharing solutions. The reality is that many of the identified precursor activities associated with the prevention of terrorist activities are also found in routine crime prevention efforts and responses. So, by

[34] "The Vigilance Project: An Analysis of 32 Terrorism Cases Against the Homeland," New York State Intelligence Center report, December 2010, p. 13.

supporting information sharing in the broader sense—*getting the right information to the right people in the right place at the right time*[35]— the work of BJA and DoJ's Global inherently supports the ISE's mission.

That being said, while Global is committed to enhancing appropriate information exchange across the larger justice and public safety enterprise, BJA and Global's collaborative recommendations and resources, particularly those advanced by the efforts of the CICC, have in the past, and continue to specifically benefit the nation's and ISE's counterterrorism efforts. For example, the NSI—a historic partnership among state, local, tribal, and federal agencies—was often referred to as "Global in Action" by former NSI Program Management Office Director Thomas O'Reilly. By leveraging a suite of BJA- and Global-supported solutions, including the Global Federated Identity and Privilege Management (GFIPM) framework; Global services; the Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities; and the National Information Exchange Model (NIEM), the NSI SAR process establishes a unified, standards-based approach at all levels of government to gather, document, process, analyze, and share information about behavior-based suspicious activities that potentially have a nexus to terrorism. It also rigorously protects the privacy, civil rights, and civil liberties of all Americans. Furthermore, the coordinated effort of analyzing this information exists with fusion centers.

Beyond the specific recommendations offered, the GAC process itself adds credibility to and buy-in for ISE endeavors. Operating under the guidance and leadership of BJA, members of this "by practitioner, for practitioner" group represent more than 30 key organizations from across the justice landscape. Working in a collaborative and transparent manner for more than 13 years, the Committee has developed an invaluable commodity: trust. Trust in each other, trust from the constituencies represented, and trust in (and respect for) Committee recommendations from federal partners and programs, including DoJ, the FBI, ODNI, and DHS.

From the beginning, PM-ISE has consistently welcomed Global members (through GAC) as critical mission partners, realizing that the Committee's foundational principles, as well as their development and vetting processes, add great value for implementing the ISE "from the bottom up." Members of the GAC have also commended PM-ISE not only for acknowledging the importance of Global-recommended solutions to the ISE mission, but for realizing the *power* of the GAC process to develop and implement information sharing solutions that are developed "for practitioners by practitioners" to protect American citizens from a wide range of potential harms.

> "Global members appreciate the solid partnership between Global and the PM-ISE in working to bring information sharing to the next level. The local, state, tribal, and federal partners involved in Global, along with the PM-ISE, are together committed to efforts to adopt information sharing solutions that are developed *for practitioners/by practitioners* to improve public safety."
>
> —Mr. Robert Boehmer
> Chair, U.S. DOJ's Global Advisory Committee
> GAC representative from the National Criminal Justice Association

[35] This is the summarizing phrase/motto of U.S. DOJ's Global Justice Information Sharing Initiative (Global).

SECTION 2:
OPTIMIZING MISSION EFFECTIVENESS

The ISE is complex – comprising many organizations with diverse cultures, missions, and methodologies. These differences make for an intricate and often complicated network of law enforcement, defense, healthcare, and many other government and industry mission partners – all striving to establish and maintain access to the best information in order to make the right decisions at the right time in the defense of the nation. The organizational differences found in the ISE can be daunting: addressing their commonalities with respect to sharing and safeguarding information is the key to advancing terrorism-related information sharing, and enhancing the effectiveness of each organization. Each ISE agency must deal with: controlling and gaining access to restricted data; reaching across networks to discover and retrieve the data that they need; aggregating and correlating data from across the enterprise; and, ensuring that the data that each maintains is discoverable and retrievable by any authorized user in the ISE.

This section addresses these common mission dependencies, highlighting the previous year's initiatives and progress made in the fields of identity, credential, and access management (ICAM); network interoperability; data aggregation (correlation); watchlisting and screening; and Controlled Unclassified Information (CUI) Implementation. As these capabilities mature and move toward common solutions, agencies can begin to overcome the barriers that exist between agencies and missions – both the technological and the policy-based – and open the door to achieving shared goals of ensuring the consistent access to the right information, across government-wide networks, by authorized users who are uniquely and universally identified on networks.

The following list is a summary of specific actions taken over the past year to optimize ISE mission effectiveness. These activities are discussed in further detail below:

- The Federal CIO Identity, Credential and Access Management Steering Committee (ICAM SC) released *FICAM Roadmap and Implementation Guide Version 2.0* and developed the *FICAM Roadmap and Implementation Guide Maturity Model*;
- ICAM SC developed the Backend Attribute Exchange (BAE) Specification v2 and led the BAE Business Case and Sustainability Analysis;
- PM-ISE and the Committee on National Security Systems (CNSS) sponsored the Secret Fabric Gap Analysis;

- The ISA IPC Federated Identity Standards Tiger Team (FISTT) produced a report on the problems with multiple independent Identity federations;
- SBU/CUI interoperability partners made measureable progress in the areas of Simplified Sign-On (SSO), Search and Discovery, and Standardized Security Controls;
- Agencies submitted plans for compliance with the provisions in EO 13556--*Controlled Unclassified Information;*
- The CUI Executive Agent – the National Archives and Records Administration - established and maintained an online public CUI registry reflecting the initial authorized CUI categories and subcategories;
- The CUI Executive Agent and the Department of Justice Office of Information Policy issued "Guidance regarding CUI and the Freedom of Information Act," November 22, 2011;
- The CUI Executive Agent reported on the implementation of the CUI program in its "Report to the President," November 4, 2011;
- Executive branch agencies submitted to the CUI Executive Agent proposed plans for compliance with the requirements of Executive Order 13556, including the establishment of initial target dates. After a review of agency plans, and in consultation with affected agencies and OMB, the Executive Agent shall establish deadlines for phased implementation by agencies;
- Interoperable ICAM solutions on federal Secret networks moved from strategic planning under the leadership of the Senior Information Sharing and Safeguarding Steering Committee to tactical implementation by the CNSS, with continued oversight of the Steering Committee;
- The ISA IPC Data Aggregation Working Group updated the report on "ISE Data Aggregation Capabilities Applicable to Terrorism";
- The DNI, Attorney General, and Director, NCTC signed updated guidelines designed to allow NCTC to obtain and more effectively analyze certain data to better address terrorism-related threats;
- PM-ISE initiated, with DHS, a geospatial portfolio initiative to drive geospatial information sharing as a national asset;
- PM-ISE canvassed the Intelligence Community and other Federal agencies to assess the state of technical collaboration and integration of U.S. Government (USG) non-traditional terrorism-related data screening and data aggregation programs, and produced an interagency report of the findings;
- PM-ISE sponsored the first whole-of-government Data Aggregation Summit in September 2011 for 160 ISE mission partners. This Summit provided a forum for identifying several persistent data-aggregation, data-integration, and data-management challenges;
- PM-ISE provided dedicated subject matter expertise to advance ICAM efforts across the whole of government;
- PM-ISE teamed with GSA to operationalize the BAE to enable systems to securely access user attributes, originating from multiple data sources, based on existing industry standards, while properly handling both security and privacy issues; and
- PM-ISE, with DoJ, sponsored the development of an Information Exchange Package Documentation (IEPD) for federated search, and sought to increase the number of agencies that share sensitive law-enforcement information.

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

IRTPA requirements for information access management necessitate interoperable identity, credential, and access management (ICAM) solutions.[36] Today, there are multiple identity federation efforts underway across the government that are critical to establishing trusted, assured identity, which is essential for responsible information sharing. However, these efforts are not necessarily coordinated, nor are their solutions functionally interoperable. The current fragmentation leads to confusion by vendors of products and services, users, and partners across the systems: it also leads to overlaps and gaps in governance. Therefore, to the maximum extent that is practical, all ICAM approaches should use the same standards and profiles. The following ICAM initiatives address these problems.

FEDERAL IDENTITY CREDENTIAL AND ACCESS MANAGEMENT (FICAM) ROADMAP AND IMPLEMENTATION GUIDE

The *Federal Identity Credential and Access Management (FICAM) Roadmap and Implementation Guide* provides mission partners with a common set of standards, functions, and services for identity and access management. According to the 2012 ISE Performance Assessment Questionnaire (ISE PAQ), 95% of respondents plan to adopt FICAM standards and 52% report having already made significant progress in implementation. Of note, DoD has fully implemented the identity and credentialing processes, and DOI has a complete identity and credentialing system requiring Personal Identity Verification (PIV) validation, and is in the process of developing a complete access management plan in compliance with FICAM standards.

The ICAM Subcommittee (ICAM SC), under the Information Security and Identity Management Committee of the Federal CIO Council, oversees FICAM implementation. PM-ISE provides dedicated subject matter expertise to the ICAM SC, to help advance coordinated ICAM efforts across the whole of government. Since June 2011, the ICAM SC, working through multiple interagency working groups and tiger teams accomplished the following:

- Released *FICAM Roadmap and Implementation Guide Version 2.0* in December 2011.[xlix] While the initial document contained the segment architecture and some overview of the implementation guidance, Version 2.0 fleshes out the implementation guidance with substantial detail.
- Developed the *FICAM Roadmap and Implementation Guide Maturity Model* in November 2011. The Maturity Model provides leadership and an accurate gauge of an organization's maturity in its implementation of the FICAM Roadmap and Implementation Guidance.
- Contributed to the development of the Secret Fabric Gap Analysis, sponsored by the CNSS and PM-ISE, and supported by the Assured Secret Network Interoperability (ASNI) Working Group of the Information Integration Subcommittee (IISC) of the ISA IPC. The purpose of this analysis was to determine whether FICAM guidance could be implemented on the Secret fabric.[l]
- Created the Access Control Attribute Governance Working Group under ICAM SC to provide governance of access control attributes for effective ICAM implementation.[li]
- Contributed to the development of the BAE Specification v2, ensuring that the specification would support credentials that are widely used by State, local, and tribal mission partners.[lii]

[36] IRTPA Sec. 1016 (b)(2)(E) and (b)(2)(I).

- ICAM SC led the effort to develop a BAE Business Case and Sustainability Analysis.
- As follow-on to this effort, GSA and PM-ISE are teaming to operationalize the BAE capability via the pilot project detailed below.

ADVANCING IDENTITY ACCESS MANAGEMENT WITH THE BACKEND ATTRIBUTE EXCHANGE (BAE) PILOT

One of the keys to responsible information sharing is enabling systems to securely access credentials that may originate from multiple authoritative sources. This is why the Federal Government has been working to develop a strong BAE capability. In 2012, PM-ISE will support an initial test scenario in which an ISE mission partner will use BAE to access information from an external portal, such as the Regional Information Sharing System (RISS). The pilot will test the portal's ability to use BAE to confirm a user's basic identity and access credentials. Using a portal like RISS, for which additional access credentials are required – such as a training certification in personal privacy information handling – will allow for a test of BAE's ability to link to the training provider's official records, making it possible for the portal to confirm that the user has the appropriate certification in order to grant access.[liii]

According to the 2012 ISE Performance Assessment Questionnaire (PAQ), 89% of respondents report they have implemented and are using an accessible, authoritative source for identity information on at least one classification domain. Of note, FBI has designed and delivered an identity broker on Law Enforcement Online (LEO), their unclassified domain; and DOI currently uses information from the Federal Payroll Processing System for user attribute information and network access control.

Once proven, GSA plans to offer a BAE Service for use by any federal system as part of an overall federal access control infrastructure that state, local, and tribal partners could utilize. PM-ISE and GSA will also seek to make the BAE architecture a public voluntary standard, which may contribute to the development of the Identity Ecosystem envisioned by the National Strategy on Trusted Identities in Cyberspace. The return on investment in the BAE is expected to be significant; however, it will require agency investment and normalization of attributes to BAE standards throughout ISE partner organizations.

IDENTITY SUMMIT AND THE FEDERATED IDENTITY STANDARDS TIGER TEAM (FISTT)

In May 2011, PM-ISE held an Identity Summit that for the first time brought together five different identity federation efforts and provided a venue for participants to discuss their identity management frameworks and future plans. In support of this meeting, PM-ISE developed a briefing template to ensure that each of the five identity federations would cover the same topics, which allowed participants to effectively compare their efforts and facilitated the exchange of ideas. As a result of the Identity Summit, the IISC chartered the Federated Identity Standards Tiger Team (FISTT) to produce a report on the problems with multiple independent Identity federations with little or no coordination between them. PM-ISE led the development of the FISTT report and coordinated it through the inter-agency process.[liv]

FISTT recommended giving the responsibility for coordinating all Identity efforts on all classification domains (fabrics) to a subordinate committee of the ISA IPC in order to ensure the government-wide sharing of lessons learned and best practices, and to enable effective engagement of nonfederal stakeholders. FISTT also recommended that the subordinate committee report to the ISA IPC as well as the Federal CIO Council, and that it be given the authority and ability to interact with all identity efforts on all fabrics across all ISE partners, including state, local, and tribal governments.[lv]

NATIONAL INFORMATION EXCHANGE FEDERATION (NIEF) CERTIFICATION FOR FICAM COMPLIANCE

PM-ISE sponsored the DHS ICAM Office to certify National Information Exchange Federation (NIEF) as a FICAM Trust Framework Provider, including qualification of the Global Federated Identity and Privilege Management (GFIPM) framework as a FICAM "accepted scheme."[37] This initiative includes consulting and related services to assist NIEF members in reaching and verifying conformance. It does not conflict with work performed by the GSA to test, review, and interact with NIEF or third parties, however, nor does it include funding for hardware, software, or services performed or paid for by NIEF member organizations to achieve conformance. Certification of NIEF as a FICAM Trust Framework Provider will provide assurance to federal agencies that using NIEF as a way to share information with their partners would be fully compatible with the OMB mandate to implement FICAM. It would also assure continued alignment between FICAM and NIEF/GFIPM as technology and standards evolve.[lvi]

ASSURED SENSITIVE BUT UNCLASSIFIED (SBU)/CONTROLLED UNCLASSIFIED INFORMATION (CUI) INTEROPERABILITY

ASSURED SBU/CUI NETWORK INTEROPERABILITY WORKING GROUP

According to the 2012 ISE PAQ, 50% of respondents have a plan to implement a capability to interconnect SBU/CUI networks in order to share terrorism and homeland security information, and 37% report having already made significant progress.

The SBU/CUI Network Interoperability Working Group, chartered under the ISA IPC, is spearheading efforts to expand the amount of information and services shared among agencies to enable frontline mission personnel to securely discover, access, and collaborate on SBU/CUI Information. Since June 2011, the Sensitive But Unclassified Working Group (SBU WG) has been focused on SSO, search and discovery, and standardized security controls between four major law enforcement, public safety, and intelligence systems[lvii]:

- The FBI's CJIS Law Enforcement Online Enterprise Portal (LEO-EP);
- Regional Information Sharing Systems Network (RISSNET);
- DHS Homeland Security Information Network (HSIN); and
- The National Security Agency's (NSA) Intelink-U.

To promote shared responsibility, leadership, and direction, the SBU WG chair rotates every six months between mission partners. PM-ISE provides dedicated subject matter expertise to the SBU WG and assists the SBU WG Chair by establishing the Working Group agenda, prioritizing mission initiatives, facilitating partner meetings and providing overall project management support.

In 2011, the SBU WG established tactical focus teams, each led by an SBU partner and supported by subject matter experts from other partners, to develop end-state goals, objectives, and roadmaps for achieving the objectives under each individual goal. Significant progress toward each of these goals is summarized below.

[37] NIEF is a collection of U.S. agencies that share sensitive law enforcement information.

In 2012, the SBU WG realigned the focus teams to concentrate on Identity and Access Management (IdAM) as foundational for the interoperability efforts across the SBU environment. An IdAM framework will be developed that aligns with the FICAM Roadmap and Implementation Guide and connects with other IdAM initiatives, like the BAE.

During 2011-12, SBU/CUI interoperability successes continued to be incremental and evolutionary. Resource constraints made it more challenging for the SBU WG Partners to fully realize all of their self-proposed consensus goals. RISS and Intelink were particularly affected. Partner connectivity to HSIN is still on hold and cannot be initiated or realized until late FY2013, due to the continued development of a general HSIN upgrade. However, during the last year, measureable progress and achievements by the SBU Partnership continues to accelerate toward the goal of full interoperability.

SIMPLIFIED SIGN-ON (SSO)

- RISSNET, LEO, and Intelink users can now access services and data on multiple SBU systems without using separate credentials or log-ins.[lviii]
- Through LEO-EP, LEO users have access to the following services: National Data Exchange (N-DEx), Intelink, RISSNET, Joint Automated Booking System, Internet Crime Complaint Center, National Gang Intelligence Center, DoJ myFX, and many other capabilities beneficial to fusion centers and law enforcement agencies.[lix]
- In 2011, Intelink began providing Common Access Card (CAC) login, leveraging the existing CAC infrastructure within DoD. Intelink and DHS began testing Personal Identity Verification (PIV) interoperability, and verified that Intelink can accept DHS PIV credentials for identity and authentication.
- Today the current Identity Providers connected to LEO-EP through SSO via the CJIS Trusted Broker are the Chicago Police Department, the FBI CJIS Division, LEO, RISS, and the U.S. National Central Bureau of INTERPOL. The FBI Unclassified Network and DoJ (via PKI) are in the final testing stages of SSO connectivity to LEO-EP at this time.
- RISS has partnered with the DHS Federal Law Enforcement Training Center (FLETC) to make the FLETC Electronic Learning Portal (ELP) available to RISSNET users via federation. RISS is now working with LEO to make the FLETC ELP further available to authorized LEO users via SSO.
- In late 2011, with PM-ISE support, RISS identified three partner agencies to join the NIEF federation: the Oregon State Information Network, the South Dakota Connect Project, and the Institute for Intergovernmental Research. Currently, RISS is working with each partner to document current mechanisms and processes; identify and recommend equipment and technical elements needed by the partners to participate in the NIEF; and identify and draft the necessary policies and procedures in order for partnering agencies to implement the NIEF on-boarding process.

SEARCH AND DISCOVERY

- Both RISS and LEO incorporated Intelink Search to enhance law enforcement information discovery. When users of either system run a search, they can now simultaneously search their own systems and Intelink with a clear delineation between search results. The new search capabilities are a substantial step forward in providing enhanced information sharing. RISS and LEO have also partnered with FLETC to make the FLETC Electronic Learning Portal available to users.[lx]

- With support from PM-ISE and DoJ, RISS is developing an IEPD to improve information sharing through federated search, and is increasing the number of partners in the NIEF. A more robust and flexible federated search could be achieved by implementing a federated search capability based upon a standard NIEM IEPD.

STANDARDIZED SECURITY CONTROLS

- Based on requirements from the Treasury Department, Intelink is implementing an ISE enterprise capability for one-way transfer that allows users to securely transfer files from the Unclassified to Secret and Top Secret domains and from the Secret to the Top Secret domain. The Intelink solution is expected to achieve an interim operational capability in the fourth quarter of FY12.[lxi]
- In order to establish security reciprocity and to harmonize the security controls within the SBU environment, the Security focus team reviewed documentation for relevant controls and security requirements, data categorization requirements, and standards for identity, credentialing and access management, and has begun documenting minimum standards related to vetting, provisioning, and de-provisioning users.[lxii]

SBU INTEROPERABILITY METRICS

The SBU WG is working to define metrics that better demonstrate progress within the SBU interoperability initiatives. Today, there are several data points that indicate progress in this area:

- Emphasizing the external connections via SSO through CJIS Trusted Broker, RISSNET, shows an increase in the number of external user logons per month from 162 in September 2010 to 1157 in January 2012.
- RISS also had 7,845 unique Federated Identity Users as of December 2011, as compared to 2,664 as of December 2010.
- Intelink has increased the amount of federated Open Source Center users from 4,771 in April 2011 to 6,221 in April 2012.
- From April 2011 to April 2012, the volume of information indexed by Intelink's centralized search capability grew from 28.4 million to 46.2 million items, with an average of just under 27,000 searches performed per month.

IC STRATEGY FOR THE UNCLASSIFIED DOMAIN

The IC CIO released an IC Strategy for the Unclassified Domain that aligns with many of the objectives of the ISE, specifically the objectives of the ISA IPC Assured SBU/CUI Network Interoperability Working Group. The inclusion of all five ISE communities in the IC Strategy will serve all entities with a national security mission. PM-ISE endorsed the strategic goals and provided additional whole-of-government context for the IC's new strategy. PM-ISE will also work with the IC CIO on the strategy's implementation.

CONTROLLED UNCLASSIFIED INFORMATION IMPLEMENTATION

There are currently more than 100 different practices for handling unclassified information that requires protection across the Executive branch. This ad hoc, agency-specific approach has created inefficiency and confusion, leading to a patchwork system that fails to adequately safeguard information requiring protection, and unnecessarily restricts information sharing by creating needless impediments.

The goal of the Controlled Unclassified Information (CUI) program is to standardize the way the Executive branch handles such information, while emphasizing and enhancing the openness, transparency, and uniformity of government-wide practices. On November 4, 2011, the CUI Executive Agent (EA) – the National Archives and Records Administration - launched the public online CUI registry after reviewing and consolidating more than 2,200 authorities proposed by 47 departments and agencies into 16 initial categories and 74 associated subcategories. These categories and subcategories were supported by 366 unique authority citations as safeguarding and/or dissemination controls from law, regulation, and Government-wide policy. When fully developed, the CUI registry will reflect all authorized categories, subcategories, and associated markings, along with applicable safeguarding, dissemination, and decontrol procedures.

On June 9, 2011, the EA issued Controlled Unclassified Information Office Notice 2011-01: Initial Directive for Executive Order 13556, entitled "Controlled Unclassified Information." The CUI's first Annual Report to the President was submitted on November 4, 2011. The EA is required to publish a report on the status of agency implementation in each of the first five years following the date of the Order, and biennially thereafter. The Annual Report is made publicly available on the CUI website at www.archives.gov/cui.

On November 22, 2011, the EA and the Office of Information Policy (Department of Justice) issued "Guidance Regarding CUI and the Freedom of Information Act" in response to inquiries from agencies regarding the relationship between CUI and the Freedom of Information Act, and to provide additional clarity as to the intent of policy references. Beginning in December 2011, the EA began focusing on supplemental policy development for safeguarding, dissemination, decontrol, and marking requirements. The EA also hosted multiple working group meetings and adjudicated respective rounds of comments with departments and agencies, representatives of the public and private sector, and State, local, and tribal partners.

The Order prescribes an ongoing conversation between the EA, federal departments and agencies, the private sector, representatives of the public, and State, local, and tribal stakeholders as this development moves forward. Consequently, the EA continually reviews and refines policy development practices and protocols to fully engage all stakeholders. In addition, the EA partnered with the National Institute of Standards and Technology in order to begin development of CUI information technology requirements.

Federal departments and agencies are expected to establish and manage an agency CUI program that develops and implements agency procedures, roles, and responsibilities regarding CUI in accordance with the Order; provides required training for affected personnel regarding implementation and maintenance of the agency's CUI program; and creates a self-inspection program to ensure compliance with the Order. Consistent with the Order, departments and agencies were requested to submit their plans for compliance to the EA no later than December 6, 2011. Currently, the EA is evaluating proposed interim target dates to establish phased implementation deadlines on the basis of continued consultation with affected agencies and OMB. The EA recognizes that the departments' and agencies' proposed target dates for implementation may require revision in light of anticipated supplemental CUI guidance. Upon issuance of such guidance, agencies will be afforded the opportunity to submit updated compliance plans.

In order to reflect the background, current status and anticipated future direction of the CUI program the EA's website is maintained on an ongoing basis. The website can be accessed at http://www.archives.gov/cui/.

CLASSIFIED NETWORK INTEROPERABILITY[lxiii]

Sharing classified information among federal and non-federal mission partners – in a consistent and predictable way, with appropriate levels of assurance – is a critical capability for national security missions. However, the policies, processes, and technologies that underpin federal classified networks were not developed with assured sharing capabilities in mind. This capability gap has resulted in barriers to mission fulfillment – and also in incidents such as the WikiLeaks breach.

Considerable foundational work to identify and begin resolving assured sharing capability gaps for classified information – reported in detail in previous ISE Annual Reports –has been completed by the ISA IPC. A key finding of the ISA IPC's work on classified information sharing was that a lack of federal-wide governance structures is at the root of many barriers to sharing classified information among mission partners in a secure and predictable manner.

The White House, through the new Senior Information Sharing and Safeguarding Steering Committee (the Steering Committee), focused on the same issues identified by the ISA IPC to improve sharing and safeguarding for federal Secret networks[38], including developing improved network mapping, and implementing interoperable ICAM policies. These major milestones were assigned to the CNSS, which is responsible for developing information assurance polices for classified systems for tactical implementation. CNSS is charged with developing this governance, including strengthened collaborative links to the ISA IPC.

One example of a key project that has moved from strategic planning to tactical implementation is the development of plans for interoperable ICAM on federal Secret networks. Over the past year, the ISA IPC's ASNI WG partnered with the ICAM SC, CNSS's Identity and Access Management Working Group, and the IC CIO Council's ICAM Working Group to analyze the applicability of federal unclassified solutions for ICAM to classified systems. This joint study found that approximately 80% of the solution set for unclassified federal systems could be applied to classified federal systems and represents a key leveraging opportunity that will save both time and money. This study also represented a key milestone in collaboration between the federal civilian, defense, and intelligence communities.

The Steering Committee has leveraged this important strategic work and identified implementing interoperable ICAM, in the form of federal Secret network access employing PKI, as a near-term priority for tactical implementation by CNSS. With the collective progress in developing federal-wide governance structures for Secret networks, and solidifying key priorities and milestones for tactical implementation, the Federal Government is positioned for continued improvements in classified information sharing and safeguarding in the coming year.

GEOSPATIAL INFORMATION AS A NATIONAL RESOURCE

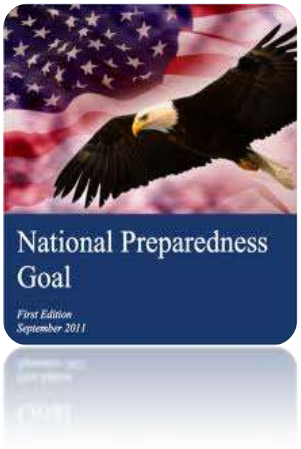
Geospatial information technologies (e.g. GPS, Remotely Sensed Imagery, Sensors, etc.) and their associated data, services, and visualization capabilities are increasingly needed to support ISE mission areas. PM-ISE and DHS have begun a geospatial portfolio initiative to drive geospatial information sharing across existing policy frameworks; adhere to open standards; and propose a technical reference model to foster interoperability between the civil defense and intelligence Geospatial Communities. The impact of these initiatives will be an increase of geospatial data and location-based services available through interoperable architecture and standards for frontline analysts,

[38] Senior Information Sharing and Safeguarding Steering Committee established by EO 13587, 7 October 2011.

responders, and operators for prevention, protection, mitigation, response, and recovery to all-hazards and all-threats that pose the greatest risk to the Nation's security.

In partnership with DHS, the Director of the Geospatial Management Office has been assigned to PM-ISE to establish a geospatial portfolio and to promote geospatial data and services sharing through interoperable architecture, standards, and policy. The primary focus will be to:

- Drive geospatial information sharing across existing policy framework, adhering to open standards;
- Propose a geospatial technical reference model to foster architecture interoperability between the civil, defense and intelligence geospatial communities;
- Add value by integrating traditional information sharing data needs into a geospatial context; and
- Enhance NIEM geospatial capacity based upon open standards.



As part of the geospatial policy alignment, PM-ISE and DHS are supporting the FEMA-led Presidential Policy Directive 8: National Preparedness Goal (PPD-8) with its goal of: "A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats that pose the greatest risk."

PM-ISE has supported FEMA in defining the geospatial capabilities and integration of mission-critical decision support tools for inclusion across the PPD-8 Mission Areas (e.g. Prevention, Protection, Mitigation, Response and Recovery), which includes the recognition of the interagency Homeland Security Geospatial Concept of Operations highlighted in the PM-ISE 2011 Annual Report. The PM-ISE, in coordination with FEMA, will develop guidance for agencies' execution of the PPD-8 National Planning Frameworks and Federal Interagency Operational Plans. The PM-ISE, in collaboration with FEMA, will also prepare memoranda providing further planning and reporting guidance for advancing the objectives of the National Preparedness Goal.

Whole-of-Government Data Aggregation Summit

In September 2011, PM-ISE hosted the first ever Whole-of-Government Data Aggregation Summit. Participants included 162 attendees from 25 agencies, including Program Managers for large data aggregation systems, Chief Information Officers (CIOs) and Chief Information Sharing Officers, enterprise and data architects, Privacy/Civil Liberties/Civil Rights Officers, DA WG members, and mission stakeholders. The objectives of the Summit were to:

- Share best practices and lessons learned from various departments, agencies, and other ISE partners who operate data aggregation systems;
- Identify architectural solutions already in use within organizations;
- Make recommendations for setting the standards by which next-generation data aggregation systems are built across the USG (to include the potential of federated access to critical data sources to span individual agency boundaries);
- Encourage information sharing among mission partner organizations that own, operate, and manage data aggregation programs; and
- Exchange ideas for moving toward distributed data aggregation solutions.

The results of this Summit also informed the development of the *ISE Data Aggregation Capabilities Applicable to Terrorism* report to the ISA IPC in March 2012.

DATA AGGREGATION[39]

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 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 access and dissemination of aggregated data within the ISE will be the capability to authenticate users across the environment. Through positive user authentication and authorization, logging of user access to data, and the ability to audit data trails, the risks to privacy associated with the sharing of aggregated data are mitigated.

According to the 2012 ISE PAQ, 65% of respondents reported that improvements in data aggregation over the previous year had a positive impact on mission outcomes. Of note, the FBI's Data Integration and Visualization System (DIVS) improved data aggregation significantly for FBI agents, analysts, and linguists by providing them with visualization, translation, and correlation tools to parse and analyze 65 datasets and approximately 1.9 billion files, improving the effectiveness and efficiency of FBI investigative and intelligence personnel by saving valuable search time for data gathered and generated by multiple sources, whether internal to the FBI or previously provided to the FBI.

DATA AGGREGATION WORKING GROUP

The Data Aggregation Working Group (DA WG), co-chaired by executives from DHS and NCTC, serves as a technical forum for providing recommendations to the ISA IPC IISC on optimizing the data sharing-related processes, standards, and architectures that underpin data aggregation capabilities in support of non-traditional screening for terrorism. Since June 2011, the DA WG has grown to from 18 to 40 federal and non-federal agency members.[lxiv]

REPORT ON ISE DATA AGGREGATION CAPABILITIES APPLICABLE TO TERRORISM

In June 2011, PM-ISE issued a survey developed by the DA WG to obtain an accurate representation of USG-wide investment in data aggregation programs, both within and outside the IC. Agency responses informed the updated report on *ISE Data Aggregation Capabilities Applicable to Terrorism,* which was delivered to the ISA IPC in March 2012. The report highlighted three themes: 1) ISE partners must embrace a whole-of-government approach to data acquisition; 2) Governance practices must be improved to ensure standards-based approaches; and 3) Information- sharing business processes must be improved while accelerating the pace of developing technical architectures that enable effective information sharing but also respecting the privacy, civil rights, and civil liberties of the American people.

INFORMATION EXCHANGE DATA AGGREGATION PILOT PROJECT

The Information Exchange Data Aggregation Pilot, funded by PM-ISE and DHS, and delivered jointly by NCTC and DHS, is a year-long initiative to improve two interagency, person-centric information exchanges. Its objectives include:

- Using a standard information-exchange model—NIEM—to improve data quality and streamline user access to the data closer to real-time;
- Developing a repeatable process for detecting and correcting corrupt data within the ISE;

[39] Data aggregation represents 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.

- Defining business-performance metrics around improving data quality and data extraction and consumption processes; and
- Developing IEPDs for two consumers of specific High Value Data Sets.

NCTC and DHS are working closely with the DA WG to ensure that it maximizes potential value to interagency efforts around person-centric data sharing. The DA WG also invited watchlisting agencies to participate in future instantiations of the pilot by defining requirements and identifying high value data sets.[lxv]

DATA AGGREGATION CHALLENGES AND NEXT STEPS

Despite many successes and improvements in technology and business processes, challenges still remain in the data aggregation community. Current data aggregation models in government rely on centralized correlation and data storage. Centralizing the data in this manner introduces privacy and security challenges: it can limit the ability of data producers to protect their data appropriately and to replicate their data multiple times to different requesting "data consumers" for aggregation. This can be very time-consuming, with expensive overhead, legal, and regulatory considerations as well (e.g., originating controls, classifications, etc.) concerning where the data may have originated from within the government.

In addition, many federal criminal justice agencies tend to use unstructured data – typically in free-form, text-heavy documents – which lack the robust labeling, cataloging, and tagging that highly structured data possesses. The electronic sharing of unstructured data is a technical and human resource challenge. Until effective tagging of unstructured data within native records management systems can occur, agencies must rely on interim solutions, such as manual records review, sharing of only pointer data, or the use of smart technology to extract, isolate, and understand information contained within free text.

Many federal databases also contain a significant amount of data from other federal agencies and even foreign governments with unique dissemination and use requirements. Several federal agencies are members of the Intelligence Community, whose databases contain classified and otherwise dissemination-caveated information.

The ISE must take strategic next steps for advancing data aggregation in the interagency, including aligning with the White House vision for data aggregation and engaging the Federal CIO Council to encourage a whole-of-government approach to data aggregation that includes both Title 50 (IC) and Non-Title 50 agencies. This whole-of-government approach to data aggregation involves working with industry for the sharing of reusable data aggregation best practices and lessons learned regardless of specific contexts.

DATA AGGREGATION CAPABILITY UPDATES AND SUCCESS STORIES

LAW ENFORCEMENT NATIONAL DATA EXCHANGE

In cooperation with state, local, and other federal partners, the FBI developed the Law Enforcement National Data Exchange (N-DEx), the first nationally-scaled criminal justice information sharing platform to provide nationwide connectivity and analytical functions to disparate local, state, tribal, and federal systems. As of June 2012, N-DEx had over 137 million searchable records—an increase of over 47 million records from the previous year—with more than 894 million entities (persons, places, things, and events); more than 52,000 total users; and with received information from 40 data sources representing more than 4000 submitting agencies.

In 2011, N-DEx proved invaluable in assisting a Kansas State Trooper by determining that the driver of a vehicle he had stopped was involved in human trafficking. In response to the trooper's query, N-DEx quickly returned pivotal information about the driver, including records on previous convictions for alien smuggling and other crimes,

several aliases, and booking photos that enabled the trooper to positively identify the driver as a convicted human trafficker. With that information, the trooper was able to solicit the assistance of Special Agents with the Department of Homeland Security: the driver was subsequently charged with human trafficking and aggravated re-entry, and his passengers were safely returned to their country of origin.[lxvi]

DHS'S NATIONAL PROTECTION AND PROGRAMS DIRECTORATE/US-VISIT'S ARRIVAL AND DEPARTURE INFORMATION SYSTEM

In December 2011, DHS's National Protection and Programs Directorate (NPPD)/US-VISIT released a NIEM-conformant update of the Arrival and Departure Information System (ADIS) Web Service architecture to offer a set of person-centric operations that allow external systems to search for ADIS identities and any additional data sets available for the selected data elements. The Department of State (DoS) played a key role in developing ADIS Web Service requirements and deployed the initial service to embassies and consulates worldwide in June 2011, culminating on average with more than 200,000 queries daily. US-VISIT is now engaged with the USCIS to provide similar support to USCIS databases.

Also in December of 2011, NPPD/US-VISIT introduced a major update to ADIS's Data Integrity Identification Validation (DIIV) tool. US-VISIT uses DIIV as a case management tool for identifying overstays. ADIS and DIIV will be essential to DHS's overstay-vetting efforts moving forward. Since August 2011, ADIS has been engaged with the Enhanced Overstay Vetting and Biographic Exit Project with ICE and CBP, identifying requirements to enhance data exchanges, close information gaps vital to processing National Security and Public Safety threat based overstays, and providing an enhanced biographic exit solution for DHS. Finally, ADIS is working with PM-ISE and the DA WG through the Pilot described above to improve two interagency, person-centric information exchanges.[lxvii]

DHS PATTERN AND INFORMATION COLLABORATION SHARING SYSTEM

In January 2012, the DHS Law Enforcement Information Sharing Initiative (LEISI) launched the DHS Pattern and Information Collaboration Sharing System (DPICS2), which replaced the U.S. Immigration and Customs Enforcement Pattern Analysis and Information Collection Tool, ICEPIC. DPICS2 allows users to simultaneously search for names and identifying numbers such as telephone numbers, in multiple DHS law enforcement databases. It also enables users to create link analysis charts for graphic presentations on subjects and associated records. Through DPICS2, users can also access N-DEx to search the records at more law enforcement agencies records than was previously possible. Since its launch, information found through DPICS2 queries has led to several administrative arrests and the issuance of numerous criminal arrest warrants.[lxviii]

RECORDS AND INFORMATION FROM DMVS FOR E-VERIFY

DHS and the Mississippi Department of Public Safety implemented the Records and Information from DMVs for the E-Verify (RIDE) initiative that will allow employers to verify the authenticity of Mississippi (MS) drivers' licenses presented during the E-Verify process. This initiative leverages existing technology that all state motor vehicle administrations currently use, making it a low-cost project for both the state and the U.S. Citizenship and Immigration Services (USCIS). As documented in an update to the existing E-Verify Privacy Impact Assessment and Systems of Record Notice, E-Verify began validating MS driver's license data in June of 2011. USCIS is in the process of signing up other state motor vehicle administrations as part of a larger initiative to curtail document fraud, and will continue to work closely with government privacy officials to ensure that the expansion of RIDE to other state driver's license agencies comes with the proper notice and comment afforded through the Privacy compliance process. E-Verify estimates that more than 80% of employees use a driver's license to establish identity on the I-9 Form. Until now, E-Verify did not check any of these documents for validity or authenticity against state databases.

The RIDE initiative will fill this critical gap, enhance the integrity of the E-Verify system, and offer greater assurance to employers that their new hires are using legitimate documents.[lxix]

WATCHLISTING AND SCREENING

Since the failed attempt by Umar Farouk Abdulmutallab to bomb Northwest Airlines Flight 253 on Christmas Day, 2009, NCTC has adopted important reforms in the watchlisting process and has improved NCTC's receipt, processing, and quality of information sharing in support of the Center's watchlisting and screening responsibilities. In particular, NCTC is taking a more aggressive and innovative approach to seeking methodologies and data repositories for ingesting biographic, biometric, and derogatory information, and to ensure the accuracy of information about individuals while complying with applicable law.[lxx] As the terrorist threats continue to evolve, NCTC's watchlisting experts are proactively working with NCTC's Pursuit Group, established in 2010, and the CT community to expedite the sharing of information to build more complete terrorist identities. NCTC has also enhanced its ability to store, compare, match, and export biometrics such as fingerprint, facial images, and iris scans.[40]

GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION

In March 2012, the DNI, Attorney General, and NCTC Director signed updated guidelines designed to allow NCTC to obtain and more effectively analyze certain data in the government's possession in order to better address terrorism-related threats, while at the same time protecting privacy and civil liberties.[41] The updated guidelines provide a framework that allows NCTC to obtain certain data held by other USG agencies to better protect the nation and its allies from terrorist attacks. The revised Guidelines permit NCTC to retain – for up to five years – certain datasets that are likely to contain significant terrorism information and are already in the lawful custody and control of other federal agencies, unless a shorter period is required by law.[lxxi]

Following the failed terrorist attack in December 2009, representatives of the CT community have concluded that it is of vital importance that NCTC be provided with a variety of datasets from various agencies that contain terrorism information; and that they have the ability to search against these datasets for up to five years on a continuing basis. These updated guidelines will enable NCTC to accomplish its mission more practically and effectively than previous guidelines allowed.

COAST GUARD CO-LOCATES ANALYSTS AT THE CBP NATIONAL TARGETING CENTER

In 2011, the Coast Guard co-located a select group of analysts with their CBP counterparts at the CBP National Targeting Center in order to improve interagency maritime screening and targeting. By using common tools, sharing access to databases, and cooperative analysis, the Coast Guard improved their own and in turn national maritime passenger, crew and cargo screening processes. The Coast Guard is now better able to contribute vessel-related intelligence expertise, resulting in improved national-level analysis. The Coast Guard and CBP have also signed a Maritime Operations Coordination Plan to improve field operations, and they began developing a Joint Targeting Architecture for data-sharing consistent with DHS Common Vetting goals.

[40] Testimony of Matthew G. Olsen, Director, NCTC, before the Permanent Select Committee on Intelligence, U.S. House of Representatives, October 6, 2011.

[41] ODNI News Release No. 5-12, Office of the Director of National Intelligence and Department of Justice Joint Statement: Revised Guidelines Issued to Allow The NCTC to Access and Analyze Certain Federal Data More Effectively to Combat Terrorist Threats.

INTERLUDE: INDUSTRY LEADERSHIP IN IMPLEMENTING THE ISE – "FROM THE OUTSIDE IN"

ISE implementation requires effective partnering between government and industry so that government's interoperability requirements are transparent to industry and vendor solutions have these requirements and associated standards "built in" to commercial products prior to responding to an acquisition. Compliance with open information sharing standards mutually benefits industry and government:

- With expanded market potential, industry becomes more competitive; and
- By procuring and reusing standards-based interoperable solutions, government becomes more efficient and controls costs.

PM-ISE is addressing industry implementation of the ISE "from the outside in" from three perspectives: government influence through participation in industry consortiums and Standards Development Organizations (SDOs); industry insight into enabling standards-based acquisitions; and the certification and testing of standards and vendor solutions through programs such as Springboard.

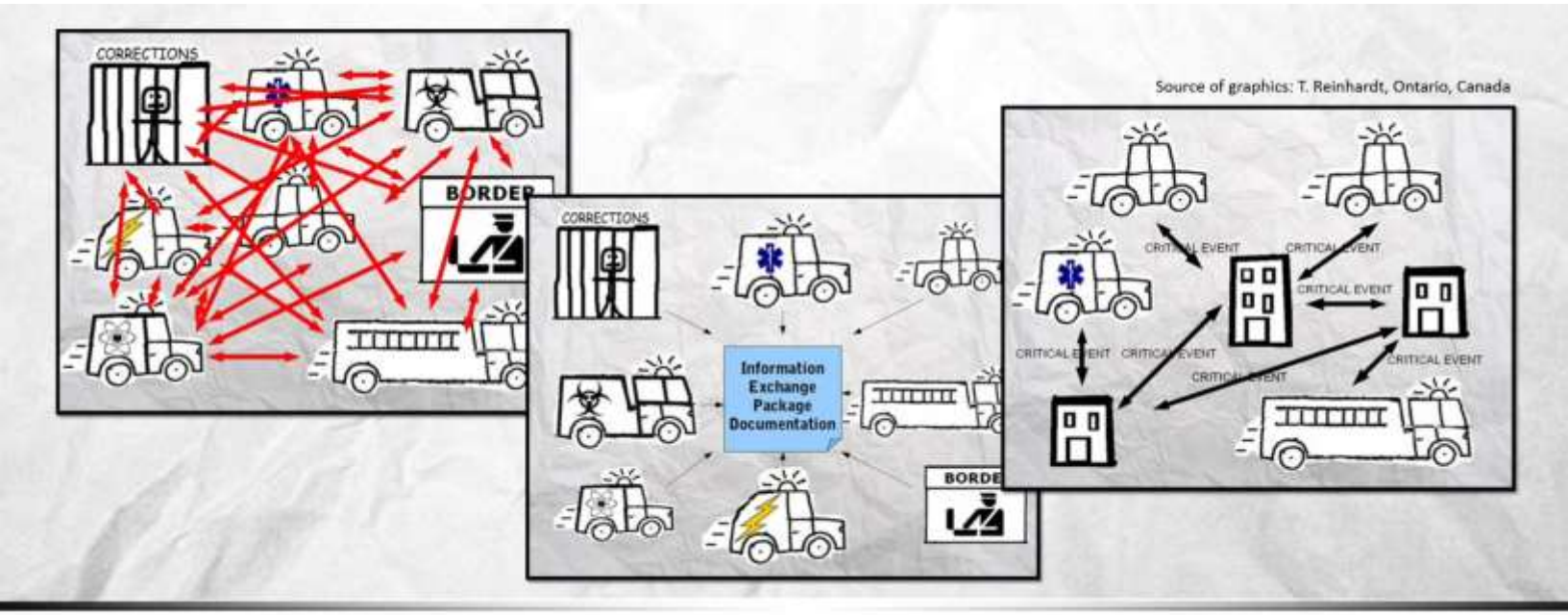
Through our participation with industry-led consortia and SDOs, the PM-ISE promotes the development, ratification, and adoption of open standards to exchange information responsibly and securely. For example, we have worked with the NIEM community of the Object Management Group to define a NIEM-UML Profile (addressed later in this report). In response, leading-edge technology vendors are beginning to market NIEM integration and compatibility as part of their product line. Another example is the coordination between the Open Geospatial Consortium (OGC) to align standards such as Geospatial Markup Language (GML) with NIEM.

The role of government cannot stop at the development of these standards. Consistent use of these standards in RFPs, grants, and other acquisition vehicles is essential so that newly acquired commercial solutions are interoperable across organizational boundaries, government jurisdictions, and mission areas. Under PM-ISE's and GSA's sponsorship, the American Council for Technology--Industry Advisory Council (ACT-IAC), http://www.actgov.org, is soliciting industry input on the extent to which industry has adopted or is adopting standards that enable information exchange for government and commercial projects. ACT-IAC will document its findings in a white paper that will provide recommendations to policy makers on what the U.S. Government can do to stimulate, broaden, and deepen the use of these standards. We have already been successful in working with the DOJ BJA to extend its grant language to include the broader set of DOJ's Global Standards, including not only NIEM, but the GFIPM and GRA. Instructional material was provided to grant managers to facilitate the incorporation of this language into future grant vehicles. We are also evaluating other best practices: for example, DHS launched a program for cross-training acquisition and IT program managers on each other's disciplines. The intent is to have an integrated toolkit that will support federal, state, local, tribal, and private sector stakeholders in taking a standards-based approach to acquisitions.

Lastly, we have been working closely with the IJIS Institute, responsible for launching the Springboard initiative, a standards-based interoperability program designed to provide industry and government with an environment for evaluating justice standards through a consensus process, testing standards, and the generation of reports certifying projects through a conformance management process. Other SDOs, such as OGC, have increased agency adoption of their standards through similar interoperability programs.

Through our participation in these activities, PM-ISE is conveying the imperative to "connect the dots" and to encourage interoperability. Information is a national asset: the widespread adoption of open, industry-accepted standards is critical for sharing data because it enables systems and networks to interoperate. The PM-ISE is broadcasting this message to industry: if you want to do business with the government, you must follow industry-led open standards for information sharing, in order to ensure that information gathered from disparate systems can help prevent terrorism and keep our nation safe.

This page intentionally left blank



SECTION 3:
STANDARDS DEVELOPMENT AND IMPLEMENTATION

ISE mission partners require innovative solutions to address the challenges they confront daily. Information architecture, standards, and technology allow mission partners to automate activities, deliver information in a more timely fashion, and acquire and implement interoperable solutions. The end objective is to provide a flexible and scalable architecture in which all partners can participate by building and employing shared services and open standards—like the Nationwide Suspicious Activity Reporting Initiative—to gather, share, analyze, and disseminate information, and to manage costs more effectively[lxxii].

The ISE's ability to responsibly share information is dependent upon a government-industry partnership in which the government comes to consensus on the standards that it will use, and industry delivers products that will truly accelerate responsible information sharing. This type of innovation will result in more cost-effective solutions and greater agility in the face of evolving threats; enable the establishment of dynamic networks across mission partners; and reduce redundancy and unnecessary complexity. Industry's support and leadership in standards development and use is fundamental to ISE's success.

The efforts undertaken since June 2011, sponsored by PM-ISE and supported by ISE partners, represent projects designed to further and foster the baseline capabilities, environment development, and mission of the ISE.

The following list is a summary of specific actions taken over the past year to develop and implement standards across the ISE:

- The ISA IPC Standards Working Group (SWG) hosted a Standards Repository Summit to identify best practices for creating and maintaining standards registries and repositories;
- The ISA IPC SWG and Standards Coordinating Council created the *Standards Way Ahead,* which captures the collective decisions from the December 2011 Workshop for Information Sharing & Safeguarding Standards (WIS3), sponsored by PM-ISE;
- The National Information Exchange Model (NIEM) – Unified Modeling Language (UML) specification was developed to enable general use of UML and Model Driven Architecture (MDA) tools to support the development and use of NIEM information exchanges and models;

Workshop for Information Sharing & Safeguarding Standards

In December 2011, PM-ISE brought together over 200 thought leaders from ISE mission partners, leading standards development organizations, and industry associations to debate, discuss, and agree on standards and frameworks to enable responsible information sharing. Discussion revolved around the vision of a market in which U.S. government agencies can purchase hardware and software solutions with responsible information sharing standards already "baked in." Presenters and panelists debated constructs of the ISE architecture including:

- Translating business requirements to technical architecture;
- Identity and access management across government;
- Federated information sharing frameworks and services; and
- Standardized information exchanges across government.

A key outcome of the event was agreement to establish a Standards Coordinating Council.

- NIEM and UCore council members began discussing NIEM-Ucore convergence;
- Trident Warrior 2011 demonstrated the use of NIEM-Maritime for sharing vessel position reports;
- PM-ISE initiated the development of a new NIEM-based Information Exchange Package Documentation (IEPD) for Requests for Information (RFI);
- PM-ISE partnered with DHS's Domestic Nuclear Detection Office (DNDO) to demonstrate the ability to connect standardized radiological/nuclear alarm data and detectors in the Global Nuclear Detection Architecture;
- PM-ISE worked with industry-led consortia and standards development organizations (SDOs) to promote the development, ratification, and adoption of open standards for commercial products and services that can easily exchange information;
- PM-ISE convened more than 200 ISE mission partners, leading SDOs, and industry associations to debate, discuss, and agree on standards and frameworks to enable responsible information sharing;
- With DoJ/BJA, PM-ISE developed training and toolkits for grant managers and grantees to implement standards-based requirements development;
- PM-ISE supported multiple meetings to help facilitate NIEM-UCore convergence, which would permit multiple communities' information systems to exchange messages;
- PM-ISE sponsored the American Council for Technology - Industry Advisory Council (ACT-IAC) to solicit industry input on data exchange technical standards, and to learn from industry what tools it needs to better work with government on standards-based IT acquisitions;
- PM-ISE, along with the Standards Working Group and the Standards Coordinating Council, began to re-evaluate the baseline set of standards needed for information exchange;
- PM-ISE sponsored the IJIS Institute Springboard effort to advance justice, public safety, and homeland security information sharing via an open standards implementation process;
- PM-ISE hosted an international training event to help implement NIEM-conformant exchanges for North American pilots for public health and public safety information sharing; and
- PM-ISE partnered with Canadian government representatives to discuss NIEM adoption for Canada's law enforcement and public safety communities.

STANDARDS GOVERNANCE

STANDARDS WORKING GROUP

As noted in last year's Report, the SWG of the ISA IPC's Information Integration Sub-Committee (IISC) was established in May 2011 to facilitate standards development and reuse by using a whole-of-government approach that fosters interoperable information exchanges within the FSLT communities. In August 2011, the Standards Working Group (SWG) hosted a Standards Repository Summit to identify best practices for creating and maintaining standards registries and repositories to determine the most efficient ways to manage existing standards and make them easily available for reuse.[lxxiii] Following this Summit, the SWG developed a Common Lexicon for standards to ensure that SWG members use a common set of terms when addressing standards and profiles. The SWG also updated the ISE-AM-300 Common Information Sharing Standards (CISS) Program Memorandum, to more accurately articulate the types of standards being developed under the auspices of the ISA IPC.

The SWG is currently updating its standards development process, outlined in the Common Information Sharing Standards Manual, so that there is more transparency in how the public and private sector work together to develop standards. Moving forward, the SWG is positioned to serve as the public pillar in a public-private sector partnership for identifying operational needs and requirements not currently supported by standards-based solutions, and to facilitate joint approaches by government and industry.

STANDARDS COORDINATING COUNCIL (SCC) AND STANDARDS WAY AHEAD

ISE partners must make informed investment decisions by using shared resources, harmonizing policy, rationalizing business processes, integrating standards activities, and deploying technology to realize joint objectives and requirements. The Standards Coordinating Council (SCC) supports the ISA IPC SWG in these efforts by addressing the challenges of coordinating and influencing information sharing standards and initiatives representing the private sector perspective.[42] The *Standards Way Ahead* was created under the auspices of the SWG and SCC, and captures the collective decisions from the December 2011 Workshop for Information Sharing & Safeguarding Standards – folding them into guiding objectives for coordinating responsible information sharing standards activities, and a baseline set of recommendations and activities to develop a roadmap and standards lifecycle to achieve the following:

- **Mission-driven**: ISE capabilities and standards must serve all mission partners' requirements and enhance operational effectiveness as a result of information and service sharing while better managing costs.[lxxiv]
- **Shared resources**: Reuse is an important aspect of ISE efficiency, effectiveness, and agility. The standards, architectures, systems, and tools of mission partners are more relevant and more easily integrated when they are capable of serving not only the counterterrorism function, but also providing additional integrated mission capabilities.[lxxv]

[42] The SCC, a subsidiary group of the ISA IPC, consists of Executive-level representatives and/or senior technical engineers from standards development organizations (SDOs), industry associations, and other industry bodies; a representative from PM-ISE; and the ISA IPC's Standards Working Group (SWG). Subject -matter experts are invited to offer their advice and counsel on specific issues. The objectives of the SCC are to advise and support through the creation of an integrated governance model; to streamline standards development activities; to adopt high-value standards initiatives; and to enhance awareness of industry standards activities by establishing a coordinated feedback channel from government to industry to focus industry efforts.

- **Integrated governance**: Governance is a key component in making the ISE capabilities efficient and effective across diverse jurisdictions and mission processes. Leveraging a multilateral structure that includes government, standards development organizations (SDOs), and industry improves the information sharing dialogue. According the 2012 ISE PAG, 78% agencies reported engaging with industry SDOs to further voluntary consensus standards.

STANDARDS IMPLEMENTATION

The PM-ISE continues to facilitate partnerships to develop functional and technical standards for responsible information sharing. According to the 2012 ISE Performance Assessment Questionnaire (ISE PAQ), 86% of ISE agencies incorporate ISE functional standards into the management and implementation of its ISE-related mission business processes. 86% of ISE agencies also incorporate ISE Technical Standards into enterprise architectures and IT capabilities. (ISE technical standards are more "extensively" used by ISE agencies. For example, DoT has recently incorporated technical standards into the architecture and design of its new SAR database.)

NATIONAL INFORMATION EXCHANGE MODEL (NIEM)

Designed by experienced practitioners, governed by ISE partners, and driven by leadership from DHS, DoJ, HHS, and PM-ISE, the National Information Exchange Model (NIEM) program is developing, disseminating, and supporting enterprise-wide information exchange standards and processes that enable jurisdictions to effectively share critical information in emergency situations, as well as to support the day-to-day operations of agencies throughout the nation. By providing a common vocabulary and a mature framework, NIEM enables diverse communities to "speak the same language" when sharing, exchanging, accepting, and translating information. As of March 2012, all 50 states and 18 federal agencies are committed to using NIEM in some capacity and at some level of maturity. The NIEM value proposition is being demonstrated every day across the country as it facilitates information to improve public safety, strengthen homeland security, and share health, human and social services information.[lxxvi]

DHS and DoJ/BJA now use NIEM as part of their IT strategic plans, Request for Proposals (RFP) to vendors, and grant language to state, local, and tribal governments.[lxxvii] These types of approaches send the clear signal to industry that we know what standards we are using, and that there will be a market for innovative products that adhere to them. DoJ has also extended its grant language to require conformance to the broader Global Standards Package. PM-ISE and DoJ/BJA are working on training and toolkits for grant managers and grantees.

NIEM UNIFIED MODELING LANGUAGE PROFILE SUBMITTED TO THE OBJECT MANAGEMENT GROUP

The rapid adoption of NIEM, especially in the justice, public safety, and public health communities, has made it clear that governance and tool support need to keep pace. To efficiently leverage NIEM resources for rapid expansion, the NIEM Program Management Office (PMO) established an approach (outlined in the NIEM High Level Tool Architecture) that supports interoperability through standard open interfaces and well-defined import/export artifacts. This removes the need for an all-in-one tool, and allows both existing and new tools to support the functions of NIEM development processes.

Consistent with this approach, the NIEM Unified Modeling Language (NIEM-UML) is a specification developed in coordination with the Object Management Group (OMG) Technical Committee, and designed to enable general use of UML and Model Driven Architecture (MDA) tools to support the development and use of NIEM information exchanges and models. The key aspects of this specification are that it is ***standards-based, simple, reusable, and agile*** – enabling the NIEM profile to be used with other standards and technologies. In addition, it allows

audiences with different levels of knowledge of NIEM technical concepts to create variations of existing NIEM exchange packages that are interoperable with other NIEM models.[lxxviii]

The profile was praised and formally recommended for approval by the OMG Architecture board for final review and approval during the June 2012 OMG Technical event, and is expected to be fully approved by the OMG Board of Directors in the 4th quarter of FY12 – thereby receiving their endorsement as an industry standard. The expected result is the development and commercial availability of vendor products that have the capability to significantly reduce the underlying complexity of NIEM, while expanding the user community. The NIEM UML Profile has received significant interest within both user and vendor communities, and a number of mission partners have expressed interest in piloting and being early adopters of the new NIEM UML Profile.

STANDARDIZING REQUESTS FOR INFORMATION

Requests for Information, or RFIs, are the common means for requesting information among the 77 fusion centers, 16 intelligence agencies, 24 DHS Operation Centers, and 18,000 law enforcement agencies that currently share information to support their missions. These entities are hampered in their ability to efficiently deliver, receive, and respond to RFIs, because there is no common standard for requests. Agencies are not required to identify a single point of entry for receipt; there is no mechanism to identify duplicate RFIs submitted by more than one agency; there is no searchable archive; and there is no mechanism to discover the status of a current or active RFI.

To address these issues, PM-ISE and the NIEM PMO have initiated the development of a new NIEM-based Information Exchange Package Document (IEPD) module for RFI. Working closely with DHS's Information Sharing and Safeguarding Governance Board, this IEPD was prototyped with DHS's Common Operating Picture (COP) program to facilitate interoperability among the disparate requirements and collection systems used by DHS components.[lxxix] In 2012, the DoJ Global Advisory Committee's Standards Council recognized the potential benefits of the DHS COP project and expressed an interest in using this IEPD to develop an RFI Service Specification Profile (SSP) for use by law enforcement partners at all levels of the government. Once complete, the SSP will be extensible to all mission partners at all levels of government that use NIEM-conformant information exchange models.

NIEM/UNIVERSAL CORE (UCORE) CONVERGENCE

Universal Core (UCore) facilitates the sharing of intelligence and related digital content across the DoD and the IC. UCore was developed as a data standard by the DoD and IC to improve information sharing by defining and exchanging a small number of important, universally understandable XML components to identify the "Who, What, When, and Where" aspects of data. When coupled with NIEM, these reusable data components can be used to construct common vocabularies and interoperable information exchange specifications for multiple

"BEST OF NIEM AWARDS"

For their commitment to advancing and substantially improving how NIEM is used, the NIEM PMO presented the second biannual "Best of NIEM" Awards at the 2011 NIEM National Training Event:

Northern Virginia CAD2CAD Exchange: Emergency services providers in four jurisdictions cut response time in half by connecting Computer-Aided Dispatch systems using NIEM.

New York State Integrated Justice Portal: Replacing dated applications with NIEM-compliant exchanges, the portal processes 1.5 million daily transactions and its 50,000 users can now access information from up to 14 data sources with a single query.

Iowa Criminal Justice Information Sharing Project: Using Global Reference Architecture and NIEM, Iowa set up 24 exchanges that now link more than 100 state and local law enforcement agencies.

Pennsylvania Data Quality Framework Project: Developed a customized toolkit for law enforcement best practices, resulting in 33 independently run counties adopting the NIEM schema for case management, with an average improvement in data quality of 271 percent.

State Department Enterprise Service-Oriented Architecture Migration: DOS's Office of Consular Systems and Technology used NIEM-conforming data exchange services to validate identities for its database—one of the largest in government, the database grows two terabytes each month.

communities of interest (COIs) in a domain. During the past year, the UCore Council, represented by DoD, IC, NIEM PMO, and PM-ISE has recognized the broad representations of multiple domains that make up NIEM, and is considering opportunities to converge UCore with NIEM. The NIEM PMO and PM-ISE have supported multiple meetings and discussions to help facilitate this transition, and the UCore Council has tentatively agreed to converge with NIEM by early 2013.[lxxx]

NIEM TRAINING EVENTS

The 2011 NIEM National Training Event, held August 23-25 in Philadelphia, drew more than 500 government and industry IT and business professionals from four countries, 38 states, 23 federal agencies, and 75 industry organizations. The ever-growing use and incorporation of NIEM for domestic and international information exchange was reflected in the diversity of the event's audience and speakers. Ellen Levy, LinkedIn's vice president of strategic initiatives, keynoted the event. Other notable speakers included Dr. Douglas Fridsma, director of the Office of Standards and Interoperability at the Office of the National Coordinator for Health Information Technology, who spoke on information exchange and interoperability in the healthcare industry; and Canada's Chief Information Officer, Corinne Charette, spoke about the Canadian government's adoption of NIEM. U.S., Mexican, and Canadian representatives presented workshops on NIEM adoption in concert with their recently-executed trilateral MOU for specific information exchanges.

To facilitate the implementation of NIEM-conformant exchanges for the North American Day (NAD) pilot projects discussed in Section 1, the NIEM PMO, in conjunction with PM-ISE, the Centers for Disease Control and Prevention, and the NAD Executive Committee hosted an international NIEM training in Atlanta, Georgia. The training consisted of technical, program manager, and Executive-level NIEM training, and included an IEPD workshop specifically focused on the NAD pilot projects[lxxxi]. During this event, participants developed initial-draft IEPDs and collaborated on how to implement these exchanges utilizing existing technology systems and architectures in each of the three countries, as well as processes for ensuring protections for privacy, civil liberties, and civil rights[lxxxii] in accordance with the regulations of each country.

INTEGRATED JUSTICE INFORMATION SYSTEMS SPRINGBOARD

Sponsored by PM-ISE and managed by the Integrated Justice Information Systems (IJIS) Institute, Springboard is a standards-based interoperability program designed to advance justice, public safety, and homeland security information sharing via an "open" standards implementation process. Through Springboard, the IJIS Institute will work with sponsor organizations to provide an environment in which industry and government can cooperatively evaluate standards through a consensus management process; test standards in a shared resources environment; generate engineering reports, implementation profiles, test suites, and reference implementations; "certify" products through a conformance management process; and steward standards and work products through standards governance partnerships.[lxxxiii] Springboard does ***not*** intend to create another SDO: rather, it strives to create a cooperative that will work with a variety of stakeholder organizations to create a governance structure and process whereby industry can work with relevant standards and leverage the technology assets developed by government and industry organizations in pursuit of the Springboard mission. The Springboard approach is based on the lessons learned from and the success of the Open Geospatial Consortium's Interoperability Program.

Initially, Springboard will work with the Global Standards Council, a part of DoJ's Global, to focus on the promotion of foundational standards including, but not limited to, NIEM, the Global Reference Architecture (GRA), the Logical Entity Exchange Specification (LEXS), and the Global Federated Identity and Privilege Management (GFIPM). As Springboard matures, the long-term plan includes working with other standards development bodies to support adoption and use of their standards.

The first initiative to go through the Springboard process will be the IJIS Prescription Monitoring Program (PMP).[43] IJIS Institute is working with government agencies and national associations to identify other national information sharing standards-based initiatives to participate in the Springboard process in order to promote broader adoption and use of these national standards.

STANDARDS-BASED ACQUISITION FOR INFORMATION SHARING

The success of the ISE requires the consistent use of interoperable standards in the products and services these organizations acquire. Effective information sharing must bridge many different systems by employing the decentralized, distributed, and coordinated approach prescribed in IRTPA. New technology is driving changes in infrastructure operations, including cloud, mobile, and SOA solutions.

In this constrained fiscal environment, agencies are focusing on controlling costs, avoiding duplication, increasing shared services, and streamlining. However, there is still little consistency when referencing or enforcing the use of information sharing frameworks, standards, and guidance in RFPs, grants, or other acquisition vehicles. According to the 2012 ISE PAQ, only about one-half of agencies consider ISE functional and technical standards when issuing RFPs for ISE-related systems. As a result, PM-ISE has begun two efforts in order to address the standards-based acquisition issue.

First, PM-ISE is working with the Standards Working Group and the Standards Coordinating Council to re-evaluate the baseline set of technical standards needed for information exchange. This effort will help create a common set of technical standards that should be incorporated into all ISE partners' enterprise architectures. The effort is informed by agency data on the specific use of technical standards in the areas of information exchange, messaging, and identity and access management. Initial observations include:

- There is general movement across the ISE to employ standards in requirements developed for contracts, indicating movement toward a "responsibility to provide information" culture;
- More than 60 SDOs were identified, nine of which are responsible for more than 20 standards each;
- There is a wide variation in the depth and breadth of standards identified;
- Agencies need to refresh their standards profiles/roadmaps, as many obsolete standards were mandated; and
- Potential barriers to standards implementation include the Federal Government's annual budget planning cycle; the time it takes to ratify a standard (often upwards of two years); the rapidity of technology change, and the ability for a standard to be defined quickly enough.

Findings from the analysis of this data will be incorporated into the CISS Manual updates. In addition, PM-ISE will work with the Administration and agencies to jointly develop guidance for standards-based acquisition across the Federal Government.

Second, PM-ISE and GSA are sponsoring an initiative through the American Council for Technology - Industry Advisory Council (ACT-IAC) that will provide an industry perspective on standards-based acquisition. ACT-IAC has received input from more than 80 vendors on technical standards used in U.S. Government IT acquisitions that use data exchange standards as part of the requirements, reference documents, and/or selection criteria. By focusing

[43] The primary program goals of the PMP are to facilitate the secure, reliable, and sustainable interstate exchange of state PMP data so that states can share prescription information with one another and potentially save lives.

on industry motivation, incentives, and rationale for using standards in software development and maintenance, the intent is to understand which kinds of standards are most valuable for enabling information exchange, and the extent to which they are adopted or being adopted for government and commercial projects. The ACT-IAC white paper will provide recommendations on what the Federal Government can do to stimulate, broaden, and deepen the use of these key standards. PM-ISE, in conjunction with GSA, will develop pilots at agencies to "test" the use of standards upfront in the acquisition and system-development lifecycles, as well as to monitor improvements in earlier conformance of vendor tools, and transparency in government requirements to industry.

PM-ISE intends to leverage the output of the analysis of agency-specific use of technical standards, the ACT-IAC White Paper, and the results from the pilots to accelerate the use of information sharing standards in acquisition and grant language, and to foster reuse of these standards across the ISE mission partners. The recommendations from these efforts will be captured in a final report to be presented to policy makers.

Industry is responding to the signal, with leading-edge technology vendors beginning to market NIEM integration and compatibility as part of their product line. In March 2011, at the request of PM-ISE, the IJIS Institute conducted a survey of their member companies to determine how many have adopted standards such as NIEM, GRA, and GFIPM in the products used at the state, local, federal, and international levels. Twenty-one companies responded, including commercial vendors, consulting firms, and defense contractors of various sizes.

These companies identified more than 2,000 state and local agencies that are sharing information with a large number of other agencies within their districts of operation. The respondents indicated that this sharing is enabled by using a variety of standards including NIEM, GJXDM, GRA, and GFIPM. For example, the Automated Regional Justice Information System (ARJIS) criminal justice enterprise network, enabled by NIEM, is used by 71 local, state, and federal agencies in the two California counties that border Mexico. The secure ARJISnet intranet integrates more than 6,000 workstations throughout the 4,265 square miles of San Diego County, and there are more than 11,000 authorized users generating more than 35,000 transactions daily.

From federal business endeavors, the respondents identified 15 federal agencies or bureaus that either have implemented or are implementing NIEM-compliant solutions. This expanded use at the federal level is further evidenced by the NIEM.gov website where, as of April 2012, 18 federal agencies have committed to using NIEM in some capacity and at some level of maturity.

NIEM-compliant products are enabling integration with national sharing initiatives such as:

- The U.S. Navy's LInX system, which has a network of 875 agencies connected through 11 regional systems using NIEM exchanges, and
- The FBI's N-DEx integration with the Navy's LinX systems, connecting more than 800 agencies nationwide through the benefit of NIEM.

Respondents also provided evidence of NIEM adoption at the international level, showing that companies are seeing potential market expansion opportunities as a result of implementing information sharing standards in their products. For example, NIEM has been adopted by The European Union's Judicial Cooperation Unit (EUROJUST) as a tool to allow the exchange of crime data between Member national case management systems and with EUROJUST. Because of the complex and diverse nature of national IT application landscapes in Europe, it became apparent that the original European Pool against Organised Crime (EPOC) software introduced in 2004 was unlikely to replace existing national case management systems. As a result, the EPOC-IV project was launched as a further evolution of the original system. NIEM was chosen as the basis for the common data model for the EPOC-IV project. Based on the NIEM model and the NIEM Naming and Design Rules, approximately 1,084 elements were defined. By comparison,

NIEM has a total of approximately 4,900 elements, so the EPOC model represents a significant effort; and the data model was proven to be 100% NIEM-conformant using the NIEM conformance tools.

PM-ISE is actively promoting these successes and continues to support all government efforts towards standards compliance to enable responsible information sharing.

DHS'S "ISE-READY" CAMPAIGN

The relevancy and importance of standards does not stop once they are incorporated into the acquisition process. Program managers also need to have the tools to understand when their programs are "ISE-ready." In other words, when is a specific program mature enough to provide enterprise information sharing capabilities in conformance with agreed-upon standards? The DHS ISE Ready program is an exemplar.

DHS launched its "ISE Ready" Campaign to assess the current DHS information sharing landscape, and to move the organization toward the target environment envisioned in its information sharing strategy. The Campaign improves responsible information sharing practices across the Department by incentivizing programs to make the cultural shift and proactively change people, policy, data, systems, and infrastructure so that, collectively, their transformed approach to information sharing is "ISE Ready".

"ISE Ready" represents a number of important achievements. First, it means that the Department as a whole is successfully deploying its key responsible information sharing capabilities—Access, Safeguarding, Interoperability, Search/Discovery, Retrieval, and Dissemination—across programs, initiatives, and systems. Second, it means that information sharing and safeguarding architecture (ISSA) is integrated into the planning, acquisition, and management of programs. Finally, being "ISE Ready" means that DHS's senior executive information sharing governing body, the Information Sharing and Safeguarding Governance Board (ISSGB), plays a central role in influencing responsible information sharing investment decisions, and directs the Department toward a greater emphasis on enterprise services for responsible information sharing.

IMPLEMENTING STANDARDS TO IMPROVE RESPONSIBLE INFORMATION SHARING

PROTOTYPE TO CONNECT THE GLOBAL NUCLEAR DETECTION ARCHITECTURE

Under the auspices of the ISA IPC, PM-ISE partnered with DHS's Domestic Nuclear Detection Office (DNDO) to demonstrate the ability to connect the nation's radiological and nuclear detection equipment and to share the sensor information in real time between federal, state, and local Global Nuclear Detection Architecture (GNDA) participants. The successful final demonstration was held in July 2011, during which live displays in watch centers from Los Angeles to Virginia allowed operators and analysts to simultaneously track simulated threat alarm data from sensors around the continent. By reusing a commercially available technology initially deployed in the banking industry and implementing a NIEM-compliant standard for sharing sensor data, DNDO connected the National Network of Fusion Centers and nationwide first responder operations centers – making a low-cost, coast-to-coast, real-time common operational environment possible.

FIRST-RESPONDER INFORMATION SHARING

When a disaster strikes, first responders must immediately share critical data – including requests for equipment and personnel, hospital capacity, and patient tracking information. The Department of Homeland Security's Science and Technology Directorate and its partners have developed a suite of emergency-messaging standards to help responders share data in any form called Emergency Data Exchange Language (EDXL). Each EDXL messaging

standard is vetted by the Organization for the Advancement of Structured Information Standards (OASIS). There are currently four standards approved by OASIS, with two more scheduled to be approved by 2013. The EDXL suite of standards continues to help improve the speed and quality of coordinated response activities in real time. Further, it allows responders to share information about life-saving resources across the full range of local, tribal, state, federal, and non-governmental organizations regardless of mission, background, or boundaries.

GLOBALIZING MARITIME DOMAIN AWARENESS (MDA) WITH DATA STANDARDS: TRIDENT WARRIOR 2011

MDA is an interagency, international effort to detect and prevent threats at sea or in any navigable waterway. The U.S. Navy uses its annual training exercise "Trident Warrior," to test and showcase new MDA concepts and innovations in naval operations. This year's primary objective, to improve information interoperability between the U.S. and coalition partners, saw the British, French, and U.S. navies using NIEM-Maritime (NIEM-M) to track and identify friendly, neutral, and hostile vessels by sharing Automatic Identification Systems data in a NIEM- conformant format. NIEM-M allowed the navies to share more than 10,000 vessel position reports and sort through the data to identify and respond to four suspicious ships that were detected in the area of operations.

NIEM IN CANADA: STANDARDS IN INTERNATIONAL INFORMATION SHARING

In December 2011, PM-ISE and Canadian government representatives met to discuss NIEM adoption for Canada's law enforcement and public safety communities. Canadian adoption of NIEM could accelerate broader international adoption of a standardized approach to information sharing. According to the Royal Canadian Mounted Police Chief Superintendent, Canada is in its infancy in developing data standards and is keen to build on the efforts and success the United States has accomplished with NIEM to improve the management, discovery, fusing, sharing, delivery, and collaboration of intelligence information. As a result, Canada is working towards the development of an ISE/NIEM office to coordinate information sharing standards across the Canadian government. In addition to exploring the establishment of their own Information Sharing Environment, Canada is exploring how to leverage the next version of the SAR functional standard for Canadian interests.

NIEM ADOPTION IN EUROPE

In March 2012, the European Pool against Organised Crime (EPOC) Final Conference in Noordwijk, Netherlands saw 80 participants from 21 EU member countries come together to discuss methods for increasing interoperability for criminal justice applications within the EU. The Conference objectives were to draft a data format to exchange structured data between different case management systems; evolve the EPOC software to connect diverse case management systems across the EU; promote the use of the software across the EU; coordinate the future evolution of the system; and, provide experimental support to the exchange of statistical information. Upon review of all potential solutions, NIEM was used as the basis for the common data model. The EPOC team is now focused on using NIEM as a method to increase interoperability and drive down the cost of implementing information exchanges.

INTERLUDE: CROSS-DOMAIN ADOPTION OF ISE FRAMEWORKS AND CONCEPTS

Information sharing issues and solutions typically revolve around topics of governance, standards, pre-harmonized data vocabularies, and interoperability profiles. There are significant similarities among these issues and solutions irrespective of the business or government domain, traversing public and private sector mission partners and users. This offers a significant opportunity to leverage best practices and resources to solve problems across multiple domains, as is demonstrated by the adoption of NIEM-based exchanges, which originated in the Justice and public safety arena and are now actively being adopted in other areas of the government like health and human services, education, and labor.

The NIEM value proposition is being demonstrated every day across the country as it is applied to addressing compelling social issues such as prescription drug monitoring and human/social services, as well as improving public safety and homeland security. New York State has been a very successful early adopter of NIEM, has some of the largest NIEM reference implementations across multiple domains, and there is growing interest in NIEM in other communities within New York State and in city agencies.

New York City Uses NIEM to Increase Service to Citizens

To better serve its more than 8 million residents, New York City has developed ACCESS NYC, a free website and online tool developed by the NYC Health and Human Services "HHS-Connect Project," which allows users to apply for more than 35 city, State, and federal human service benefit programs; search for office locations; and create pre-populated application forms. The overarching theme of the project is to enable information sharing among disparate NYC agencies by implementing point-to-point data transfers that allow additional agencies to participate by using existing data assets. NIEM made this possible by allowing the same information exchange to be used for data transfer between HHS and the U.S. Department of Education (DOE), as well as between HHS, the NYC Department of Social Services, and the Human Resources Administration (HRA).

NYC HHS Connect was the proud recipient of the 2009 Best of NIEM Award and was also featured in the New York Times in July 2011 with a particular focus on integrated service delivery and how New York City successfully addresses privacy considerations.

New York State Develops a "One-Stop" Integrated Criminal Justice (IJP) Portal

New York State, considered a leader and trendsetter in integrated criminal justice, has recognized that in order to keep up with the evolving demands of their stakeholders in Justice, they needed to upgrade the mainframe-based systems that connected their law and justice entities to more than 20 in-state and out-of-state federal justice agencies and services. The legacy systems, which had evolved over 20 years, were experiencing issues related to age and organic growth, including multiple point-to-point connections, proprietary and legacy protocols and formats, lack of standard business vocabulary, and islands of data with no unified view of information.

The project uses NIEM to develop a "canonical" enterprise view of the information architecture-based data components that were reused among all common and shared services. The Integrated Criminal Justice Portal (IJP) replaces 351 legacy business transactions with NIEM IEPD-based business services, and is deployed in a shared, or cloud, infrastructure. IJP was the proud recipient of the 2011 Best of NIEM Award.

There are a number of projects at the New York State and New York City level that are actively using NIEM to drive data standardization efforts. In a recent NIEM training event hosted in Rochester, NY by the IJIS Institute, there were 78 attendees from the following agencies: Department of Health, Department of Labor, Department of Motor Vehicles, State Education Department, Workers' Compensation Board, Office for People with Developmental Disabilities, and Office of Children and Family Services. Attendees spanned the spectrum from CIOs to technical developers, and represent a glowing example of NIEM's value proposition as an enabler for information sharing.

SECTION 4:
STRENGTHENING SAFEGUARDING TO SUPPORT RESPONSIBLE INFORMATION SHARING

The need to both protect and share national security and counterterrorism-related information stored on and disseminated electronically from U.S. Government information systems has become increasingly critical. Sharing and safeguarding requires that we enforce the controls necessary to protect sensitive and classified information – and the privacy, civil rights, and civil liberties of individuals – while also providing efficient access to mission-critical information in order to enable analysts, operators, and investigators to effectively perform their jobs.

This section describes key achievements over the past year in safeguarding capabilities that most directly relate to the advancement of information sharing, and specifically to the relevant characteristics of the ISE. It does not attempt to describe *all* federal government security-related activities or achievements.

The following list is a summary of specific actions taken over the past year to develop and implement safeguarding capabilities that directly relate to the advancement of information sharing:

- Catalyzed by the WikiLeaks breach, a new federal-wide approach to safeguarding and governance for classified information and systems was developed;
- The President signed EO 13587, affirming the primary responsibility of agencies that handle classified information on computer systems to share and safeguard such information, consistent with appropriate protections for privacy and civil liberties;
- The Senior Information Sharing and Safeguarding Steering Committee (SISSC) began to facilitate implementation of the five near-term tactical priorities for improving the safeguarding of classified information on computer systems;
- The SISSC directed the development and implementation of plans of action with specific milestones to improve technical safeguards on classified networks and established Key Information Sharing and Safeguarding Indicators;
- The National Insider Threat Task Force developed a National Insider Threat Policy to deter, detect, and mitigate insider threats;

- The IC issued ICD 502--*Integrated Defense of the Intelligence Community Information Environment*--and a concept of operations to improve the security of its networks;
- The IC CIO launched a plan to improve the efficiency of the IC Information Technology Enterprise that will significantly enhance the IC's ability to share and safeguard intelligence;
- DoD completed a successful pilot project for sharing cyber-threat information with private sector companies that comprise the Defense Industrial Base;
- DoD is developing plans to issue Public Key Infrastructure (PKI) certificates for federal Secret networks;
- The White House released the Executive branch's proposal for comprehensive cybersecurity legislation, which places a new focus on sharing cyber-threat information, and released its International Strategy for Cyberspace;
- In February 2012, DHS issued an implementing directive for EO 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*;
- The United States and India signed an MOU to promote the timely sharing of cybersecurity information;
- PM-ISE supported the development of cybersecurity information sharing strategies and proposals by applying the ISE's proven information sharing techniques and processes to the cyber-information sharing problem set; and
- PM-ISE established the Classified Information Sharing and Safeguarding Office (CISSO) in concert with E.O. 13587 structural reforms, affirming PM-ISE's cross-cutting leadership role in both information sharing and safeguarding.

SAFEGUARDING-RELATED CHARACTERISTICS OF THE ISE

IRTPA recognized the complex relationship between information sharing and information safeguarding in its description of the characteristics associated with the ISE. As shown in the table below, nearly all of the fifteen characteristics of the ISE enumerated in IRTPA directly involve or strongly imply aspects and capabilities of information and systems security.[44]

[44] IRTPA Sec. 1016 (b)(2).

ISE Characteristic from IRTPA §1016 (b)(2)	PM-ISE Assessment of Safeguarding Aspect
(A) Connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;	"Appropriate" is shorthand for "with appropriate security considerations and mission need"
(B) Ensures direct and continuous online electronic access to information;	"Online" access to information strongly implies the expectation of security controls, which are a feature of all online activity
(C) Facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations, and operations;	"Availability" of information is one of the three pillars of information security – confidentiality, availability, and integrity
(D) Builds upon existing systems capabilities currently in use across the Government;	"Existing systems capabilities" for all federal systems includes security capabilities
(E) Employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;	"Access management" is a key security capability
(F) Facilitates the sharing of information at and across all levels of security;	Horizontal and vertical sharing both entail crossing security domains, and thus, ensuring security
(G) Provides directory services, or the functional equivalent, for locating people and information;	Enabling authorized access and preventing unauthorized access
(H) Incorporates protections for individuals' privacy and civil liberties;	Although protections of privacy and civil liberties are policy-based, implementation of such policies usually involves information technology security controls[45]
(I) Incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls;	Audits, authentication, and access controls are all key security capabilities
(J) Integrates the information within the scope of the information sharing environment, including any such information in legacy technologies;	
(K) Integrates technologies, including all legacy technologies, through Internet-based services, consistent with appropriate security protocols and safeguards, to enable connectivity among required users at the federal, state, and local levels;	Security protocols and safeguards are specifically called out for sharing with all levels of government
(L) Allows the full range of analytic and operational activities without the need to centralize information within the scope of the information sharing environment;	

[45] In fact, NIST's newest version of the federal security controls catalogue, SP 800-53 Rev 4, incorporates security controls for privacy for the first time.

ISE Characteristic from IRTPA §1016 (b)(2)	PM-ISE Assessment of Safeguarding Aspect
(M) Permits analysts to collaborate both independently and in a group (commonly known as 'collective and non-collective collaboration'), and across multiple levels of national security information and controlled unclassified information;	Multiple levels of national security information describes cross-domain functionality – an aspect of security
(N) Provides a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and	"Access" is a key security capability, part of the resolution process described
(O) Incorporates continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.	Audit functions are a key security capability

Table 1. PM-ISE Assessed Safeguarding-related Aspects of the ISE

It is clear that IRTPA views information sharing and information safeguarding as indivisible – two sides of the same coin – and that responsible information sharing is an overarching goal for the ISE.

EXECUTIVE ORDER 13587 AND CLASSIFIED INFORMATION SHARING AND SAFEGUARDING STRUCTURAL REFORMS

Given the ISE's existing mission for responsible information sharing, PM-ISE was a logical focal point for coordinating post-WikiLeaks improvements concerning the sharing and safeguarding of classified information. Consequently, a considerable level of effort was provided by PM-ISE and ISE mission partners over the past year to support the White House's structural reforms. The response to the WikiLeaks breach and subsequent changes to the Federal Government's management of classified information and systems constituted the most visible safeguarding results achieved for the ISE this year.

Both PM-ISE and ISE mission partners participated in the framing of the problem space undertaken by the National Security Staff and the interagency process, and the subsequent Administration decisions on reforms which were announced in May 2011. The President signed Executive Order 13587, detailing structural reforms to improve the sharing and safeguarding of classified information, on October 7, 2011.[lxxxiv]

EO 13587 affirmed the primary responsibility of departments and agencies that handle classified information on computer systems to share and safeguard such information, consistent with appropriate protections for privacy and civil liberties. The executive order also created four new governance entities to help agencies improve classified sharing and safeguarding: the Senior Information Sharing and Safeguarding Steering Committee (the Steering Committee) co-chaired by NSS and OMB; the Insider Threat Task Force, co-chaired by ODNI and the Department of Justice; the Executive Agent for Safeguarding Classified Information on Computer Networks, co-chaired by DoD and NSA; and the Classified Information Sharing and Safeguarding Office (CISSO) within PM-ISE.[lxxxv]

The establishment of the CISSO within PM-ISE affirms PM-ISE's cross-cutting leadership role in both information sharing and safeguarding, and the ISE's special focus on both goals. In further alignment with PM-ISE's broad-based stakeholder community, CISSO is staffed with detailees and assignees, as needed and appropriate, from agencies represented on the Steering Committee. The following ISE mission partners have detailed or assigned personnel to the CISSO: CIA, DHS, FBI (2), and NSA.

The key improvements envisioned by EO 13587 included: affirming classified information sharing and safeguarding as integrated goals, and establishing a governance structure to address both together; mandating the development of a government-wide insider threat policy and program covering for the first time all federal agencies that handle classified information; mandating a third-party independent assessment process covering the security of information, personnel, and systems, to assess the implementation of sharing and safeguarding policies; and the integration of senior-level policy governance with resource management functions to ensure appropriate resourcing alignment with policy priorities.[lxxxvi]

In its first months of operation, the Steering Committee accomplished several key tasks. First, it began to facilitate the implementation of the five near-term tactical priorities for improving the safeguarding of classified information on computer systems. These priorities include:

1. Clarifying and standardizing policies, processes, and technical controls for removable media;
2. Reducing anonymity through improved identity management;[lxxxvii]
3. Creating a national program to address insider-threat issues, and drafting a national insider-threat policy;[lxxxviii]
4. The institution of more robust access controls to enable authorized users access to appropriate classified information and systems, while simultaneously preventing unauthorized access; and[lxxxix]
5. The enhancement of audit capabilities across classified networks.[xc]

Second, the Steering Committee established Key Information Sharing and Safeguarding Indicators (KISSI). These key indicators measure progress, on a recurring and consistent basis, against the five key priorities across all federal departments and agencies that access classified information on computer systems. These key indicators bring together high-level data across all aspects of security to create a consolidated view of the security posture for federal classified information and systems for the first time.

Third, in accordance with EO 13587 and ISE implementation guidance, the National Insider Threat Task Force developed a National Insider Threat Policy to deter, detect, and mitigate insider threats. This policy applies to all agencies that operate or access classified computer networks; all users of classified networks; and all classified information on those networks. It leverages existing federal laws, statutes,

EXECUTIVE ORDER 13587 – STRUCTURAL REFORMS TO IMPROVE THE SECURITY OF CLASSIFIED NETWORKS AND THE RESPONSIBLE SHARING AND SAFEGUARDING OF CLASSIFIED INFORMATION

On October 7, 2011, the President signed Executive Order 13587, which directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks. According to the Order, agencies bear the primary responsibility for sharing and safeguarding classified information, consistent with appropriate protections for privacy and civil liberties. EO 13587 established the Senior Information Sharing and Safeguarding Steering Committee (Steering Committee), which is responsible for fully coordinating interagency efforts and ensuring that agencies are held accountable for implementation of information sharing and safeguarding policy and standards; a Classified Information Sharing and Safeguarding Office (CISSO) within the office of the PM-ISE to provide sustained, full-time focus on sharing and safeguarding of classified national security information; an Executive Agent for Safeguarding Classified Information on Computer Networks (Executive Agent), led jointly by DoD and NSA, to develop technical safeguarding policies and standards and conduct assessments of compliance; and an interagency Insider Threat Task Force (ITTF) to develop a government-wide program for insider threat detection and prevention to improve protection and reduce potential vulnerabilities of classified information from exploitation, compromise or other unauthorized disclosure.

authorities, policies, programs, systems, and architectures in order to counter the threat of any insiders who might use their authorized access to compromise classified information. The policy is in the final stages of review and is expected to be issued in the near term.

Fourth, the Steering Committee directed the development and implementation of plans of actions with specific milestones to improve technical safeguards on classified networks. The Committee is monitoring the implementation of those plans on an ongoing basis.[xci]

Finally, the Steering Committee drafted a 90 Day Report to the President on improving the sharing and safeguarding of classified information on computer networks. Using data from the KISSI exercise and a number of other sources, this report found a number of incremental improvements since the WikiLeaks incident, as discussed in the classified supplement. Pursuant to EO 13587, subsequent improvements will be reported on annually to the President each year.

OTHER KEY SAFEGUARDING ACCOMPLISHMENTS

While EO 13587 and classified information sharing and safeguarding were a key focal point over the past year, a number of safeguarding accomplishments continued for the ISE's existing, characteristics-based responsible sharing mission. The section below highlights key safeguarding results achieved by the five ISE communities. These results are cross-walked to the ISE characteristics they support.

INTELLIGENCE COMMUNITY (IC)

Enhancing auditing capabilities across Federal Government classified networks is a priority, and planning has been initiated to define the policy and develop standards for collecting and sharing audit data. In June 2011 ODNI issued Intelligence Community Standard (ICS) 500-27, *Collection and Sharing of Audit Data*, which mandates that audit data be collected on all IC information resources and shared with each user's IC element. This collection effort includes audit data on both contractors and government personnel. This standard identifies the minimum set of audit data that will be collected and shared to support community audit needs.[xcii]

In 2011, the Intelligence Community completed a new directive, ICD 502, *Integrated Defense of the Intelligence Community Information Environment,*[46] and a concept of operations to improve the security of its networks. This policy specifically calls for "procedures for defending the IC information environment from threats or incidents that could affect information sharing or the protection of sources and methods from unauthorized disclosure"[47] and requires IC elements to report and share information regarding security incidents and vulnerabilities.[xciii] ICD 502 and its associated operational guidelines provide key improvements in sharing security information as a means to protect networks. PM-ISE participated in the development of this guidance, and is providing advice on developing the first national exercise to test the implementation of the policy, in 2012.

In the past year, as announced by Director Clapper in October 2011, the IC also launched a plan to improve the efficiency of the IC Information Technology Enterprise (ITE). In addition to providing cost savings, this initiative is expected to improve the overall integration of the IC and to support information sharing. The development of the ITE will support assured sharing in the following ways:

- Enable interoperability and increased use of common standards, including identity, credential, and access management standards;

[46] http://www.dni.gov/electronic_reading_room/ICD_502.pdf
[47] ICD 502, section (D)(2)(a)(1).

- Enable shared architectures such as cloud platforms and common services; and
- Enable improved security through improved sharing of cybersecurity situational awareness, audit processes, and insider threat information.

DEFENSE

The Defense community recently completed a successful pilot project for sharing cyber-threat information with private sector companies that comprise the Defense Industrial Base (DIB). In May, 2012, the DoD issued an Interim Final Rule,[48] expanding an existing voluntary cybersecurity information sharing program between DoD and eligible DIB companies, and outlining the eligibility and other operational requirements for participation in the newly expanded program. The Interim Rule authorizes eligible companies to receive certain threat information and to share information regarding network intrusions that could compromise critical DoD programs and missions. This effort represents important progress in overcoming the legal, policy, and technical barriers to sharing classified cyber-threat information between the Federal Government and the private sector.[xciv]

In 2012, the DoD developed an implementation plan for the migration to PKI hard-token access for all Secret networks. In becoming a provider of shared services to other federal agencies, DoD is leveraging its expertise to gain efficiencies for the Federal Government as a whole.

DoD is becoming a provider of Public Key Infrastructure (PKI) certificate shared services to other federal agencies, leveraging its expertise to gain efficiencies for the Federal Government as a whole. This will facilitate the development of interoperable certificates, which will support information sharing among the different agencies that operate and use federal Secret networks.[xcv]

HOMELAND SECURITY AND CRITICAL INFRASTRUCTURE

Given the increasing frequency, impact, and sophistication of attacks on information and information systems in the United States, cybersecurity is an increasing focus for national security efforts. The Federal Government has a complex role in cybersecurity, which includes protecting federal systems and information, and assisting the private sector in protecting systems that comprise the nation's critical infrastructure.

While there are many technical aspects to protecting systems and information from cyber-threats, a key function underlying many cyber defense and response activities is effective, secure information sharing. This critical linkage was recognized in the White House's 2009 Comprehensive National Cybersecurity Initiative (CNCI), particularly in Initiative #5, which calls for sharing and collaboration among federal strategic operations centers.

The critical role of information sharing in cybersecurity has found renewed emphasis during the past year. In the summer of 2011, the White House released the Executive branch's proposal for comprehensive cybersecurity legislation, which aimed to update a number of existing cybersecurity laws but also placed a new focus on sharing cyber-threat information between the Federal Government and private sector owners of critical infrastructure.[xcvi] In response to this proposal and throughout the past 12 months, Congress has developed and introduced a number of bills related to cybersecurity, many of which contain provisions mandating improved cybersecurity information sharing and cross-sector coordination.

PM-ISE has supported the development of cybersecurity information sharing strategies and proposals, through applying the ISE's proven information sharing techniques and processes to the cyber information sharing problem set. PM-ISE has also provided assistance in developing solutions to leverage ISE privacy protections to cyber-

[48] DoD-Defense Industrial Base (DIB) Voluntary Cyber Security Information Assurance (CS/IA) Activities, 77 Fed. Reg. 27615 (May 11, 2012).

defense network-monitoring processes. In the coming year, as new legislation emerges in this area, information sharing related to cybersecurity functions will play an increasing role in the ISE.

STATE, LOCAL, AND TRIBAL GOVERNMENTS

In accordance with FY2012 ISE Implementation Guidance, DHS issued an implementing directive for EO 13549, *Classified National Security Information Program for State, Local, Tribal, and Private sector Entities*, in February 2012. Under the authority of the Order, and through the implementing directive, a governance and oversight structure are put in place that will serve to instill and promote the uniform application of security standards within the Executive branch and SLTPS communities, while maintaining consistency with existing polices and standards as promulgated through statutes, executive orders, regulations, and other directives. This directive, which represents the combined and collaborative efforts of stakeholders within the Federal and SLTPS communities, will serve to lay a consistent security foundation across the ISE, thereby enhancing the confidence necessary to support classified information sharing.

Cybersecurity Information Sharing and the Comprehensive National Cybersecurity Initiative

Initiative #5. Connect current cyber ops centers to enhance situational awareness.

There is a pressing need to ensure that government information security offices and strategic operations centers share data regarding malicious activities against federal systems, consistent with privacy protections for personally identifiable and other protected information and as legally appropriate, in order to have a better understanding of the entire threat to government systems and to take maximum advantage of each organization's unique capabilities to produce the best overall national cyber defense possible. This initiative provides the key means necessary to enable and support shared situational awareness and collaboration across six centers that are responsible for carrying out U.S. cyber activities.

The National Cybersecurity and Communications Integration Center within the Department of Homeland Security will play a key role in securing U.S. Government networks and systems under this initiative by coordinating and integrating information from the six centers to provide cross-domain situational awareness, analyzing and reporting on the state of U.S. networks and systems, and fostering interagency collaboration and coordination. (http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative)

INTERNATIONAL PARTNERS

INTERNATIONAL STRATEGY FOR CYBERSPACE

In May 2011, the White House released its International Strategy for Cyberspace.[49] The International Strategy lays out the President's vision for the future of the Internet, and sets an agenda for partnering with other nations and peoples to achieve that vision. This strategy recognizes the successes that networked technologies have brought us, due in large part to the freedom and innovation that has characterized the Internet. While the strategy is realistic about the challenges of securing cyberspace, it emphasizes that U.S. policies must continue to support the core principles of freedom, privacy, and the free flow of information.

In launching the strategy, Howard Schmidt, the President's former Cyber Security Advisor, issued a call for international sharing and safeguarding:

"To achieve our vision, the United States will build an international environment that ensures global networks are open to new innovations, interoperable the world over, secure enough to support people's work, and reliable enough to earn their trust. To achieve it, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law.

"The International Strategy is larger than any one department or

[49] http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

agency. It is a strong foundation for the diverse activities we will carry out across our entire government. It is about the principles that unite our nation, the vision that unites our policy, and the priorities that unite our government.

"With our partners around the world, we will work to create a future for cyberspace that builds prosperity, enhances security, and safeguards openness in our networked world. This is the future we seek, and we invite all nations, and peoples, to join us in that effort."[50]

THE UNITED STATES AND INDIA SIGN CYBERSECURITY AGREEMENT

In July 2011, The United States and India signed an MOU to promote closer cooperation and the timely sharing of information between the organizations of their respective governments that are responsible for cybersecurity. The MOU establishes best practices for the exchange of critical cybersecurity information and expertise between the two governments through their respective Computer Emergency Response Team components. Through this arrangement, the respective governments and the broader cybersecurity communities in both the United States and India will have the ability to coordinate with their counterparts on a broad range of technical and operational cyber issues.[xcvii]

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) AND THE INTERNATIONAL ELECTRO-TECHNICAL COMMISSION (IEC) PUBLISH NEW STANDARDS ON BIOMETRIC DATA SECURITY

In August 2011, ISO and IEC published a joint security and privacy standard - *ISO/IEC 24745:2011, Information technology – Security techniques – Biometric information protection* – regarding the use of biometric data for authenticating persons when accessing applications via the internet.

Biometrics is regarded as a powerful solution for authentication because of its unique link to an individual that is nearly impossible to fake. Maintaining the security of biometric information, however, is critical, because unlike other authentication methods, such as passwords or tokens, problems with compromised biometric data can be nearly impossible to rectify. To address these concerns, the new standard outlines specific "solid countermeasures" to protect the security of biometric data while ensuring personal privacy. While on the one hand, the distinct association with an individual provides assured authentication, the binding which links biometrics with personally identifiable information carries some risks, including the unlawful processing and use of data. ISO/IEC 24745 is an invaluable tool for addressing those risks.[51xcviii]

UPDATE ON POLICY/PROCEDURAL FRAMEWORK FOR SECURITY RECIPROCITY

Developing security measures that are commonly understood across communities - using common taxonomies, security controls, and processes – is foundational to increasing trust among interconnected mission partners. The benefits of transparency and commonality for security measures are well known: increased efficiency through reciprocity and reuse, increased transparency supporting informed risk management decisions at all levels, and, of course, support for increased interoperability and assured information sharing.

The premier effort blazing the trail toward a common federal baseline for information technology security has been the National Institute for Standards and Technology's (NIST's) *Joint Task Force Transformation Initiative*. This multi-year initiative is an ongoing collaboration between the Department of Defense, the Intelligence Community, the Committee on National Security Systems, and the Department of Homeland Security to develop a core suite of five IT systems security standards that all federal departments and agencies can reference in developing security

[50] http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace
[51] http://www.iso.org/iso/catalogue_detail?csnumber=52946

protocols tailored to their specific environments; in effect forming a de facto common security standards baseline for all federal IT systems.

NIST Special Publication	Date of Latest Release	Title
SP 800-30 Rev. 1	Sept. 19, 2011	DRAFT Guide for Conducting Risk Assessments
SP 800-37 Rev. 1	Feb. 2010	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
SP 800-39	Mar. 2011	Managing Information Security Risk: Organization, Mission, and Information System View
SP 800-53 Rev. 4	Feb. 28, 2012	DRAFT Security and Privacy Controls for Federal Information Systems and Organizations (Initial Public Draft)
SP 800-53 A Rev. 1	Jun. 2010	Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans

Table 2. NIST IT Systems Security Special Publications[52]

Significant progress was made on the *Joint Task Force Transformation Initiative* over the past 12 months, with the publication of Special Publication 800-30 Revision 1 and Special Publication 800-53 Revision 4. In particular, the publication of an expanded security controls catalogue, SP 800-53, Revision 4, represents the culmination of a year-long initiative to update the content of the security controls catalog and the guidance for selecting and specifying security controls for federal information systems and organizations.[xcix]

Major changes in Revision 4 include:

- New security controls and control enhancements;
- Clarification of security control requirements and specification language;
- New tailoring guidance, including the introduction of overlays;
- Additional supplemental guidance for security controls and enhancements;
- New privacy controls and implementation guidance;
- Updated security control baselines;
- New summary tables for security controls to facilitate ease-of-use; and
- Revised minimum assurance requirements and designated assurance controls.

In addition to the five core security standards that form the common federal baseline, in September 2011 NIST also issued Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.[c] This new guidance supports White House priorities[53] for cybersecurity, the Federal

[52] http://csrc.nist.gov/publications/PubsSPs.html
[53] http://www.whitehouse.gov/blog/2012/03/23/federal-departments-and-agencies-focus-cybersecurity-activity-three-administration-p?utm_source=related

Government's overall move towards improved security through continuous monitoring techniques, and advocates using automated tools to optimize monitoring. The special publication further recommends that automated tools be interoperable to enable sharing information among security tools, and to support enterprise-wide Security Information and Event Management (SIEM) functions.

Collectively, these special publications form a common foundation to improve the overall security of all federal IT information technology systems, and also support the enablement of assured information sharing among the widest possible set of stakeholders.

Initiatives for Cyber Information Sharing

PM-ISE and ISE mission partners are working within the following cybersecurity initiatives to improve cyber-threat information sharing.

National Level Exercise 2012

The National Level Exercises (NLE) are a series of congressionally mandated preparedness exercises designed to prepare participants for potential catastrophic events. NLE 2012 will emphasize the shared responsibility among the government, the private sector, and the international community to secure cyberspace and respond together to a cyber incident. (http://www.fema.gov/plan/nle)

DoD-Defense Industrial Base Cyber Pilot

In May 2012, the Department of Defense expanded a cybersecurity information sharing program between DoD and Defense Industrial Base companies. This expansion authorizes eligible companies to receive certain threat information in return for sharing network intrusion information that could compromise DoD programs and missions. (http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf)

INTERLUDE: EXTENDING ISE BEST PRACTICES – "LATERAL" IMPLEMENTATION

Cyberspace is increasingly being used by terrorists for operational activities,[54] and the threat of cyber terrorism has been a focus of worldwide concern since the well-publicized cyber-attacks against Estonia (2007) and Georgia (2008). Current and former top U.S. officials, including the former director of the CIA's Counter-Terrorism Center[55] and Deputy Secretary of Defense William J. Lynn,[56] have predicted the expansion of terrorist capabilities for using cyberspace for destructive attacks.

As with traditional terrorist threats, sharing information about cyber-threats and incidents – with the right people at the right time - is widely viewed as a key means to protect the nation's networks and the critical infrastructure which they support. However, also as with traditional terrorist threats, cyber-based threats are subject to the same challenges to information sharing:

- Whom to share with, and the establishment of trust;
- What information to share, and at what classification level;
- The means to share, including common standards, architectures, and information repositories;
- Organizational culture and biases against sharing;
- Timeliness of sharing, and the need for "real time" dissemination of critical threats;
- Sharing across security classification domains and extremely broad stakeholder communities;
- Handling and making sense out of large volumes of threat data to achieve effective decision support and action;
- Insufficient collaboration between mission owners and the technical operators who provision secure platforms; and
- Protecting privacy and civil liberties while sharing.

[54] "*Terrorist Use of the Internet: Information Operations in Cyberspace*." Congressional Research Service. March 8, 2011.
[55] Ferran, Lee "*Former CIA Counter-Terror Chief: Al Qaeda Will Go Cyber*." August 4, 2011. http://abcnews.go.com/Blotter/cia-counter-terror-chief-al-qaeda-cyber/story?id=14224256
[56] "Remarks on the Department of Defense Cyber Strategy." As Delivered by Deputy Secretary of Defense William J. Lynn, III, National Defense University, Washington, D.C., Thursday, July 14, 2011. http://www.defense.gov/speeches/speech.aspx?speechid=1593

Consequently, the tactics, tools, and processes developed by the ISE to improve traditional counterterrorism-related information sharing are highly extensible to the cyber-threat information sharing problem space. PM-ISE and ISE mission partners are beginning to extend ISE information sharing solutions to the effort to share cyber-information in the following ways:

- Driving the development of standard data formats, like NIEM, and processes, like SAR, for cyber-threat and incident information sharing;
- Promoting adoption of common standards through requirements definitions for acquisitions;
- Promoting the development of mechanisms for common governance, such as those outlined in E.O. 13587, to build trust among stakeholders, facilitate agreement on common needs, and act collectively;
- Supporting the development of policies, like E.O. 13549, to facilitate assured sharing of classified information with appropriate non-federal partners; and
- Leveraging the ISE's privacy guidelines as a model for protecting privacy when sharing cyber-threat and incident information.

PM-ISE expects the focus on cyber-terrorism and the need to share cyber-threat and incident information to continue in 2012. A number of developments support this outlook. New cybersecurity legislation, including programs that directly address cyber-threat information sharing, is progressing in Congress. National exercises involving cyber-threat scenarios are uncovering persistent information sharing gaps, which are hindering the defense of federal networks. Consolidation of security tools by industry through procurements sets the stage for the development of integrated security product suites – and an opportunity to influence interoperability. Existing initiatives for improving the security of our networks and information continue to mature.

And, of course, the threat from cyber-based attacks to our national critical infrastructure continues.

"Underlying all of these [cyber defense] efforts is the need to acquire the best possible information about the state of our networks and the capabilities and intentions of our cyber adversaries. We must also make critical cybersecurity information available to and usable by everyone who needs it, including network operators and defenders, law enforcement and intelligence agencies, and emergency management officials in the Federal, State, local, and tribal governments, private industry, and allied governments."

http://www.whitehouse.gov/cybersecurity"

This page intentionally left blank

SECTION 5:
IMPLEMENTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTIONS

Counterterrorism efforts hinge on the timely access to and analysis of often very personal details and circumstances of individuals and organizations that pose threats to U.S. national security. Departments and agencies assess the need for information to mitigate threats to our national security while preserving the cherished constitutional protections and legal rights granted to Americans.

To ensure that information is shared in a manner consistent with privacy, civil rights, and civil liberties (P/CR/CL) protections, it must be understood in the organizational culture, business processes, and technologies, and be reinforced in training. These protections are mandated by law, including: the Intelligence Reform and Terrorism Prevention Act and Privacy Act (IRTPA); various Executive Orders; and the 2007 National Strategy for Information Sharing.

The following section provides an assessment of the P/CR/CL protections afforded in the ISE. Actions taken in the preceding year to implement or enforce these protections in accordance with IRTPA include increased focus on development and implementation of federal policies consistent with the ISE Privacy Guidelines; training for fusion centers and front-line law enforcement officers; and expanded membership to the ISA IPC's Privacy and Civil Liberties (P/CL) Subcommittee to include a state and local advisory representative. Performance data is provided where it exists for selected initiatives.[ci]

The following list is a summary of specific actions taken over the preceding year to implement or enforce the P/CR/CL protections afforded in the ISE:

- ISE mission partners made significant progress in either issuing or developing privacy policies consistent with the ISE Privacy Guidelines;
- All federal partners reported having some mechanisms in place that allow for agency verification that personnel are in compliance with agency privacy and civil liberties policies;
- Sixteen state and major urban area fusion centers have conducted peer-to-peer P/CR/CL compliance reviews using a compliance verification template issued by Global and the Criminal Intelligence Coordinating Council (CICC); and

- All ISE departments and agencies reported that their training addresses the protection of privacy and civil liberties.

DEVELOPMENT AND IMPLEMENTATION OF ISE PRIVACY POLICIES

The ISE Privacy Guidelines ("Guidelines"), mandated by IRTPA, and approved by the White House in 2006, established the framework for the sharing of terrorism-related information through the ISE while protecting P/CR/CL. The Guidelines set forth core P/CR/CL principles and require ISE departments and agencies to implement policies and processes to protect the P/CR/CL of U.S. citizens and legal permanent residents in the sharing of such information.[57] The Guidelines also require non-federal partners seeking to access this information from federal partners to put in place protections that are "at least as comprehensive" as those contained in the Guidelines.

ISE mission partners continue to progress in the development and implementation of policies, business processes, and procedures consistent with the ISE Privacy Guidelines. As shown in the figure below, significant progress has been made since the issuance of the Guidelines. As of June 30, 2012, nine ISE agencies have issued ISE privacy policies and submitted their policies to the ISA IPC P/CL Subcommittee. The Department of Defense, the Department of Energy, and the Department of Commerce have developed draft policies and are moving those policies through formal departmental clearance. The Department of Treasury has drafted its privacy policy, but has deferred formal departmental clearance until the proposed policy is validated through completion of a pilot for the interagency compliance review self-assessment checklist under development by the P/CL Sub-Committee. The Department of Health and Human Services is on schedule for completion of its ISE privacy policy by October 2012,[cii] per ISE implementation guidance.[58]

[57] Section 1016(d)(2)(A) of IRTPA required the President to issue guidelines to "protect privacy and civil liberties in the development and use of the ISE." In response, and under the authority of the Homeland Security Act of 2002, Executive Order 13388 and other Presidential authorities, the President issued Guideline 5, "Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment," which implemented this requirement. http://www.ise.gov/sites/default/files/guideline%205%20-%20privacy%20rights%20and%20legal%20protections.pdf. Guideline 5 addressed the mandate to develop "guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information."

[58] Implementation Guidance for FY 2013 Programmatic Guidance for the Information Sharing Environment (ISE), PM-ISE memo dated August 8, 2011.

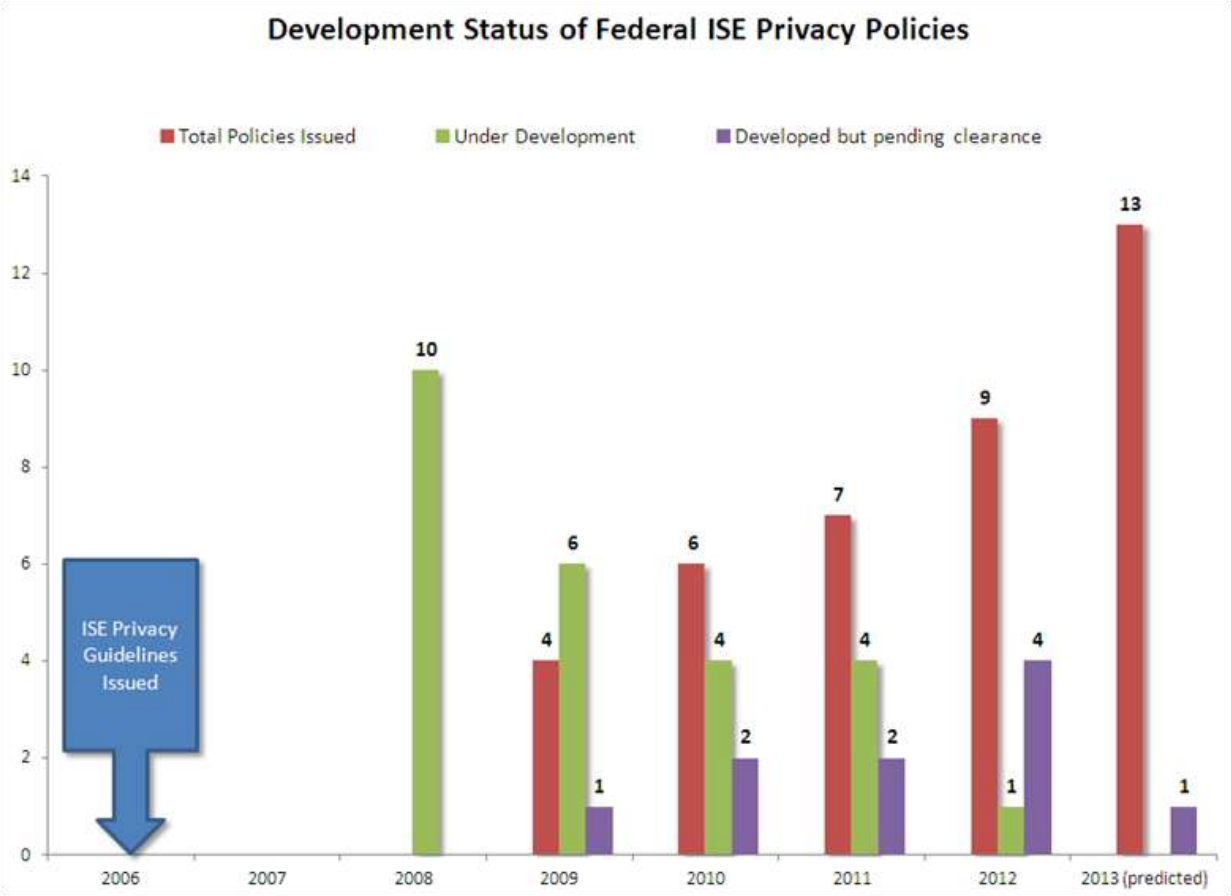


Figure 1. Timeline of Federal ISE Privacy Policy Development and Issuance[59]

In 2011, all designated state and major urban area fusion centers were determined by the DHS Privacy Office to have privacy policies that are "at least as comprehensive" as the ISE Privacy Guidelines[ciii]. 79% of federal ISE mission partners reported that few (0-20%) agency programs or business processes require modification to align with the agency's ISE privacy policy. While some agencies are still identifying potential modifications, other agencies have incorporated requirements into their planning cycle, resulting in limited modifications to ensure alignment with privacy policies. As DHS notes, "DHS processes are designed to incorporate privacy from the onset." A new measure for 2012 focused on the number of complaints received that would require action under the agency's ISE privacy policy. No federal ISE mission partner reported receiving any complaints that met these criteria.

All federal ISE partners reported having some mechanisms in place to verify that personnel are in compliance with their privacy and civil liberties policies. As of mid-2012, 16 fusion centers have conducted peer-to-peer P/CR/CL compliance reviews using a compliance verification template developed and issued by Global and the Criminal Intelligence Coordinating Council (CICC)[civ].

[59] Figures reflect an eventual total of 14 federal departments and agencies. The difference in yearly totals is due to the fact that some agencies did not begin development of their ISE privacy policies until after 2010.

PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES (P/CR/CL) TRAINING AND OUTREACH

ISE mission partners have placed a strong emphasis on training and technical assistance in order to standardize and reinforce P/CR/CL protections. All ISE departments and agencies reported that their respective training addresses the protection of privacy and civil liberties. For example, DoD reports that in addition to annual privacy training, it is in the process of "instituting additional civil liberties training for those personnel with specialized civil liberties requirements."

DHS CRCL and Privacy Offices, with support from DHS I&A, have created a four-pronged program to support fusion centers that includes the following: 1) on-site training for staff at fusion centers; 2) train-the-trainer course for fusion center privacy and civil liberties officers (delivered with support from the PM-ISE); 3) a Web portal (www.it.ojp.gov/PrivacyLiberty) that provides a single point of access to federal resources that provide guidance and/or training on P/CR/CL issues in the ISE; and 4) a technical assistance program for the fusion center privacy and civil liberties officers[cv].

PM-ISE Establishes a Social Media Presence

In August 2011, the PM-ISE became the first component of the ODNI to establish an official presence on Facebook and Twitter. PM-ISE conducted an adapted Privacy Impact Assessment of its intended use of social media (available at http://ise.gov/privacy-impact-assessments) and developed privacy policies for the ISE.gov website, PM-ISE's use of social media, and a comment policy for PM-ISE's Blog and PM-ISE's presence on social media sites (available at http://ise.gov/site-policies). The PM-ISE is committed to communicating with its partner communities through the use of technology, and in a way that is transparent and compliant with applicable privacy safeguards.

As part of the training "road show," DHS has trained 1,046 fusion center staff and liaison officers since 2009. Additionally, an estimated 650 staff, liaison officers, and other fusion center personnel have been trained as part of various workshops and other presentations. As of the end of the second quarter of FY 2012, DHS had conducted training at 34 sessions hosted by 38 fusion centers in 25 states and the District of Columbia. DHS anticipates training fusion centers in another 14 states by the close of FY 2012, at which time DHS CRCL will have trained fusion center staff in three-quarters of the states. DHS has also trained the privacy and civil liberties officers from 68 of the 77 total fusion centers. The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) has developed and implemented a comprehensive and multi-tiered approach to analyst/investigator training, emphasizing the importance of P/CR/CL protections in the process of identifying and documenting suspicious activity[60], as discussed later in Section 6. The NSI PMO has been working to expand training to personnel from fire, emergency management, public safety and private sector critical infrastructure; and anticipates rolling out this training program in mid-2012.

In addition to the 64% of agencies reporting outreach activities with state, local, tribal, and private sector partners, the ISA IPC P/CL Sub-Committee's Executive Committee participated in ISE-hosted events, including a Data Aggregation Summit, a Workshop for Information Sharing and Safeguarding Standards (WIS3), and a conference on Adapting and Improving an Expanded Information Sharing Environment.

[60] The ISE SAR Functional Standard version 1.5 defined "suspicious activity" as "[o]bserved behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." See http://ise.gov/sites/default/files/ISE-FS-200 ISE-SAR Functional Standard V1_Issued 2009.pdf.

PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTIONS AND OPERATIONAL MISSIONS

Federal, state, local, and tribal partners have continued to operationalize the legal and policy framework for P/CR/CL by modifying business processes and updating sharing agreements to align with ISE P/CR/CL protections. For example, the FBI and NSI PMO, in conjunction with the ISA IPC, are working to modify the business processes to ensure that all SARs get reported to the FBI, either through eGuardian or through the NSI Shared Space.

Looking forward, mission partners are considering how they can identify the requirements for and the foundational research needed to automate the implementation of ISE privacy protection policies while facilitating streamlined information exchanges. DHS and the PM ISE have forged a close working relationship to lead the federal effort to build the first iteration of a standardized set of machine-interpretable and implementable rules for a data safeguarding and handling policy[cvi].

PRIVACY AND CIVIL LIBERTIES (P/CL) SUB-COMMITTEE

The Privacy and Civil Liberties (P/CL) Sub-Committee consists of senior privacy and civil liberties officials from all departments and agencies who are represented on the ISA IPC. The Sub-Committee is guided by an Executive Committee consisting of senior privacy and civil liberties officials of ODNI, DHS, and DoJ.

In 2011, the leadership of the P/CL Sub-Committee rotated from the Civil Liberties Protection Officer for the Office of the DNI to the DHS Officer for Civil Rights and Civil Liberties.[61] The rotation of leadership demonstrates both shared commitment and shared responsibility for implementing P/CR/CL protections throughout the Federal Government.

The Sub-Committee also includes representation from an advisory group consisting of state and local ISE partners, who contribute valuable insight into operational realities and incorporate state and local perspectives into Sub-Committee deliverables.

In 2011, the Sub-Committee and its working groups have remained active in examining P/CR/CL protections in the ISE by:

- Establishing a mechanism by which the Sub-Committee would provide advisory opinions to other ISA IPC Sub-Committees, working groups, and member agencies;
- Examining the ISE Privacy Guidelines and making recommendations to the ISA IPC on potential clarifications and/or revisions;
- Drafting a proposed compliance review self-assessment checklist designed to assist federal ISE partners in identifying gaps in their agency's compliance with both the polices and the related internal procedures implementing those guidelines;
- Collaborating with other ISA IPC Sub-Committees and working groups in: drafting a response to the Deputies Committee report on US Government Data Aggregation capabilities; considering options for the automation of information policies, including privacy policies; and working on aligning the FBI's eGuardian system with the policy requirements and standards of the NSI;
- Finally, in accordance with FY2013 ISE Implementation Guidance, the Sub-Committee reviewed and concurred with the P/CR/CL protections afforded to U.S. Persons as part of the watchlisting nomination and screening processes[cvii]

[61] With the departure of the DHS Officer for Civil Rights and Civil Liberties in 2011, the DHS Chief Privacy Officer took on the leadership role of the P/CL Sub-Committee.

This page intentionally left blank

INTERLUDE: FEDERAL IMPLEMENTATION OF THE ISE – "FROM THE TOP DOWN"

Effective and responsible information sharing requires strong commitment and participation from agencies. A number of ISE partners have embraced the ISE culture in their planning and implementation – they have developed effective internal governance structures and practical measures to ensure that information sharing and risk management goals and objectives are fully integrated in their day-to-day operations.

In particular, the Department of Homeland Security (DHS) is an exemplar of an agency that has built an outstanding culture for advancing responsible information sharing. Their commitment to implementing and innovating information sharing best practices throughout the Homeland Security Enterprise sets the standard for the ISE as a whole. DHS senior leadership has established an effective department-wide internal governance structure to develop policies and to oversee the execution of responsible information sharing priorities. DHS's most senior leaders take active, hands-on roles in the Department's information sharing governance processes, and through their guidance and direction ensure that the complex information needs of the Homeland Security Enterprise are met through effective coordination within the Department. In addition, the Department's active participation in government-wide responsible information sharing governance through the ISA IPC, the Senior Information Sharing and Safeguarding Steering Committee, the Committee on National Security Systems (CNSS), and other interagency committees such as the Intelligence Community Information Sharing Steering Committee, ensure information exchanges between and among federal, state, local, tribal, and territorial partners and the private sector.

> *"The need to securely share actionable, timely, and relevant classified information among state, local, tribal, and private sector partners in support of homeland security is critical as we work together to address evolving threats."*
> - DHS Secretary Janet Napolitano, 9 March 2012, Issuance of Directive to Strengthen the Sharing of Classified Information with State, Local, Tribal, and Private Sector Partners

DHS's Information Sharing and Safeguarding Governance Board (ISSGB) is their executive-level steering committee and policy-making body for information sharing in the Department. Chaired by the Under Secretary for Intelligence and Analysis, who serves as the Department's Chief Executive for Information Sharing, the ISSGB provides DHS leaders with a forum for overseeing responsible information sharing initiatives, strengthening partnerships, and de-conflicting issues. The Department uses this committee to assign responsibility and track the progress of more than 60 priority tasks that were contained in the FY2013 ISE Implementation Guidance. As a result of this oversight capability, DHS has met all milestones to date. In October 2011, the ISSGB adopted a new charter, broadening its mission to address information safeguarding and expanding Board membership to include additional Departmental leaders in responsible information sharing – this included appointing the DHS CIO as Vice Chair and appointing the Department's Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties as full voting members.

Further, in the wake of the post-WikiLeaks reform, DHS chartered the Information Safeguarding and Risk Management Council (ISRMC) as part of its information sharing governance structure. The ISRMC addresses many of the responsibilities of the Department resulting from Executive Order 13587. It is intended to ensure that information on both classified and unclassified networks is properly protected to preserve privacy and civil liberties.

Beyond driving information sharing efforts within the Department, DHS has been engaged with federal interagency efforts as an active member of the ISA IPC, filling key leadership roles in the IPC's sub-committees and working groups. DHS also participates in the Intelligence Community Information Sharing Steering Committee, chaired by the IC Information Sharing Executive. In order to provide homeland security information sharing expertise, DHS has deployed detailees to a number of ISE Departments and Agencies, including the PM-ISE and the Intelligence Community, to foster greater interagency cooperation. Through engagement in these interagency forums, DHS has been a key partner on core ISE initiatives including support for the National Network of Fusion Centers, the Nationwide Suspicious Activity Reporting Initiative, Sensitive But Unclassified interoperability, and Federal Government-wide data aggregation efforts.

"For all of the U.S. government, threats require us to accelerate responsible information sharing."
- Director of National Intelligence James Clapper, 26 January 2012, Center for Strategic and International Studies Forum on Information Sharing

It's important to note that the strong partnerships between DHS and the Intelligence Community noted above are possible not only due to DHS's active pursuit of information sharing opportunities, but are also made possible by ODNI's responsible information sharing activities. The ODNI leadership's sustained commitment to information sharing across the Intelligence Community is evidenced by their publishing of the DNI's *2011-2015 Strategic Intent for Information Sharing,* which provides the framework to improve responsible and secure sharing across the IC as well as with external partners and customers. It supports the DNI's strategic goal to "Drive Responsible and Secure Information Sharing," and is fully consistent with both the *National Intelligence Strategy* and the Administration's priorities for information sharing and safeguarding.

ODNI oversees the implementation of the strategy's goals through the IC Information Sharing Steering Committee – the IC's executive-level information sharing governance body. External to the IC, the IC Information Sharing Executive[62] is a member of both the ISA IPC and the Senior Information Sharing and Safeguarding Steering Committee, and collaborates very closely with PM-ISE to identify best practices for information sharing across the Federal Government. Like DHS, ODNI makes responsible information sharing a priority and gives weight to their information sharing initiatives – backing them with the authority of their most senior leaders. ODNI and NCTC senior leadership, such as the Civil Liberties Protection Officer, serve in key leadership roles on ISA IPC sub-committees and working groups. By replicating the actions and commitment of both DHS and ODNI across the federal ISE, stakeholders will serve to strengthen and mature government-wide information sharing and advance broader ISE priorities.

[62] In 2010, the Director of National Intelligence appointed an Intelligence Community Information Sharing Executive (IC ISE) to serve as the DNI's senior accountable officer providing oversight and program management for all Offices of the Director of National Intelligence (ODNI) and Intelligence Community (IC) information sharing efforts. The IC ISE coordinates activities within the ODNI and across all IC elements to prioritize, harmonize, and accelerate information sharing initiatives.

SECTION 6:
MANAGING AND FOSTERING A CULTURE OF RESPONSIBLE INFORMATION SHARING

Exercising government-wide authority over responsible sharing of terrorism-related information requires PM-ISE and ISE agencies to foster a culture that is built upon mutual trust and a shared responsibility for the overall national security mission. Integrated governance, ISE-wide performance management, budget-performance integration, training that extends to all mission partners, incentives in the form of personnel appraisal objectives and award criteria, promotion of collaboration events, and tools and sourcing of best practices and innovations are the means to mature the culture from a partially-realized ISE to a tightly knit association of mission partners whose development, adoption, and implementation of common practices and standards comprise a coherent whole.

The following list is a summary of specific actions taken over the preceding year to mature the management capabilities in the ISE:

- ISE agencies are increasingly assigning executives and dedicated staff to oversee responsible information- sharing functions;
- DHS and federal partners hosted a series of workshops and seminars on countering violent extremism, analytic tradecraft, security, classified information sharing, and fusion center liaison programs;
- NSI PMO, in partnership with PM-ISE, developed and is now implementing Suspicious Activity Reporting (SAR) awareness training for other key non-law-enforcement constituencies, or "hometown security partners" that are important to the SAR effort;
- NSI developed an NSI Federated Search Tool Technical Assistance process;

Federal, State, Local, and Tribal Information Sharing: Diversity of Stakeholders and Communities Involved

- 300+ million people
- 50 States
- 3,000+ counties
- 500+ Federally recognized Indian Tribes
- 18,000+ Law Enforcement Organizations
- 1 million+ Security personnel

U.S. law provides for a reasonable expectation of privacy for all U.S. persons.

- The FBI developed three Web-based, information sharing-related training modules and made them available to federal, state, local, and tribal law enforcement partners and fusion center personnel via their Unclassified Virtual Academy;
- The National Association of Security Companies (NASCO), the nation's largest contract security industry association, endorsed the SAR Training Video for private sector security personnel;
- Agencies increased the nomination of candidates for information sharing and collaboration awards;
- PM-ISE, in partnership with DHS, convened the National Fusion Liaison Officer Program Workshop to facilitate sharing of best practices and lessons learned across the National Network; and,
- PM-ISE created a set of illustrative, mission-based scenarios to translate White House strategic goals and initiatives into mission-specific narratives to assist agencies in planning for and executing goal-based initiatives.

IMPROVING GOVERNANCE

The safe and consistent sharing of terrorism-related information between ISE stakeholders and communities demands efficient governance to help facilitate timely and effective decision making. Given the number and diversity of stakeholders and communities involved, PM-ISE's ability to convene is critical in terms of getting partners to the table to agree upon common practices and standards, and to hold them accountable for their implementation. A number of instances referred to in preceding sections of this Report demonstrate PM-ISE's ability to bring large groups of like-minded people together to develop solutions for responsible information sharing challenges, such as data aggregation. At the smaller end of the spectrum, PM-ISE "opened some really critical doors" according to Dr. Molly Jahn at the University of Wisconsin, who sought PM-ISE's assistance to bring federal and IC partners together with academia to solve an agriculture-related information sharing challenge.

PM-ISE's ability to convene continues to mature as it has had success in promoting communication between and among existing governance bodies that deal with responsible information sharing across the Federal Government. PM-ISE continues the difficult task of aligning efforts both horizontally, between departments and agencies, and vertically within communities of interest.

With PM-ISE, in 2012 mission partners have commenced preliminary efforts to streamline ISE governance. In partnership with PM-ISE and the ISA IPC, ISE mission partners are exploring opportunities to optimize the current ISA IPC governance structure and to improve coordination with other federal governance bodies. According to the 2012 ISE Performance Assessment Questionnaire (ISE PAQ), 94% of agencies reported communicating with the ISA IPC on their responsible information sharing initiatives.[cviii]

ISE agencies are increasingly assigning dedicated staff to oversee responsible information sharing governance bodies and to participate in interagency processes to implement whole-of-government best practices. According to the 2012 ISE PAQ, 84% of ISE agencies report that they have designated a senior official who is accountable for the sharing and safeguarding of classified information on computer networks in compliance with EO 13587, and 93% report that their ISA IPC representative has direct access to their Senior Information Sharing Executive.[cix]

As detailed below, ISE agencies have made demonstrable progress in expanding their internal governance capabilities. These activities, taken together with the positive trends in information sharing-related performance management, appraisal criteria, and awards that are detailed later in this section, are the visible signs of a culture being built upon a foundation of ever stronger management practices and agency collaboration.

- In October 2011, the DHS Information Sharing Governance Board (ISGB) modified their existing charter to incorporate additional security-related activities. The ISGB has been renamed as the Information Sharing and Safeguarding Governance Board (ISSGB);[cx]
- The FBI's Information Sharing Policy Board identifies agency initiatives related to responsible information sharing, and communicates these initiatives to the Senior Information Sharing and Safeguarding Steering Committee and the ISA IPC through its Chief Information Sharing Officer;
- DoT's ISE Program Manager has direct access and communicates regularly with the CISSO concerning the implementation of EO 13587;
- At DoD, the Undersecretary of Defense for Intelligence (USDI) reorganized its information sharing elements and is conducting extensive outreach, with emphasis on intelligence information sharing;
- At the state and local level, the International Association of Chiefs of Police (IACP) formed the Information and Intelligence Sharing Sub-Committee, which serves as a forum for members to raise issues and make strategic decisions relating to information sharing among law enforcement member organizations;[63cxi]
- The DHS Common Operating Picture (COP) Integrated Project Team (IPT) deployed a new COP, provided access to interoperable data and shared services, and created an enduring governance structure to oversee the Department's transition to a common COP architecture; and[64]
- In August 2011, ODNI published the *Strategic Intent for Information Sharing,* which clarifies the role of the IC Information Sharing Executive (ISE) in leading an IC-wide effort to improve information sharing capabilities.[65] The role also provides governance, removes or reduces policy and legal impediments, protects privacy and civil liberties, and promotes a culture that embraces information sharing as a core and fundamental responsibility of every IC officer.

THE ISE PERFORMANCE FRAMEWORK

In 2011, PM-ISE updated the ISE performance management framework in order to align it with White House priorities for responsible information sharing. As a roadmap for ISE agencies, the framework provides maturity-driven and time-sequenced actions for agencies as they strive to implement responsible information sharing initiatives to achieve strategic goals. The framework's integrated performance measures allow PM-ISE to accurately assess improvements to the nations' ability to detect, analyze, and respond to terrorism, WMD, and homeland security threats. ISE agency performance data, an output of this process, is discussed throughout this report, and is detailed in Appendix A.

To assist agencies in planning for and executing the framework's goal-based initiatives, PM-ISE created a set of illustrative scenarios that translate strategic goals and initiatives into mission-specific narratives. Each narrative is specific to an ISE stakeholder's mission and each shows how that mission can be expected to be impacted as responsible information sharing capabilities mature – from current capabilities to those that are expected in five to seven years. For each scenario, PM-ISE has created performance measures that reflect expectations for responsible information sharing capabilities at each level of maturity, in the areas of community, process, and

[63] http://theiacpblog.org/2011/11/09/improving-information sharing/
[64] http://www.dhs.gov/ynews/testimony/20120217-mgmt-duplicative-it-investments.shtm
[65] http://www.dni.gov/reports/11152526_strategic_intent_info_sharing.pdf

technology,[66] giving agencies the tools to set milestones and track progress made towards the strategic goals. These measures are standardized across all mission scenarios – a methodology which provides a common lexicon for discussing the actions needed to achieve our strategic goals for each ISE stakeholder mission. An example of a mission-based scenario is shown in Appendix B.

BUDGET-PERFORMANCE INTEGRATION

Each year, OMB and the National Security Staff issue programmatic guidance on ISE priority areas for responsible information sharing. PM-ISE subsequently issues annual ISE Implementation Guidance that provides more specific direction for agency activities in order to achieve the priorities defined in the programmatic guidance.

The programmatic guidance targets budget year funding priorities and the implementation guidance, developed collaboratively with the agencies, provides budget year actions, as well as focused immediate and near-term activities for agencies to execute. ISE Implementation Guidance is an important tool for coordinating the ISE-specific activities of federal agencies and PM-ISE, through the ISA IPC governance process, tracks the progress of these activities and milestones, ensuring that the ISE continues to successfully advance toward meeting its goals and objectives, and serves as a basis for objective system-wide performance goals for the following year.[cxii] Actions are capabilities-focused, aligned with mission-objectives, and subject to the annual performance assessment process PM-ISE conducts.

Throughout the year, PM-ISE works with agencies to complete the collaborative actions specified in the ISE Implementation Guidance. The table below gives a status of actions due to be completed during the period of July 1, 2011 to June 30, 2012.

[66] Community: engagement with state, local, federal, tribal and international partners; Process: common methodologies and practices that enable joint operational accomplishments; and Technology: technical solutions that automate shared agreements and make solutions interoperable between ISE partners.

Implementation Guidance Action	Owner	Status
Ensure that all fusion centers have privacy, civil rights, and civil liberties protections in place.	DHS	Complete
Develop a collection methodology and solicit an inventory of federal costs dedicated to the National Network of Fusion Centers	DHS	Complete
Ensure that all IC agencies are expeditiously sharing relevant threat analyses with the responsible state, local, and/or tribal entities at the lowest possible classification.	ODNI	Complete
Ensure that IC agencies are incorporating state, local, and tribal priority information needs into intelligence production plans and that the dissemination of relevant products is underway	ODNI	Complete
ISE agencies involved in terrorist watchlisting and screening activities reported to the ISA IPC and the ISA IPC Privacy and Civil Liberties sub-Committee on each agency's processes for protecting P/CR/CL of US persons during the watchlisting and screening processes, as well as any lessons learned that could be shared with other agencies	ISE Agencies	Complete
Develop a plan to improve the agility and timeliness of the CNSS standards-setting process to perform continuous government-wide monitoring of the implementation of established policy and standards	DoD, NSA	Ongoing
Develop a collection methodology and solicit an inventory of federal costs dedicated to the NSI	DoJ	Not Completed

Table 3. Progress toward ISE Implementation Guidance

Each year, PM-ISE evaluates these actions, not only to track progress, but to monitor the collective contribution to responsible information sharing by ISE partners. The results inform OMB's budget decisions in subsequent years and changes to PM-ISE's ISE implementation guidance to achieve responsible information sharing mission objectives. These actions also inform the performance scenarios, which play a vital role in helping leadership determine if the ISE is achieving its desired goals and objectives, as discussed in Appendix B.

Resource tradeoffs have resulted in the delay or reprioritization of some actions. For the actions listed above whose status is "not completed," PM-ISE will work through the ISA IPC governance process to bring these actions to closure to achieve mission objectives. A detailed account of ISE investments can be found in Appendix C.

TRANSFORMING THE CULTURE FROM "NEED TO SHARE" TO "NEED TO RESPONSIBLY SHARE"

Achieving effective responsible information sharing requires a management approach that fosters a culture of responsible information sharing that extends beyond traditional organizational and community boundaries. Agencies can foster culture change by integrating responsible information sharing elements into personnel performance plans and appraisals, training the workforce on its importance, and rewarding positive behavior through awards and incentives. The Office of Personnel Management (OPM) and the PM-ISE have issued guidance to assist ISE agencies in the development of information sharing priority elements for inclusion in employee performance appraisals.[67]

RESPONSIBLE INFORMATION SHARING TRAINING

Sharing terrorism-related information across the whole of government, with the private sector, and with international allies—in the right format, with the right people, and in a manner that protects privacy, civil rights, and civil liberties—is a tall order. Success depends upon each individual in the ISE consistently and properly executing responsible information sharing duties. This consistent execution is grown from robust agency-based programs that provide constant and continuous sustainment training to analysts, operators, and investigators with direct ISE responsibilities.

In response to PM-ISE's 2012 Performance Assessment Questionnaire, 90% of agencies reported implementing mission-specific training that supports information sharing and collaboration – up from 66% the previous year (see Figure 2 below). 88% of agencies that have implemented this type of training reported seeing improvements with respect to information sharing and stewardship as a result of these training programs ***– a 135% increase when compared to the previous year***. In addition, DHS, DoJ, DoD, ODNI, DoS, the CIA, and DIA require all employees to complete annual privacy training, a practice that is trending upward for other ISE agencies.[68cxiii]

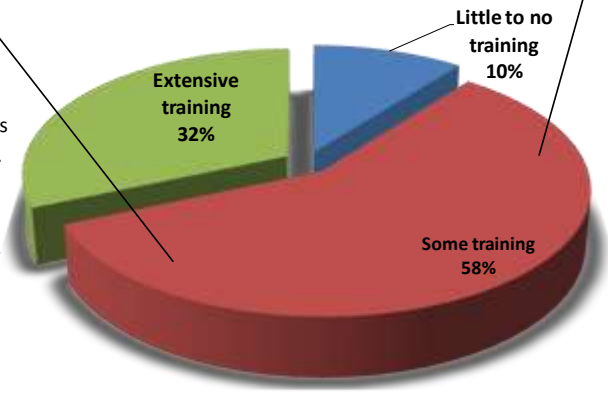
[67] *Inclusion of Information Sharing Performance Evaluation Element in Employee Performance Appraisal Memorandum,* ISE Guidance, September 23, 2008; and, *Inclusion of Information Sharing Performance Evaluation Element in Employee Performance Appraisal Memorandum,* OPM Guidance, September 24, 2008.

[68] See Appendix A for more detail.

What degree has your agency implemented any mission-specific training that supports information sharing and collaboration? Please provide examples.

"All incoming DHS employees receive privacy, civil rights and civil liberties training during orientation. DHS also provides information sharing training to its Federal, State and local partners. For example, SLPO works closely with DHS components and other federal partners, including ODNI, PM-ISE, DOJ and the FBI, to develop and implement mission-specific training specifically designed to help fusion centers improve their ability to share and safeguard information and to improve information sharing collaboration."

- **DHS**



"HHS developed a cadre of private sector liaison officers (LNOs) from among our critical infrastructure protection partnership. These individuals have received training on emergency response operations, including relevant ICS (Incident Command System) courses and tailored training related to HHS and ESF-8 emergency response. The LNOs serve as a conduit for information sharing with the private sector as a whole. HHS also supports a Protected Critical Infrastructure Information (PCII) program, and adhere to the necessary training requirements for users of PCII. (b) Additionally, HHS participated in DNI training on information safeguarding and collaboration."

- **HHS**

Figure 2. Excerpt from 2012 ISE Performance Assessment Questionnaire

FUSION CENTER TRAINING

Training is critical to mitigating capability gaps and increasing the overall capacity of the National Network of Fusion Centers. Over the past year, DHS and federal partners hosted a series of workshops and seminars focused on countering violent extremism, analytic tradecraft, security, classified information sharing, and liaison programs. For example:

- In August 2011, DHS, in partnership with DoJ, the FBI, NCTC, and ODNI, hosted the National Countering Violent Extremism (CVE) Workshop. This is the first time Fusion Center Directors and major city police department intelligence unit commanders were brought together to address homeland security threats. Subject-matter experts from all levels of government, fusion centers, academia, and the IC provided information on emerging issues related to violent extremism.[cxiv]
- In November 2011, DHS, DoJ, PM-ISE, and the NSI PMO co-sponsored the National Fusion Center Analytic Workshop and Risk Analysis Seminar. Nearly 130 analysts attended this event, which included a range of panels and workshops focused on enhancing analytic tradecraft, analysis of SAR, and emerging intelligence trends.[cxv]
- In November 2011, DHS hosted the National Fusion Center Security Liaison Workshop. This "train-the-trainer" style workshop focused on implementation of baseline security requirements[69] and requirements

[69] Per Baseline Capabilities for State and Major Urban Area Fusion Centers (2008).

established by Executive Order 13549—*Classified National Security Information Program for State, Local, Tribal, and Private sector Entities*

- In March 2012, DHS and the PM-ISE convened the National Fusion Liaison Officer (FLO) Program Workshop in Monterey, CA. The workshop facilitated the sharing of best practices and lessons learned between fusion centers with mature FLO programs as well as discussions on common and consistent standardization of liaison officer programs[70] across the National Network.
- In April 2012, nearly 600 federal, state, local, tribal, and territorial fusion center stakeholders attended the sixth annual National Fusion Center Training Event and Spring Strategy Meeting in Phoenix, AZ. This event serves as a key forum for designated fusion centers to receive training and technical assistance and to exchange best practices to support the implementation of the COCs and ECs.[cxvi]

NSI TRAINING

The NSI training strategy is designed to increase the effectiveness of SLTT law enforcement and public safety professionals and other frontline partners in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism. While continuing to provide high-quality training for the law enforcement community as described below, the NSI PMO, in partnership with PM-ISE, also developed and is now implementing SAR awareness training for other key non-law-enforcement constituencies, or "hometown security partners" that are important to the SAR effort, including fire and emergency medical service personnel, call takers (e.g., 9-1-1 operators), emergency managers, corrections, probation, and parole officers, and other related occupations, such as those responsible for protecting the nation's critical infrastructure. The purpose is not to empower public safety officials to act on behalf of law enforcement, but to have them understand the critical role they play in identifying and reporting suspicious activity to SLTT law enforcement.

2012 ISE PAQ data indicates that over three-quarters of federal agencies provide SAR training to personnel. To date, DHS has trained more than 400 personnel in SAR analyst training and 65,000 personnel in line officer training. The DoD plans to train an additional 1,000 personnel in FY2012. At the Department of Interior (DOI), SAR training will be mandated for all frontline officers and security personnel this year. In partnership with the NSI, the National Maritime Intelligence-Integration Office (NMIO) is developing a SAR awareness training program focused on the maritime industry.[71] NMIO and NSI plan to complete the development of the maritime industry sector training by the fall of 2012.[cxvii]

NSI Technical Assistance and Analyst Training - To enhance the fusion process, the NSI developed an NSI Federated Search Tool Technical Assistance process to assist fusion center analysts in quickly and effectively searching for relevant information within the NSI Federated Search. Analysts will learn how to display the data in a geospatial format using the Map It/Link It tool. In addition to searching and mapping the data, analysts will also learn how to save queries, set alert notifications, and locate contact information. Also over the past year, the NSI PMO worked to deliver 24 analyst training sessions across the country, reaching almost 700 analysts. In addition, DHS conducted three rounds of training in 2011 that were attended by personnel from nine DHS components.[cxviii]

Line Officer Training Update - The NSI PMO continues to provide SAR training to law enforcement and support personnel to help ensure that they are properly trained to recognize behavior and incidents identified by law enforcement officials and counterterrorism experts as being reasonably indicative of criminal activity associated

[70] Also known as Terrorism Liaison Officers, Intelligence Liaison Officers, and Field Intelligence Officers.
[71] http://nmio.ise.gov/techbulletin.htm to download

with terrorism. With the support of state and local law enforcement associations[72], the NSI PMO has increased the number of line officers receiving SAR training to nearly 250,000 in 2011. The NSI PMO goal is to ensure that every line officer across the country is properly trained in SAR.

NEW FBI TRAINING OFFERED TO LAW ENFORCEMENT PARTNERS

During calendar year 2011, the FBI developed training that was made available to federal, state, local and tribal law enforcement partners and fusion center personnel, via the Unclassified Virtual Academy. Three Web-based, information sharing-related training modules were released: 1) ISE Core Awareness Training, 2) Introduction to Collection Management, and 3) the Correctional Intelligence Initiative. In addition, 84 commercial Web-based training modules were purchased by the FBI and added to the Unclassified Virtual Academy. These additional modules offer training on a wide variety of topics. The Unclassified Virtual Academy currently hosts 8,523 registered agencies and 11,488 active users. A total of 18 FBI-developed Web-based training modules are available, along with 2,108 commercial Web-based training modules.

NATIONAL ASSOCIATION OF SECURITY COMPANIES ENDORSES DOJ/DHS SAR TRAINING VIDEO FOR PRIVATE SECURITY

In April 2012, the National Association of Security Companies (NASCO), the nation's largest contract security industry association, representing private security companies that employ more than 250,000 security officers serving every business sector, endorsed the SAR Training Video for private sector security personnel. Developed with input from private sector security organizations, including NASCO and NASCO member companies, the SAR Training Video for Private Sector Security is designed to expand the nation's capability to prevent terrorist activity by increasing the number of "eyes and ears" looking for suspicious activity, and having those eyes and ears trained properly to distinguish activity that should be reported, and how to report such activity to the appropriate authorities. Private security officers are a critical component of defending our homeland. They outnumber law enforcement personnel by more than two to one, and provide security at approximately 90% of critical infrastructure sites in the nation. The free training is available online at: http://nsi.ncirc.gov/training_online.aspx.

INFORMATION SHARING TRAINING FOR LAW ENFORCEMENT EXECUTIVES

The International Association of Chiefs of Police (IACP), in partnership with the Bureau of Justice Assistance, developed a curriculum designed to inform law enforcement executives of the various aspects to the ISE. Special emphasis is given to NSI, implementation of Terrorism Liaison Officer (TLO) programs, increased interaction and connectivity with fusion centers, and the privacy, civil rights, and civil liberties of citizens. The no-cost training includes a seminar, online tutorials, and a resource tool kit to help guide law enforcement executives.[cxix]

PERFORMANCE APPRAISALS AND AWARDS

Effective and secure information sharing is ultimately the result of, and completely dependent upon, the daily actions of the individuals in the ISE. A workforce that is well trained and incentivized to share and protect information in the execution of their daily duties is a requisite precondition for achieving a cultural shift from “need to know” to “need to share” to “need to responsibly share.” Incentives like

[72] Including the Association of State Criminal Investigative Agencies, the International Association of Chiefs of Police, Major Cities Chiefs Association, Major County Sheriffs Association, the National Fusion Center Association, and the National Sheriffs’ Association.

performance appraisals that include responsible information sharing objectives, and agency awards for responsible information sharing are powerful tools to affect this change, and agencies across the ISE are increasingly implementing them. This increase is evident in the responses to PM-ISE's 2012 ISE Performance Assessment Questionnaire, in which 36% of responding agencies reported an increase in the nomination of candidates for information sharing and collaboration awards, and 80% of agencies reported that "information sharing and collaboration" is an evaluated performance objective for employees with direct ISE responsibilities. [73]

BUILDING BLOCKS OF THE ISE

PM-ISE is launching "Building Blocks," a knowledge management tool available on www.ise.gov that details five foundational components that government agencies and organizations can use to build responsible information sharing programs: Governance, Budget & Performance, Acquisition, Standards & Interoperability, and Communications & Partnerships. PM-ISE's vision for Building Blocks is to catalyze and accelerate the identification, distillation, capture, validation, and dissemination of responsible information sharing best practices and innovations via online communities that are the mechanism for sourcing and sharing this content. The tool is designed to help ISE federal mission partners as well as state, local, tribal, and international partners find and share best practices, guidelines, and lessons learned. Key is the idea that best practices and innovations will be sourced to the extent possible across all communities. Building Blocks will also showcase our partners' success stories by outlining how they were able to implement information sharing guidelines within their own environments, in particular demonstrating how they leveraged the underlying best practice or innovation. Over time, we hope and expect to see new innovations or best practices emerging from collaboration within and across stakeholder communities via the building blocks platform.

[73] See Appendix A, Sec 1.3 for more details.

WAY FORWARD

Responsible information sharing to protect the American people is a top priority of the President. The White House leads interagency policy prioritization, development, and coordination. The Office of Management and Budget (OMB) oversees the development of the President's budget and ensures that agency budgets are consistent with the priorities for responsible information sharing, as described in programmatic guidance.

PM-ISE, on behalf of the President, plans for, manages, and oversees the implementation of responsible information sharing. PM-ISE leads Federal Government-wide implementation by managing a coherent set of management processes to align policy, governance, budget, performance, standards, technologies and architectures. In collaboration with the White House, federal agency representatives, and other stakeholders, PM-ISE has updated its vision, mission, and objectives for responsible information sharing. By updating the target vision, PM-ISE has exercised its legal authorities and White House-mandated responsibilities.

Agencies have a vital leadership role for the delivery, operation, and use of the ISE, and are accountable to the White House for programmatic and ISE implementation guidance. Agencies are committed to responsible information sharing through their participation in the White House and PM-ISE-led Information Sharing and Access Interagency Policy Committee (ISA IPC), and their active engagement with the White House-chaired Senior Information Sharing and Safeguarding Steering Committee.

Leadership from federal, state, local, tribal and private sector organizations with operational, investigative, and/or analytic missions have a voice through the ISA IPC working group and sub-committee governance processes to propose improvements to information sharing.[74] Through this collective engagement and leadership commitment from the White House, PM-ISE, agencies, and other ISE stakeholders, we collectively accelerate responsible information sharing to strengthen our Nation's security.

[74] IRTPA Sec 1016(b)(2)(C).

MANAGING IMPLEMENTATION OF RESPONSIBLE INFORMATION SHARING

PM-ISE's capability-focused Implementation Guidance provides the basis for an objective, system-wide set of performance goals for the following year as required by the IRTPA.[75] Annually, in collaboration with the ISA IPC, PM-ISE issues Implementation Guidance that is sequentially derived from, and reinforces, White House programmatic guidance. The Implementation Guidance contains actions assigned to specific federal agencies, with milestones and timeframes that align programs, systems, and initiatives with requirements to improve responsible information sharing. Annual performance assessments against these actions are included in PM-ISE's Annual Report to Congress, providing accountability and progress over time, and enabling leadership to make informed program and budget decisions in subsequent years. Overall, the annual planning cycle moves agencies closer to the target vision of responsible information sharing. The annual planning cycle is depicted in Figure 3.

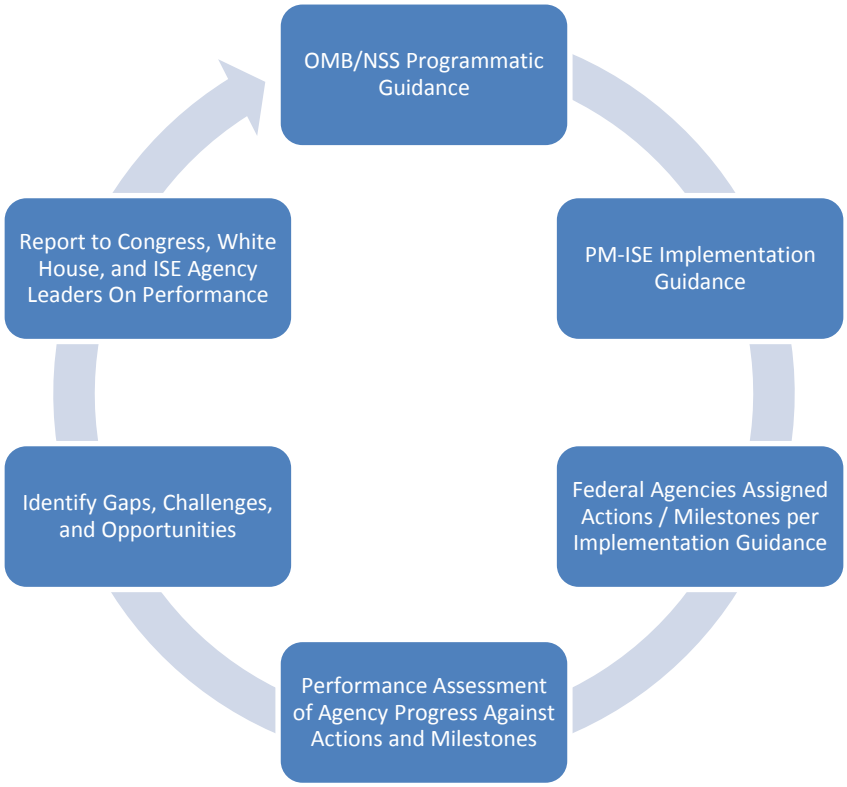
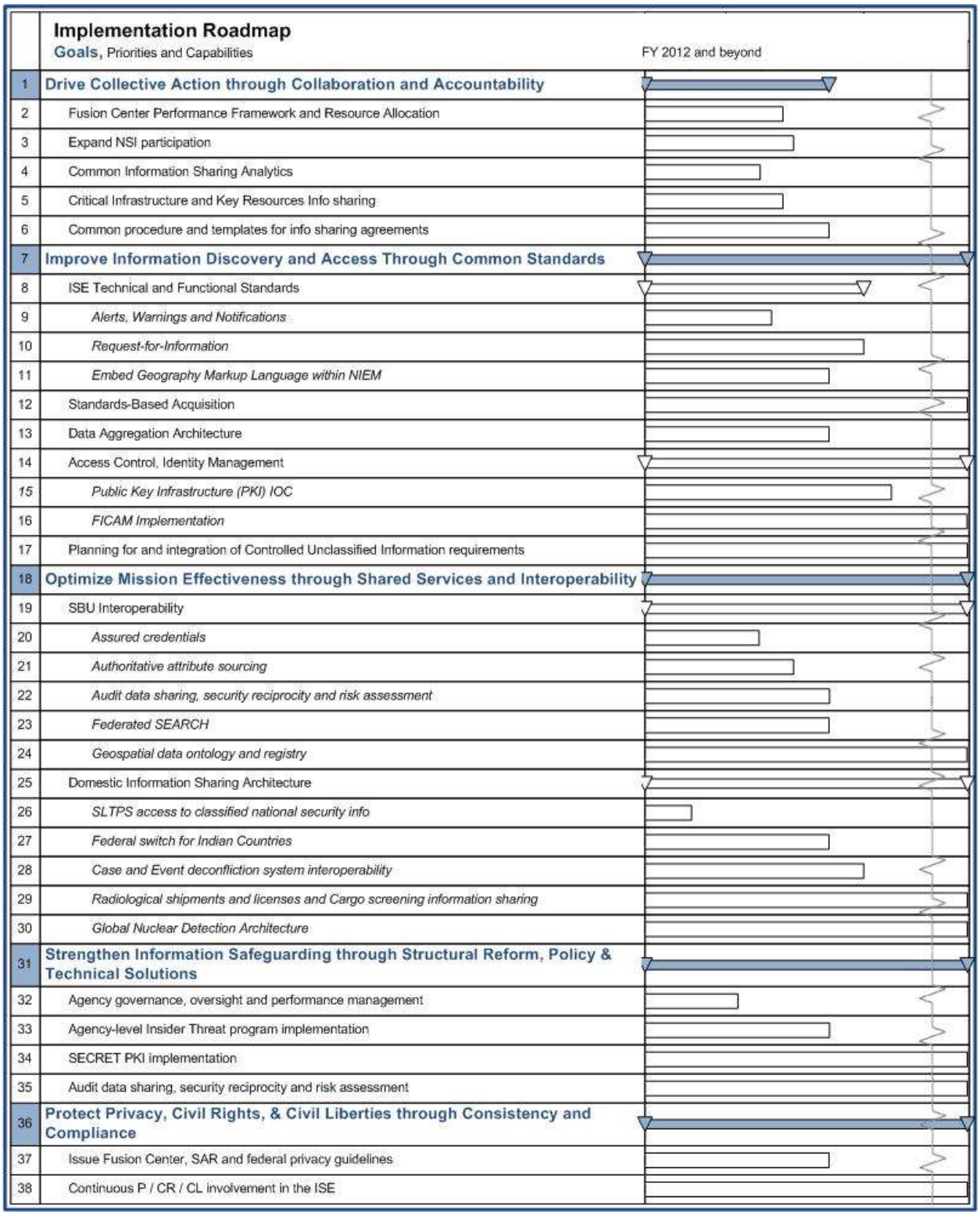


Figure 3. Annual Planning Cycle

IMPLEMENTATION ROADMAP

PM-ISE's Implementation Guidance enables prioritized implementation of responsible information sharing capabilities,[cxx] in line with a maturity-oriented implementation roadmap as shown below. The roadmap is subject to the availability of appropriations based on agency budgets and may be adjusted through a change management process led by the ISA-IPC. Changes to the implementation roadmap will be incorporated into the ISE performance framework and will be reflected in next year's annual report to the Congress.

[75] IRTPA Sec 1016 (h)(2)(B).


Implementation Roadmap
Goals, Priorities and Capabilities
FY 2012 and beyond
1 Drive Collective Action through Collaboration and Accountability
2 Fusion Center Performance Framework and Resource Allocation
3 Expand NSI participation
4 Common Information Sharing Analytics
5 Critical Infrastructure and Key Resources Info sharing
6 Common procedure and templates for info sharing agreements
7 Improve Information Discovery and Access Through Common Standards
8 ISE Technical and Functional Standards
9 Alerts, Warnings and Notifications
10 Request-for-Information
11 Embed Geography Markup Language within NIEM
12 Standards-Based Acquisition
13 Data Aggregation Architecture
14 Access Control, Identity Management
15 Public Key Infrastructure (PKI) IOC
16 FICAM Implementation
17 Planning for and integration of Controlled Unclassified Information requirements
18 Optimize Mission Effectiveness through Shared Services and Interoperability
19 SBU Interoperability
20 Assured credentials
21 Authoritative attribute sourcing
22 Audit data sharing, security reciprocity and risk assessment
23 Federated SEARCH
24 Geospatial data ontology and registry
25 Domestic Information Sharing Architecture
26 SLTPS access to classified national security info
27 Federal switch for Indian Countries
28 Case and Event deconfliction system interoperability
29 Radiological shipments and licenses and Cargo screening information sharing
30 Global Nuclear Detection Architecture
31 Strengthen Information Safeguarding through Structural Reform, Policy & Technical Solutions
32 Agency governance, oversight and performance management
33 Agency-level Insider Threat program implementation
34 SECRET PKI implementation
35 Audit data sharing, security reciprocity and risk assessment
36 Protect Privacy, Civil Rights, & Civil Liberties through Consistency and Compliance
37 Issue Fusion Center, SAR and federal privacy guidelines
38 Continuous P / CR / CL involvement in the ISE

PM-ISE'S VISION, MISSION, AND OBJECTIVES

> ***"PM-ISE is working hard at embracing common operating models and shared services - that implies greater integration horizontally across community stovepipes, as well as vertically – from federal, state, local, tribal and private sector partners, and our allies."***
>
> - DNI Clapper, 26 January 2012, Center for Strategic and International Studies Forum on Information Sharing

While the White House provides a strategy for information sharing and safeguarding, and agencies are largely responsible for implementing specific actions based on White House and PM-ISE guidance, PM-ISE has updated the vision and mission for responsible information sharing in order to continue to advance the ISE consistent with existing legal authorities and Executive Orders.[76] PM-ISE's updated vision and mission are shown below:

PM-ISE'S VISION: NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

PM-ISE's Mission:

I. Advance responsible information sharing to further counterterrorism and homeland security missions

II. Improve nationwide decision making by transforming from information ownership to information stewardship

III. Promote partnerships across federal, state, local, and tribal governments, the private sector, and internationally

DELIVERING CAPABILITIES

PM-ISE's vision and mission are supported by capability-focused objectives, which, when implemented by federal agencies, accelerate the delivery of the decentralized, distributed, and coordinated terrorism-related information sharing environment envisioned by Congress. Additionally, PM-ISE ensures alignment with White House priorities for information sharing and safeguarding by planning for, managing, and overseeing the delivery of these capabilities. Mission-based test scenarios, developed by PM-ISE in coordination with ISE agencies, document how and how well ISE partners are achieving mission capabilities. For further detail, see Appendix B.

I. ADVANCE RESPONSIBLE INFORMATION SHARING TO FURTHER COUNTERTERRORISM AND HOMELAND SECURITY MISSIONS

Objective: Transform the domestic information sharing architecture to better identify and respond to threats

The need to transform the Nation's justice and public safety information sharing business model through more effective, efficient, and coordinated technical, policy, and funding solutions and practices is greater than ever. When aggregated, successful solutions to the following prioritized information sharing issues will yield a positive, transformative shift in the overall justice and public safety enterprise: 1) Single sign-on (SSO) and federated query capabilities; 2) leverage private cloud solutions; 3) improve offender reentry initiatives; 4) provide effective deconfliction and coordination of regional activities; and 5) ensure shared services.

[76] Pursuant to IRTPA Section 1016; EO 13388; and EO 13587.

At its core, ***establishing trusted interoperable networks*** to efficiently and effectively share and safeguard controlled unclassified information across government networks serves to fully protect the privacy, civil rights, and civil liberties of individuals, and ***to facilitate the discoverability and accessibility of information by individuals and organizations at the local, state, tribal, and federal levels of government who are responsible for decision making*** to prevent harm against the United States and its people. This objective is illustrated in mission-based test Scenario #5 – Enabling Deconfliction to Promote Officer Safety – which deals with improving the mechanisms to perform case and event deconfliction in the public safety arena to improve mission effectiveness and officer safety.[77]

Objective: Build and deliver capabilities to manage, integrate, and make sense of vast stores of information

Agencies have achieved an unprecedented ability to gather, store, and use information consistent with their missions and applicable legal authorities. Moving away from agency-specific networks and applications, we aim to build an enterprise-wide approach in which we secure and authorize access to information in ways that allow it to be shared across agencies. ***Connecting data holdings in a way that allows data originators to see responsible information sharing policies enforced***, while also ***facilitating discovery and correlation of information across disparate holdings, can mean the difference between identifying a threat during the planning stage and taking action to prevent it, and seeing the connections only after the attack***. Data correlation and advanced analytic capabilities ***enable users to reference authoritative, up-to-date information across holdings to identify relationships among people, places, things and characteristics that are otherwise not obvious***. With the completion of the ISE Data Aggregation Capabilities Applicable to Terrorism Report this year, PM-ISE is now developing strategic next steps for accelerating data aggregation solutions across interagency counterterrorism missions, including cyber-threat information sharing.

Objective: Innovate and standardize information sharing capabilities nationwide to support decision making more effectively and efficiently

PM-ISE supports the Steering Committee for Information Sharing and Safeguarding and ISA IPC to refine and crystallize policy decision points, clarify potentially competing priorities to ease resource competition, streamline governance, and improve accountability. This improved, results-oriented, Executive-level support **enables transformation of domestic information sharing architecture and the capability to make sense of the vast stores of information made available through its transformation; it prioritizes interoperability, standards-based acquisition, and information-access management standards, while at the same time protecting P/CR/CL**. It looks beyond the Federal Government and encourages a cultural change of governance throughout other echelons of government—state, local and tribal—as well as throughout the private sector. Scenario #7, which deals with modernizations to the SAR process in the CIKR domain, highlights work in the ISE corresponding to this objective.[78]

II. IMPROVE NATIONWIDE DECISION MAKING BY TRANSFORMING FROM INFORMATION OWNERSHIP TO INFORMATION STEWARDSHIP

Objective: Achieve greater interoperability through an open development approach and standards-based acquisition

An approach to acquisition based on commonly accepted standards that are utilized throughout the ISE is essential for deploying interoperable technology solutions and shared services. Collaboration between government agencies should be encouraged in order to promote interoperable capabilities through the reuse or reconfiguration of existing solutions and the development of enterprise-wide acquisition priorities. Leveraging an open development approach and aligning acquisition requirements across the ISE community: ***facilitates identification and leverages***

[77] See Appendix B: Scenario 5 – Enabling Deconfliction to Promote Officer Safety.
[78] Appendix B: Scenario 7 – Using SARs to Detect CIKR Threats.

existing capabilities; creates broader awareness and understanding of initiatives; maximizes purchasing power when acquiring new products or services; decreases risk while integrating common solutions; promotes standardization of agency-level services as they align across the enterprise; and enables accountability in purchasing decisions. In sum, an open development approach and standards-based acquisition not only saves taxpayer dollars, but it can also drive the development of more open industry-wide standards and technologies, and have a broader impact on national economic development. Standards-based acquisition not only enhances efficiency, it enhances operational effectiveness as seen in Scenario #4, where work towards modernizing the acquisition process shows concrete improvement in the government's ability to procure effective information sharing mission systems.[79]

Objective: Drive responsible information sharing by interconnecting existing networks and systems with strong identity, access, and discovery capabilities

A federation of interconnected networks represents the strongest, most efficient architecture for mission support. PM-ISE promotes strong policies and practices for identity, credential, and access management, implemented at a granular level using common standards to ensure interoperability. ***Common data-level standards provide for improved information security through shared audit and cyber-threat information on interconnected networks, improved information discoverability, and improved information sharing***. Consistently-applied policies and practices for tagging people and information form the foundation for securely sharing information across the broadest community of federal, state, local, tribal, private sector and international mission partners. Consistent tagging also makes it possible to increase protections for privacy, civil rights, and civil liberties, even as sharing of information increases. Finally, consistent tagging and standards promote efficiency through standards-based acquisition, shared services, and re-use. Progress towards improving the ISE's capabilities in this area can be seen in Scenario #3, which deals with federated search and discovery over interconnected networks to improve the ability of investigators to accomplish their missions.[80]

Objective: Standardize, reuse, and automate information sharing policies and agreements with strong protection of privacy, civil liberties, and civil rights

While implementation of common standards, policies, and practices promotes information sharing efficiencies through re-use of best practices and capabilities across federal, state, local, tribal, public sector, and international communities of action, the ISA IPC will promote the development of ***re-usable standards and practices that ensure protections for privacy, civil rights, and civil liberties***. Common processes, such as a model for developing information sharing agreements, ***enable mission partners to reduce the amount of time needed to build sharing agreements and focus more attention on sharing information with the appropriate users in a timely and trusted manner***. As federal, state, local, tribal, and private sector communities leverage common standards, the ability to increasingly streamline processes may be realized at some point in the future through technology, where audit and control mechanisms govern the enforcement of privacy, civil rights, and civil liberties protections. An example of the ISE's path forward in this area is shown through one of the mission-based scenarios, which deals with improving role-based access to SAR information based on repeatable standards and practices for sharing and policy automation.[81]

[79] Appendix B: Scenario 4 – Accelerating Federal Acquisition.
[80] Appendix B: Scenario 3 – Improving Secure Access through Federated Search.
[81] Appendix B: Scenario 1 – Improving Role-Based Access to SAR Information.

III. PROMOTE PARTNERSHIPS ACROSS FEDERAL, STATE, LOCAL, AND TRIBAL GOVERNMENTS, THE PRIVATE SECTOR, AND INTERNATIONALLY

Objective: Build organizational capacity through engagement, coordination, training, and management support

Through the ISA IPC, PM-ISE will incentivize responsible information sharing through in-place governance processes by promoting the ***sourcing of best-practices innovation and expanded re-use of existing information sharing tools and technologies that optimize information sharing across federal, state, local, tribal, and public sector domains.*** Additionally, in coordination with federal agencies, PM-ISE will ensure an optimized and properly aligned governance structure that enables information sharing goals, objectives, and strengthened partnerships with international partners. This is demonstrated in one of the mission-based scenarios, where efforts to improve the international sharing of gang-related and terrorism-related information are highlighted.[82]

Objective: Encourage cultural change through communities of action

PM-ISE, along with the NSS, through the ISA IPC governance processes, promotes ISE implementation actions that foster change toward a culture of greater information sharing across federal, state, local, tribal, public sector, and international boundaries. ***Developing the instinctive desire to share terrorism, homeland security, and weapons of mass destruction-related information*** between communities of action within federal, state, local, tribal, private sector, and international partners ***provides for improved fidelity of information on which decision makers rely***. Transforming the domestic information sharing architecture with capabilities that make sense of vast amounts of information originating from the federal, state, local, tribal, and private sector inherently encourages a culture of change toward greater information sharing, which is shown in our scenarios, where cross-governmental insider threat information sharing demonstrates a cultural shift in how the government does business.[83]

[82] Appendix B: Scenario 8 – Globalizing NIEM to Enable International Sharing.
[83] Appendix B: Scenario 6 – Incentivizing Insider Threat Information Sharing.

ENDNOTES

[i] IRTPA Sec. 1016 (h)(1), (h)(2)(A)
[ii] IRTPA Sec. 1016(h)(2)(I)
[iii] IRTPA Sec. 1016(h)(2)(I)
[iv] IRTPA Sec. 1016(h)(2)(J)
[v] IRTPA Sec. 1016(h)(2)(G)
[vi] IRTPA Sec. 1016(h)(2)(F)
[vii] IRTPA Sec. 1016 (h)(2)(A)
[viii] IRTPA Sec. 1016 (h)(2)(F),(G)
[ix] IRTPA Sec. 1016 (b)(2)(B)
[x] IRTPA Sec. 1016 (h)(2)(F)
[xi] IRTPA Sec. 1016 (h)(2)(c)
[xii] IRTPA Sec. 1016(h)(2)(C)
[xiii] IRTPA Sec. 1016 (b)(2)(B); (h)(2)(F)
[xiv] IRTPA Sec. 1016 (b)(2)(C),(D),(F),(M)
[xv] IRTPA Sec. 1016 (h)(2)(F)
[xvi] IRTPA Sec. 1016 (b)(2)(C)
[xvii] IRTPA Sec. 1016 (h)(2)(F)
[xviii] IRTPA Sec. 1016 (h)(2)(E),(G)
[xix] IRTPA Sec. 1016 (h)(2)(G)
[xx] IRTPA Sec. 1016 (b)(2)(C); (h)(2)(F)
[xxi] IRTPA Sec. 1016 (b)(2)(L)
[xxii] IRTPA Sec. 1016 (b)(2)(A),(B),(D),(J)
[xxiii] IRTPA Sec. 1016 (h)(2)(F)
[xxiv] IRTPA Sec. 1016 (b)(2)(C),(G),(J),(L)
[xxv] IRTPA Sec. 1016 (b)(2)(C),(M)
[xxvi] IRTPA Sec. 1016 (b)(2)(C),(J),(L)
[xxvii] IRTPA Sec. 1016 (b)(2)(A),(D),(K)
[xxviii] IRTPA Sec. 1016 (b)(2)(G)
[xxix] IRTPA Sec. 1016 (b)(2)(K)
[xxx] IRTPA Sec. 1016 (h)(2)(F)
[xxxi] IRTPA Sec. 1016 (h)(2)(F)
[xxxii] IRPTA Sec. 1016(h)(2)(F)
[xxxiii] IRTPA Sec. 1016 (h)(2)(F)
[xxxiv] IRTPA Sec. 1016 (h)(2)(F)
[xxxv] IRTPA Sec. 1016 (b)(2)(C)(M)
[xxxvi] IRTPA Sec. 1016 (b)(2)(C); (h)(2)(H)
[xxxvii] IRTPA Sec. 1016 (h)(2)(H)
[xxxviii] IRTPA Sec. 1016 (h)(2)(F)
[xxxix] IRTPA Sec. 1016 (b)(2)(A),(D),(F),(K)
[xl] IRTPA Sec. 1016 (b)(2)(C)(J)
[xli] IRTPA Sec. 1016 (b)(2)(G)
[xlii] IRTPA Sec. 1016 (h)2)(G)
[xliii] IRTPA Sec. 1016 (h)(2)(F),(G)
[xliv] IRTPA Sec. 1016 (h)2)(G)
[xlv] IRTPA Sec. 1016 (b)(2)(C),(M)
[xlvi] IRTPA Sec. 1016 (h)(2)(F)
[xlvii] IRTPA Sec. 1016 (b)(2)(C)
[xlviii] IRTPA Sec. 1016 (b)(2)(C)
[xlix] IRTPA Sec. 1016 (b)(2)(E),(I)
[l] IRTPA Sec. 1016 (b)(2)(E)(I)
[li] IRTPA Sec. 1016 (b)(2)(E)(I)

[lii] IRTPA Sec. 1016 (b)(2)(E)(I)
[liii] IRTPA Sec. 1016 (b)(2)(E)(I); (h)(2)(H)
[liv] IRPTA Sec. 1016 (b)(2)(E)(I); (h)(2)(H)
[lv] IRTPA Sec. 1016 (b)(2)(E)(I); (h)(2)(H)
[lvi] IRTPA Sec. 1016 (b)(2)(E),(I)
[lvii] IRTPA Sec. 1016 (b)(2)(A),(B),(D),(F),(J),(K),(M)
[lviii] IRTPA Sec. 1016 (b)(2)(A),(B),(F)
[lix] IRTPA Sec. 1016 (b)(2)(A),(D),(F),(K)
[lx] IRTPA Sec. 1016 (b)(2)(A),(D),(K)
[lxi] IRTPA Sec. 1016 (b)(2)(F)
[lxii] IRTPA Sec. 1016 (b)(2)(E),(I); (h)(2)(J)
[lxiii] IRTPA Sec. 1016 (b)(2)(A),(D),(F),(K),(N)
[lxiv] IRTPA Sec. 1016 (h)(2)(F)
[lxv] IRTPA Sec. 1016 (b)(2)(J)
[lxvi] IRTPA Sec. 1016 (b)(2)(A),(C),(D),(K); (h)(2)(F)
[lxvii] IRTPA Sec. 1016 (b)(2)(C); (h)(2)(H)
[lxviii] IRTPA Sec. 1016 (b)(2)(A),(C),(D),(K),(M)
[lxix] IRTPA Sec. 1016 (b)(2)(D); (h)(2)(F)
[lxx] IRTPA Sec. 1016 (h)(2)(h)
[lxxi] IRTPA Sec. 1016 (b)(2)(N)
[lxxii] IRTPA Sec. 1016 (b)(2)(A),(C),(J),(K),(M)
[lxxiii] IRTPA Sec. 1016 (b)(2)(D)
[lxxiv] IRPTA Sec. 1016 (b)(2)(C),(F),(L)
[lxxv] IRTPA Sec. 1016 (b)(2)(D)(K)
[lxxvi] IRPTA Sec. 1016 (b)(2)(C),(F),(K)
[lxxvii] IRTPA Sec. 1016 (h)(2)(D)
[lxxviii] IRTPA Sec. 1016 (b)(2)(C),(F),(K)
[lxxix] IRTPA Sec. 1016 (b)(2)(A),(C),(D),(F),(J),(K),(L)
[lxxx] IRTPA Sec. 1016 (b)(2)(A),(C),(D),(K)
[lxxxi] IRTPA Sec. 1016 (b)(2)(A),(C),(D),(F),(J),(K),(L)
[lxxxii] IRTPA Sec. 1016 (b)(2)(H)
[lxxxiii] IRTPA Sec. 1016 (h)(2)(D)
[lxxxiv] IRTPA Sec. 1016(b)(2)(I)
[lxxxv] IRTPA Sec. 1016(b)(2)(I)
[lxxxvi] IRTPA Sec. 1016(b)(2)(I)
[lxxxvii] IRTPA Sec. 1016(b)(2)(I)
[lxxxviii] IRTPA Sec. 1016(b)(2)(I)
[lxxxix] IRTPA Sec. 1016(b)(2)(E), (I)
[xc] IRTPA Sec. 1016(b)(2)(O)
[xci] IRTPA Sec. 1016(b)(2)(I)
[xcii] IRTPA Sec. 1016(b)(2)(O)
[xciii] IRTPA Sec. 1016(b)(2)(I)
[xciv] IRTPA Sec. 1016(b)(2)(C), (F); (h)(2)(G)
[xcv] IRTPA Sec. 1016(b)(2)(E)
[xcvi] IRTPA Sec. 1016(b)(2)(C); (h)(2)(G)
[xcvii] IRTPA Sec. 1016(b)(2)(C), (F)
[xcviii] IRTPA Sec. 1016(h)(2)(H)
[xcix] IRTPA Sec. 1016(b)(2)(I)
[c] IRTPA Sec. 1016(b)(2)(O)
[ci] IRTPA Sec. 1016 (h)(2)(I)
[cii] IRTPA Sec. 1016 (b)(2)(H)
[ciii] IRTPA Sec. 1016 (b)(2)(H)
[civ] IRTPA Sec. 1016 (b)(2)(H)
[cv] IRTPA Sec. 1016 (b)(2)(H)
[cvi] IRTPA Sec. 1016 (b)(2)(H)

[cvii] IRTPA Sec. 1016 (b)(2)(H)
[cviii] IRTPA Sec. 1016 (b)(2)(N)
[cix] IRTPA Sec. 1016 (b)(2)(N)
[cx] IRTPA Sec. 1016 (h)(2)(J)
[cxi] IRTPA Sec. 1016 (h)(2)(F)
[cxii] IRTPA Sec. 1016(h)(2)(B)
[cxiii] IRTPA Sec. 1016 (h)(2)(I)
[cxiv] IRTPA Sec. 1016 (h)(2)(F)
[cxv] IRTPA Sec. 1016 (b)(2)(C)
[cxvi] IRTPA Sec. 1016 (h)(2)(F)
[cxvii] IRTPA Sec. 1016 (h)(2)(F)(G)
[cxviii] IRTPA Sec. 1016 (b)(2)(C)
[cxix] IRTPA Sec. 1016 (h)(2)(F)
[cxx] IRPTA Sec. 1016(h)(2)(B) and (f)(2)(A)(3)

APPENDIX A – ISE PERFORMANCE DATA

As discussed in the body of this report, the ISE Performance Framework allows PM-ISE to accurately assess improvements to the nations' ability to detect, analyze, and respond to terrorism, WMD, and homeland security threats. ISE agency performance data is discussed throughout this report, and is detailed below.

PM-ISE maps the 2012 Performance Assessment Questions (detailed later in this appendix) to the capability areas of community, process, and technology, which allows for the assessment of ISE agency performance within each of these areas. Figure 4a below shows aggregate performance over the preceding year within each capability area and for each of ISE Performance Framework topics, which are aligned with the Administration's strategic goals for responsible information sharing. Responses to the 2012 ISE Performance Assessment Questions are scored on a 0-1 scale; the aggregate scores for responses to questions within each capability area are calculated as a percentage of the total possible score. The performance scores shown in green below are consistent with the expected maturity level of ISE agency capabilities; the performance scores in yellow indicate areas in which performance is not meeting expectations.

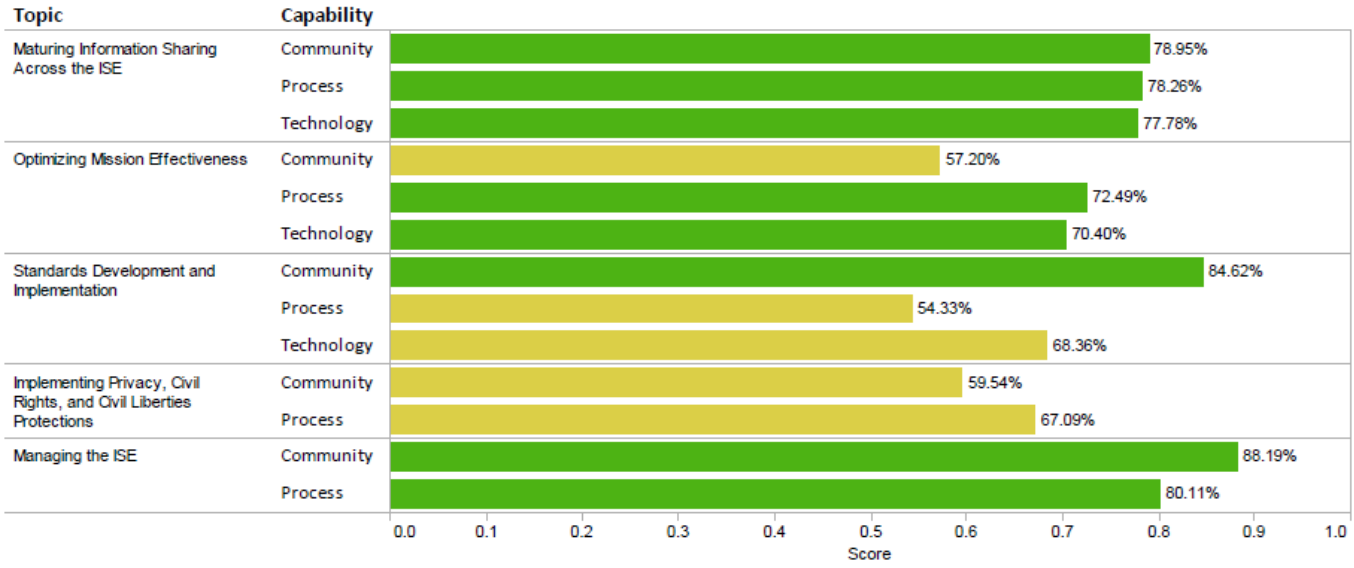


Figure 4a. Overall Performance by Topic and Capability Area

The following chart depicts how well ISE agencies are performing against the topics and subtopics of the ISE Performance Framework at incremental levels of maturity. These topics and subtopics are aligned to the Administration's strategic guidance and priorities, and to the required ISE attributes per IRTPA Section 1016(b)(2). Each ISE Performance Assessment Question is aligned to a specific subtopic and a maturity stage. These alignments allow PM-ISE to use agency responses to the ISE Performance Assessment Questionnaire to determine ISE-wide performance against both the Administration's priorities and the attributes of the ISE. 2012 is a baseline year for using this methodology; therefore, responses to "Maturity Stage 1" questions are the focus of this year's performance assessment and are highlighted. The performance scores shown in green are consistent with the expectations for ISE agency capabilities at Maturity Stage 1 and the performance scores in yellow indicate areas in which performance is not meeting expectations. (Blank cells are not applicable at this maturity stage)

		Maturity		
Topic	**Subtopic**	Current Env.	2-3 yrs.	5-7 yrs.
Maturing Information Sharing Across the ISE	Mature the Use of Common Operating Models	78.08%	80.95%	65.71%
Optimizing Mission Effectiveness	Develop Clear Policies and Rules for Discovery and Access	78.95%	64.65%	
	Enhance Enterprise Data Correlation		55.56%	57.78%
	Improve Assured Network Interoperability	58.73%	58.73%	75.00%
	Improve Information Stewardship and Identity-Based Access Controls	83.01%	85.42%	62.78%
	Share Services that Benefit All Partners		59.48%	65.46%
Standards Development and Implementation	Develop and Enforce Use of Voluntary Consensus Standards	85.96%	69.21%	
	Leverage Federal Acquisition Processes	67.57%	44.78%	
	Promote Entity / Person Tagging	80.00%	44.29%	
Implementing Privacy, Civil Rights, and Civil Liberties Protections	Ensure Accountability and Compliance Mechanisms	66.67%	76.47%	78.95%
	Increase Consistent Government-wide Application of Privacy Protections	73.13%	29.97%	
Managing the ISE	Encourage Progress through Performance Management, Training, and Incentives	77.18%	78.86%	86.67%
	Improve Governance and Remove Barriers to Collaboration	89.95%	85.45%	

Figure 4b. Overall Performance by Topic, Subtopic, and Maturity Stage

PM-ISE's methodology for measuring the capabilities expected at each maturity stage is included in the table below. Each ISE Performance Assessment Question measures performance at a specific maturity stage.

	Maturity Stage 1: Current Environment	***Maturity Stage 2:*** 2-3 Year Time Horizon	***Maturity Stage 3:*** 5-7 Year Time Horizon
Community	Designed to measure a baseline awareness of and participation in the ISE.	Designed to measure agencies' familiarity with the goals of the ISE and their ability to measure themselves against those goals and an increased level of involvement in the ISE community.	Designed to measure agencies equating responsible information sharing progress to mission performance. Shows that agencies are linking information sharing metrics to mission performance metrics.
Process	Designed to measure compliance with ISE processes in agencies' planning efforts.	Designed to measure compliance with ISE processes and functional standards.	Designed to measure the degree to which mission partners have incorporated ISE processes in the execution of their missions.
Technology	Designed to measure compliance with ISE technical direction in agencies' acquisition planning efforts.	Designed to measure the degree to which the information systems used by agencies are compliant with ISE technical standards and interoperable with those in other agencies.	Designed to measure the degree to which mission partners have incorporated and are complying with ISE technical standards in the execution of their missions.

Table 4. ISE Performance Framework Capability Areas and Maturity Stages

Twenty agencies participated in the 2012 ISE Performance Assessment Questionnaire (ISE PAQ:

Central Intelligence Agency
Department of Energy
Department of Homeland Security
Defense Intelligence Agency
Department of Commerce
Department of Defense
Department of Health and Human Services
Department of Interior
Department of Justice
Department of State
Department of Transportation
Department of the Treasury
Federal Bureau of Investigation
National Counterterrorism Center
National Geospatial Agency
National Reconnaissance Office
Office of the Director of National Intelligence
Marine Corps Intelligence
Air Force Intelligence
Army Intelligence

Agency responses are detailed below. Responses to "Yes/No" questions are represented by a bar graph – the percentage shown corresponds to the number of "Yes" responses. Responses to multiple choice questions are represented as a pie chart with the percentage of agency responses for each available question depicted. In addition, agencies were requested to provide narrative examples of activity for all relevant questions. Agency narratives that best represent the activities and trends in the ISE over the past year, both positive and negative, accompany each graphic to enrich the response data.

Note that the percentages depicted below are based on the total number of responding agencies for this question. For example, if only 15 out of the 20 agencies responded to a "Yes/No" question and 10 responded "Yes", the resulting percentage would be 67% (10 out of 15).

Maturing Information Sharing Across the ISE

Figure 5. Joint Terrorism Task Forces Participation (% of agencies that answered "Yes") – Maturity Stage 2

*DoD will have 60 persons operating in JTTFs by the end of FY12. – **DoD***

*IRS-**CI** has over 62 Special Agents that are on JTTFs across the country. These agents hold positions of either full-time/part-time or liaison. – **Treasury***

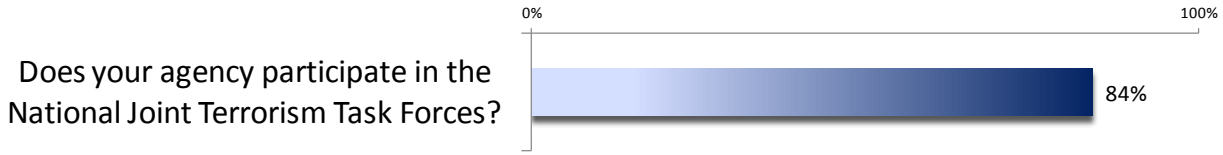


Figure 6. National Joint Terrorism Task Forces Participation (% of agencies that answered "Yes") – Maturity Stage 2

*The TSA regularly coordinates the dissemination of products from the Office of Intelligence and Analysis and Office of Security Policy and Industry Engagement (OSPIE) with the National Joint Terrorism Task Forces (NJTTF). – **DHS***

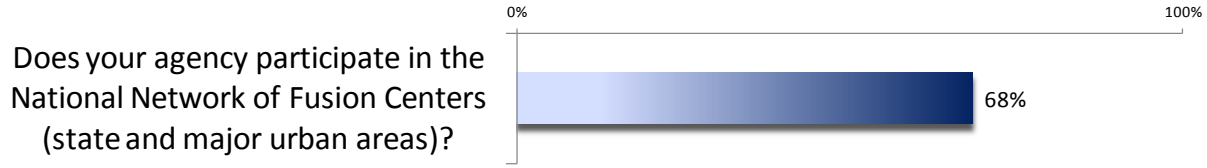


Figure 7. National Network of Fusion Centers Participation (% of agencies that answered "Yes") – Maturity Stage 2

*96 FBI personnel (Special Agents, Intelligence Analysts) are assigned to fusion centers nationwide. The FBI's computer network (FBINet) is installed in 47 of the fusion centers in which we participate. – **DoJ***

*Diplomatic Security participates in the Northern Virginia Regional Intelligence Coordination Center, and DS Agents assigned to JTTF SQUADS sit in fusion centers where their FBI Squad is detailed. – **DoS***

Maturing Information Sharing Across the ISE

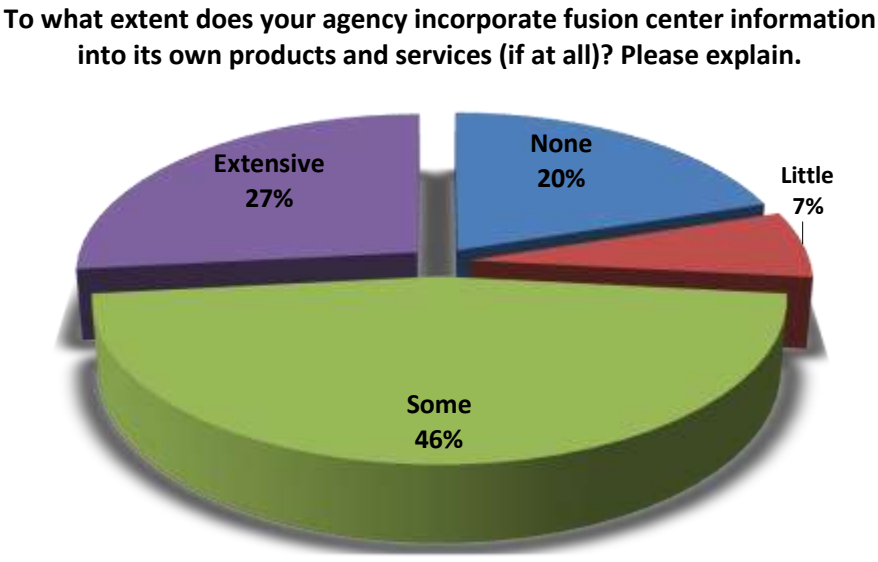


Figure 8. Fusion Center Related Products (% of agency responses) – Maturity Stage 3

> ***Little*** *— HHS prepares terrorism threat analysis products based upon fusion center information.* ***– HHS***

> ***Extensive*** *— Our State and Local Program Office regularly collaborates with Fusion Center personnel to ensure that DHS products are coordinated with Fusion Center partners and that Fusion Center information is incorporated into DHS products and briefings.* ***– DHS***

Figure 9. NSI Participation (% of agencies that answered "Yes") – Maturity Stage 1

> *The DHS SAR Initiative-Management Group (DSI MG) is the lead for DHS' engagement with the NSI. The DSI MG attends NSI core team meetings and regularly includes the NSI PMO in their weekly meetings. The current Director at the NSI PMO is detailed from the DSI MG.* ***– DHS***

Maturing Information Sharing Across the ISE

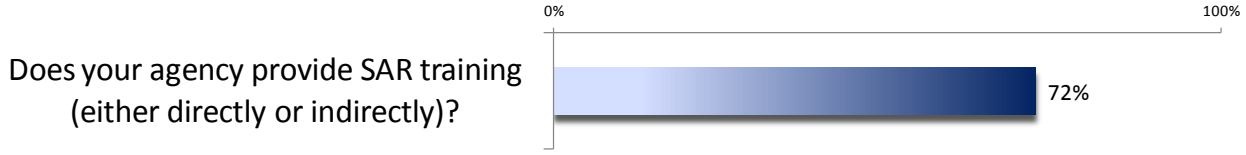


Figure 10. SAR Training (% of agencies that answered "Yes") – Maturity Stage 1

The DHS SAR Initiative-Management Group (DSI MG) conducts quarterly training sessions for SAR Analysts. To date DHS has provided SAR analyst training to over 400 personnel and SAR line officer training to 65,000 personnel. - ***DHS***

SAR training will be mandated for all front line officers and security personnel this year. - ***DOI***

The DoD plans to provide SAR training to an additional 1000 personnel in FY12. – ***DoD***

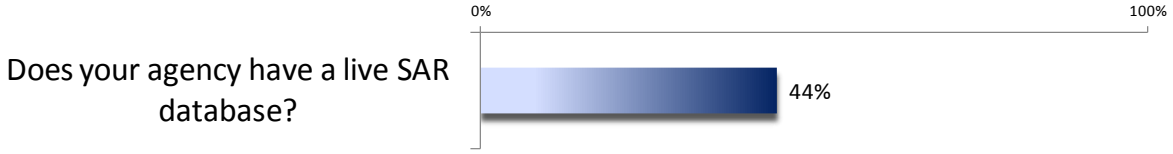


Figure 11. SAR Database (% of agencies that answered "Yes") – Maturity Stage 1

The DoT SAR Database, known as Blue Mercury, went live on October 1, 2011; actual SAR information was entered into Blue Mercury in January 2012. - ***DoT***

Figure 12. eGuardian (% of agencies that answered "Yes") – Maturity Stage 1

Protective Services has multiple eGuardian accounts used to provide SAR information. - ***NGA***

DoD has 1,700 eGuardian accounts. – ***DoD***

Maturing Information Sharing Across the ISE

Figure 13. SARs Validation (% of agencies that answered "Yes") – Maturity Stage 2

All SARs will be validated in the Office of Intelligence, Security, and Emergency Response (S-60) Intelligence Division by trained intelligence analysts. – ***DoT***

The DHS validation process is in keeping with the standards set forth by the PM ISE and the NSI as they relate to training and the utilization of the sixteen behavioral indicators outlined with ISE SAR FS 1.5. – ***DHS***

How often does your agency forward all validated SARs to the NSI (if at all)?

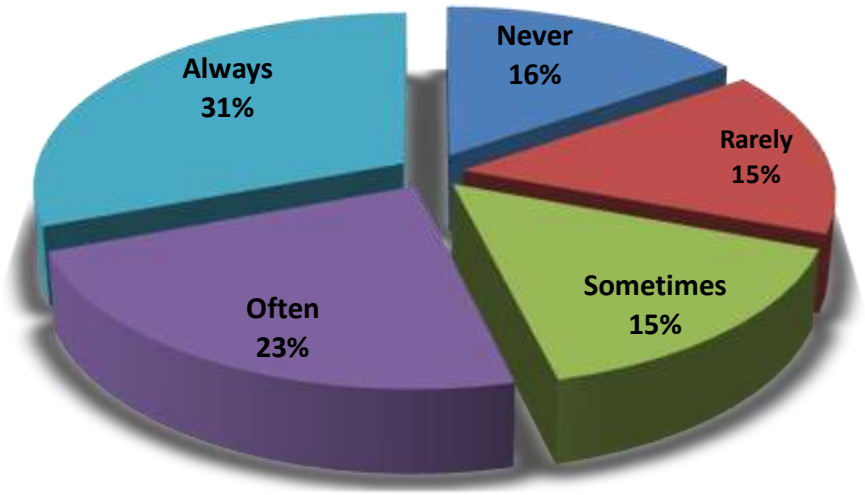


Figure 14. SARs Forwarded to NSI (% of agency responses) – Maturity Stage 2

Always *— Upon validation, SARs meeting the functional standard are then pushed to the NSI via the SAR Vetting Tool. -* ***DHS***

Often *— eGuardian has forwarded over 11,000 SARs to the NSI. -* ***FBI***

Often — SARs are forwarded from the field to our 24/7 Operations Center and then to eGuardian. Our IMARS system will automate this process and retain the second level approval process. - **DOI**

Maturing Information Sharing Across the ISE

To what extent is information gathered from international partners integrated into the watchlisting and screening process?

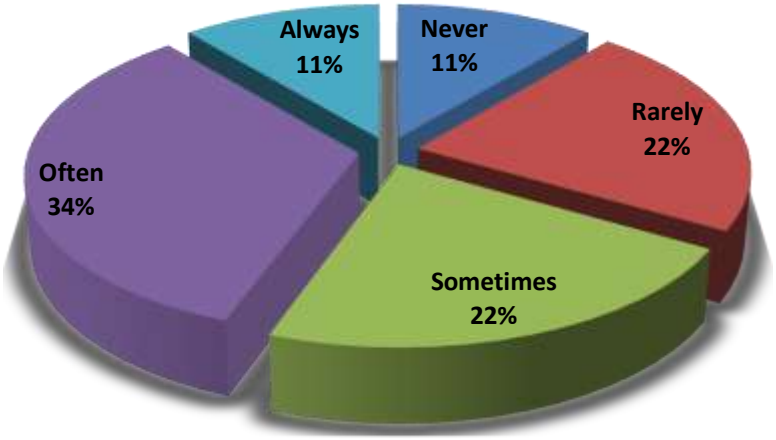


Figure 15. International Watchlisting Influence (% of agency responses) – Maturity Stage 2

*"**Often** — Information gathered from international partners pursuant to Homeland Security Presidential Directive (HSDP)-6 agreements is made available to downstream consumers of the U.S. Government's consolidated terrorist watchlist by the Terrorist Screening Center. - **DHS***

Optimizing Mission Effectiveness

Does your agency have an accessible authoritative source (on 1 or more classification levels) for attribute information on users, for the purpose of making access control decisions?

Figure 16. Authoritative Source (% of agencies that answered "Yes") – Maturity Stage 2

Yes. Virtual directory is currently being utilized. There is also an effort to migrate to CNSS and there is an SBU effort which will require PIV for outbound exchanges. - ***DoJ***

DOI currently uses information found in the Federal Personnel and Payroll System (FPPS) and the DOI Access system as authoritative sources for attribute information on users. Information is then used to configure Active Directory accounts (network access control) and provide information for the creation of DOI Access Cards (PIV 2 Smart Cards). - ***DOI***

For our unclassified system "LEO", we have designed and delivered an identity broker that will allow and support 4 levels of access: 1) Username/Password, 2) Username/Password and Advanced Authentication, 3) Username/Password and Two Factor Authentication, and 4) PKI. In addition, FBI/CJIS accepts SAML supporting Single-Sign On (SSO) from the Identity Provider. – ***FBI***

If your agency does have an accessible authoritative source for attribute information on users for the purpose of making access control decisions, has your agency implemented an accessible authoritative source at any classification level?

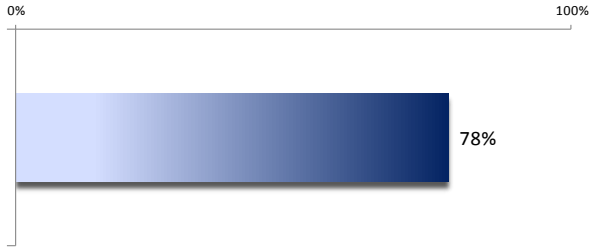


Figure 17. Accessible Authoritative Source (% of agencies that answered "Yes") – Maturity Stage 3

For unclassified systems all access is based on CJIS services being at the unclassified level (SBU/LES). For classified systems the Bureau continues to maintain the Enterprise Directory Service (EDS) , an integrated Commercial Off-The-Shelf (COTS) solution, on FBINET, its Secret enclave. - ***FBI***

The DoD Enterprise Identity Attribute Services (EIAS) is available on classified and unclassified networks. - ***DoD***

Optimizing Mission Effectiveness

From how many federal agencies or departments does your agency accept (and make accreditation decisions without retesting) IT security certification bodies of evidence?

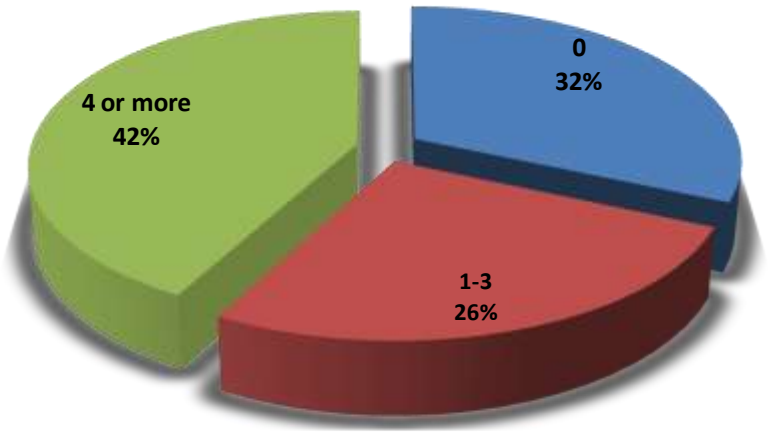


Figure 18. Federal IT Security Certification (% of agency responses) – Maturity Stage 3

1-3 *— We accept DOJ's Cyber Security Assessment and Management (CSAM) solution under their role as an ISSLoB Shared Services Center (SSC) provider; we are in the early stages of exploring the use of DoS's Security Tips of the Day (TOD) solution and leveraging their assessment results and authorization decision; we use an existing C&A from NTSB for various training applications; and we anticipate using the assessments and provisional authorizations conducted by FedRAMP and their Joint Authorization Board (JAB). -* ***DOI***

1-3 *— We participate in the Federal PKI Bridge. -* ***DoS***

1-3 *— We have begun to PIV enable our server infrastructure. We also plan to accept externally issued PIV credentials by the end of the calendar year for access to a number of our web based applications through our Single Sign On solution. -* ***Treasury***

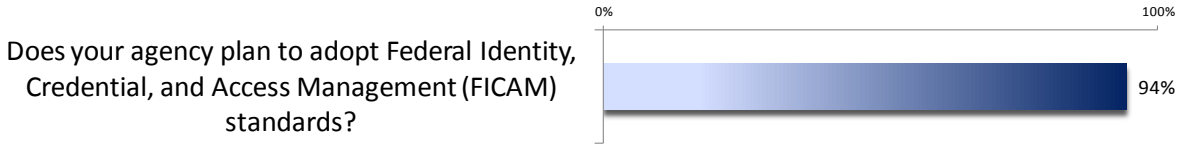


Figure 19. FICAM Adoption (% of agencies that answered "Yes") – Maturity Stage 2

As a DoD Combat Support Agency we have adopted a common identity standard and issued Common Access Cards [CAC] to all personnel. CAC is evolving to align with FICAM and HSPD-12. DoD has also established Personal Identity Verification [PIV]/PIV-Interoperability [PIV-I] credentialing for networks, websites, & applications as well as physical site access. – ***DIA***

For Unclassified systems we are in the process of evaluating these standards, determining how they would affect current systems and requirements, and will make the determination at a later point in time. For Classified systems, the Bureau plans to adopt FICAM standards in future out-years as funding becomes available for the development, piloting, testing and evaluation, and implementation of its Provisioning and Access Control System (PAC). - ***FBI***

Optimizing Mission Effectiveness

To what extent has your agency implemented FICAM standards?

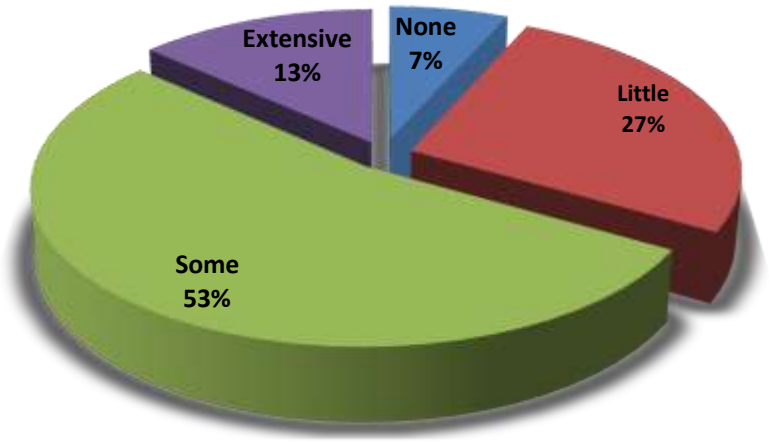


Figure 20. FICAM Standards (% of agency responses) – Maturity Stage 2

> ***Some*** *— For classified systems the Bureau has identified and defined its requirements for an enterprise level identity management solution that would facilitate the adoption of FICAM standards. The Provisioning and Access Control System (PAC) will provide the core functionality for provisioning and de-provisioning user access to key FBI related functions such as Active Directory, Microsoft Exchange, WebTA, User's Home Drive and Office Communicator. -* ***FBI***

> ***Some*** *— DHS is implementing the FICAM standards across the department and is developing and implementing the DHS ICAM Roadmap and Implementation guidelines that provide courses of action and technical solution in alignment with the FICAM standards. -* ***DHS***

> ***Some*** *— DOI has a complete identity and credentialing system for employees, contractors & other support personnel requiring PIV validation and is in the process of developing a complete access management plan in keeping with Government-wide FICAM guidance. -* ***DOI***

> ***Extensive*** *— DoD has fully implemented identity and credentialing processes and is now improving on dynamic access. -* ***DoD***

Optimizing Mission Effectiveness

To what extent does your agency use PKI for ISE related information and mission systems?

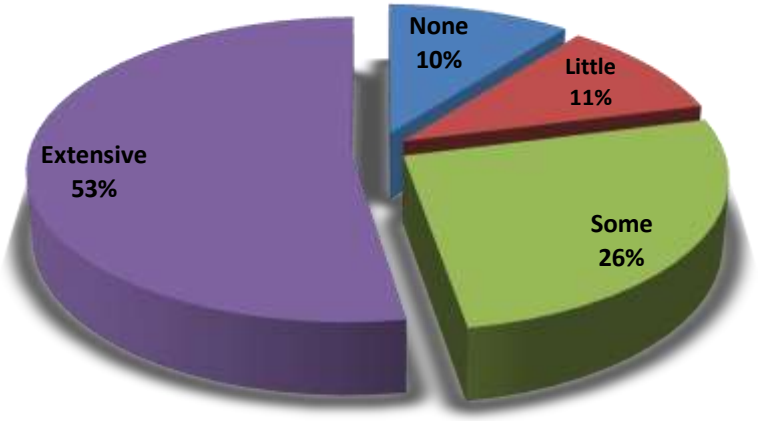


Figure 21. PKI Usage (% of agency responses) – Maturity Stage 1

Extensive *— For unclassified systems the LEO-EP can support PKI for users logging in directly. LEO-EP can also accept SAML credentials with PKI related information and pass that on to respective Service providers. For classified systems the Bureau continues to manage and update its Public Key Infrastructure (PKI) Program which maintains PKI certificates that allow access to websites accessible through its Top Secret/Sensitive Compartmented Information enclave, SCION. -* ***FBI***

Extensive *— DoD is a heavy user of PKI in their business and mission processes. Uses include authentication, digital signatures and encryption. -* ***DoD***

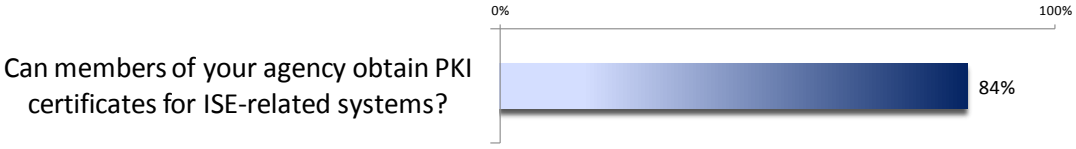


Figure 22. PKI Certificates (% of agencies that answered "Yes") – Maturity Stage 1

For classified systems the FBI's PKI Program supports 30,000 plus subscribers to include certificates for ISE-related systems. This program has a FBI Intranet website which provides up-to-date information on contacts, forms, policies, and procedures for both the FBI's Secret and TS/SCI enclaves. - ***FBI***

Optimizing Mission Effectiveness

Does your agency have a defined MOU/MOA development process that covers discovery and access to data by external partners and systems?

Figure 23. MOU/MOA Process (% of agencies that answered "Yes") – Maturity Stage 2

NGA has an established sharing arrangement process for all international partnerships. – ***NGA***

If your agency has a defined MOU/MOA development process that covers discovery and access to data by external partners and systems, to what extent is this process used?

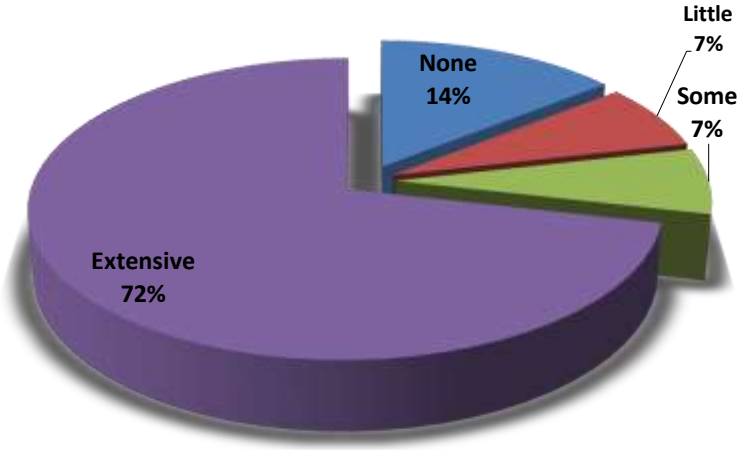


Figure 24. MOU/MOA Process Used (% of agency responses) – Maturity Stage 3

Some *— DHS offices and entities are required to use the MOU/MOA development process pursuant to the "One DHS" Memorandum issued by the Secretary of Homeland Security in 2007. –* ***DHS***

Optimizing Mission Effectiveness

If your agency has a defined MOU/MOA development process that covers discovery and access to data by external partners and systems, what effect has it had on your ability to share information?

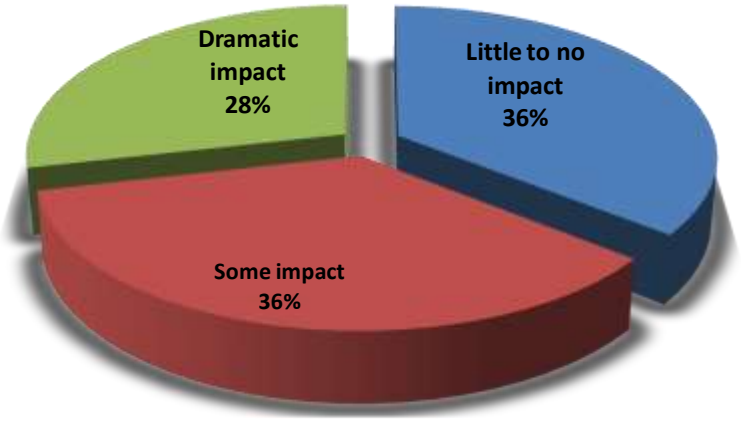


Figure 25. MOU/MOA Effect (% of agency responses) – Maturity Stage 3

Little to no impact *— Development and storing of MOUs/MOAs within the EAIR has allowed for heightened search/discovery of existing MOUs/MOAs which could be leveraged for future use. -* ***DHS***

In regards to privacy, does your agency have a single MOU/MOA repository for system-to-system sharing and access agreements?

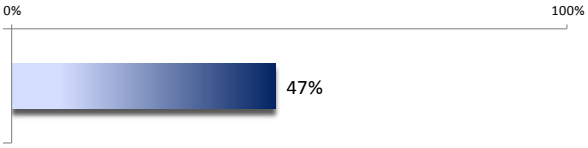


Figure 26. MOU/MOA Repository (% of agencies that answered "Yes") – Maturity Stage 2

Yes. Corporate policy directive 0273D and policy guide 0273PG (Memoranda of Understanding and Non-Contractual Agreements), set forth the procedures and responsibilities for the approval, maintenance, and disposition of MOAs and MOUs. - ***FBI***

The Cyber Security Assessment & Management system (CSAM) is DOI's repository for this information. DOI currently stores MOUs/MOAs and Interconnection Security Agreements (ISAs) in keeping with NIST Special Publication 800-47: Security Guide for Interconnecting Information Systems. - ***DOI***

Yes, the Enterprise Architecture Information Repository (EAIR). - ***DHS***

Optimizing Mission Effectiveness

What impact have improvements in Enterprise Data correlation had on mission outcomes in your agency?

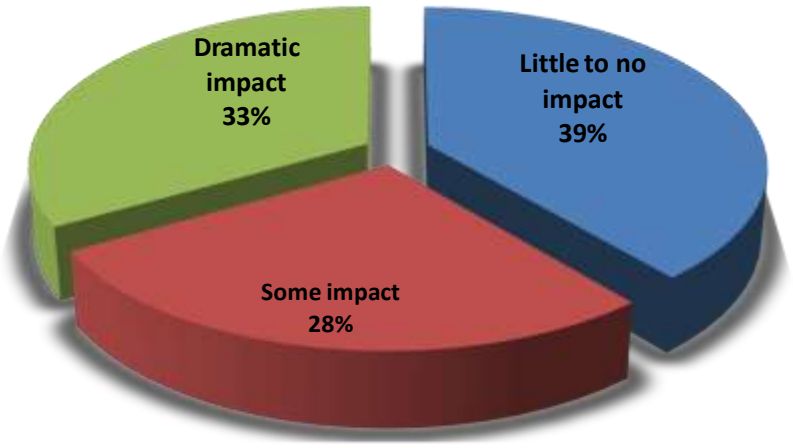


Figure 27. Data Aggregation (% of agency responses) – Maturity Stage 3

Dramatic impact *— Improvements in enterprise data correlation have had a major impact on mission outcomes. For example, CBP supports a system which correlates query requests for current and recurrent vetting of Terrorist identities across data sources. ICE has a similar capability for correlating person identities across major enforcement data sources in response to simple and complex search requests. -* ***DHS***

Some impact *— Dramatic Impact at the component level, as evidenced by the FBI's Data Integration and Visualization System (DIVS) and Law Enforcement National Data Exchange (N-DEx). Deployed in October 2010, DIVS provided the first-ever capability within the FBI to access and perform in-depth searches of intelligence and investigative data from multiple sources previously provided to or collected by the FBI through a single Information Sharing Environment. By the close of FY2011, DIVS was able to search 51 datasets which totaled approximately 1.7 billion information files. As of September 2011, DIVS was being used by all 56 of the FBI's Field Offices, FBIHQ, and eight Legal Attaches (LEGATS) in overseas locations. N-DEx provides incident and case reports, arrest, incarceration and booking data, probation and parole data to approved criminal justice agencies in near real time. During the past year, N-DEx has increased searchable records to over 137 million, from 40 data submitters representing over 4,000 agencies and is adding millions of searchable records via external data sources. -* ***DoJ***

Optimizing Mission Effectiveness

What is your agency's current stage in regards to an information sharing segment architecture?

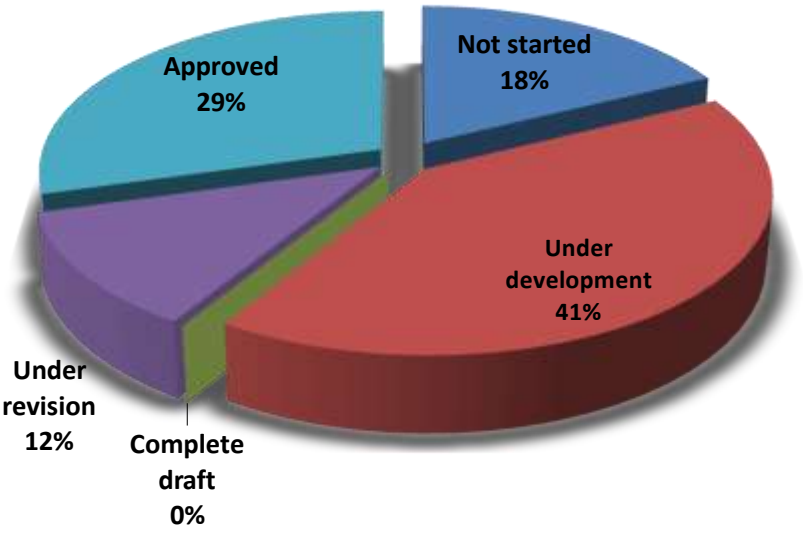


Figure 28. Segment Architecture (% of agency responses) – Maturity Stage 2

Approved *— There have been three versions of the Information Sharing Segment Architecture (ISSA) produced which includes standards, frameworks, systems, and exchanges used across the Department and components to share information. -* ***DoJ***

Under revision *— During CY2011, the FBI established an Enterprise Data Management Program Management Office (EDM PMO) under its Chief Technology Officer. The EDM PMO assumed the position of the FBI's Principal Data Architect, responsible for the Data Reference Model and Information Sharing Segment Architecture for the FBI. This position currently is vacant. -* ***FBI***

Approved *— The DoD Net-Centric Information Sharing Segment Architecture is in draft. The draft architecture addresses enterprise-wide information sharing, to include Suspicious Activity Reporting (SAR). -* ***DoD***

Optimizing Mission Effectiveness

To what extent has your agency's ability to discover, access, and retrieve information needed to accomplish the mission improved based on services shared from external agencies and systems?

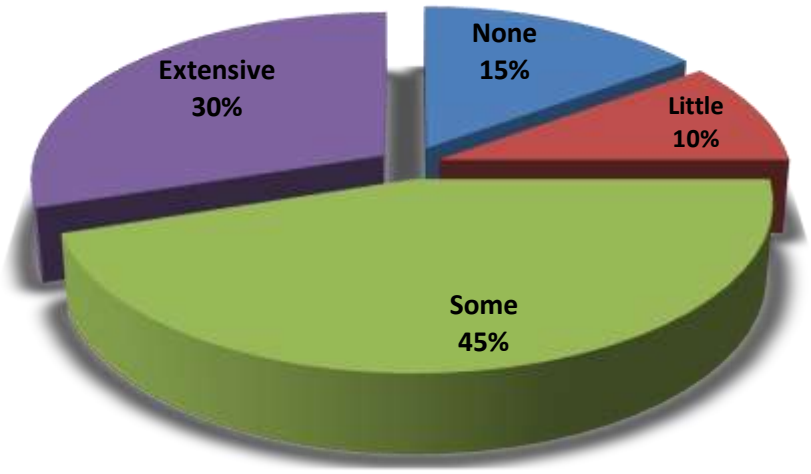


Figure 29. Shared Services (% of agency responses) – Maturity Stage 3

Extensive *— The FBI has enhanced its ability extensively during CY2011. Among other initiatives, the Terrorist Screening System (TSS) leveraged shared data warehousing and business intelligence technology to make metrics available for operational decisions on a real-time basis; the Data Integration and Visualization System (DIVS) increased its usage with the substantial addition of datasets previously provided to the FBI by various sources related to terrorism, counterintelligence, and intelligence; and the FBI increased its capability for foreign language translation by obtaining and deploying the FLUENT application from another government agency on its secret enclave, FBINET. FLUENT, which is available on DIVS, is an enterprise language translation system which quickly translates 70 foreign languages into English and can translate from English into 14 languages. -* ***FBI***

Optimizing Mission Effectiveness

To what degree is there improvement in your agency's terrorism information sharing processes (since last year's survey) with other ISE partners by implementing an ISE Shared Space in your organization?

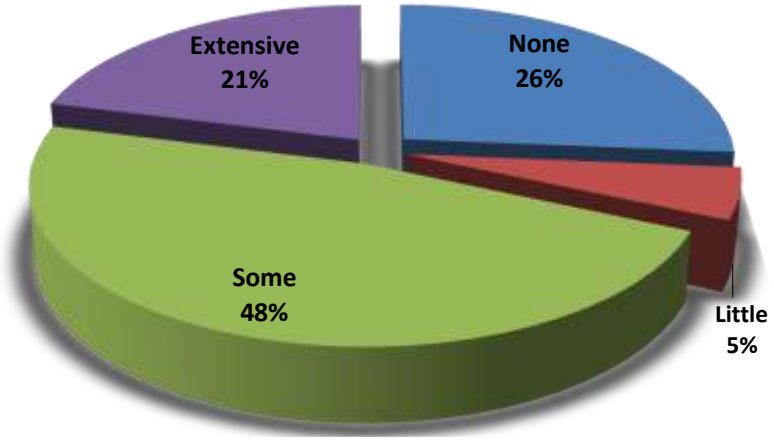


Figure 30. Shared Space Process Improvement (% of agency responses) – Maturity Stage 3

Some *— Over the past year, the Department the transitioned the Homeland Security State and Local Intelligence Community of Interest (HS SLIC), a community of 3,000 state, local, tribal, and territorial intelligence analysts, to the Homeland Security Information Network (HSIN). Further, the Office of Infrastructure Protection has improved the HSIN-Critical Sectors (HSIN-CS) portal to include a capability for critical infrastructure stakeholders to submit SARs to the Department and to the Nationwide SAR Initiative. HSIN-CS serves over 15,000 stakeholders, allowing them to share sensitive but unclassified threat information. -* ***DHS***

Some *— The DOI's Incident Management, Analysis and Reporting System (IMARS) is identifying initial requirements to develop an interface with the FBI's e-Guardian system which will be used as the Shared Space for reporting suspicious activities.* ***– DOI***

Was there a cost savings in regards to your ISE related information sharing processes? Please describe qualitatively.

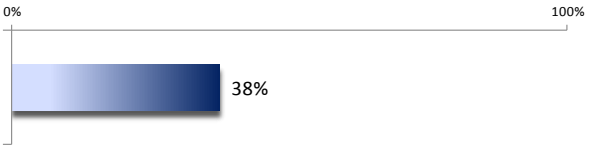


Figure 31. ISE Sharing Cost Savings (% of agencies that answered "Yes") – Maturity Stage 3

DHS consolidated other portals on the system, resulting in a $1.2 million annual cost avoidance that will carry out in future years. - ***DHS***

Undetermined. No analysis has been conducted to determine the level of cost or time savings achieved based on implementation of ISE Shared Space. ***- DoD***

Optimizing Mission Effectiveness

Was there a time savings in regards to your ISE related information sharing processes?
Please describe qualitatively.

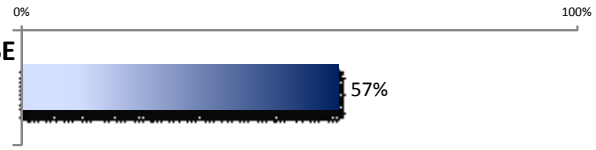


Figure 32. ISE Sharing Time Savings (% of agencies that answered "Yes") – Maturity Stage 3

SARs are shared more efficiently and are searchable using automated systems provided by FBI (eGuardian) and State/Local/Tribal partners, coordinated by BJA/OJP. - ***DoJ***

To what extent has access to terrorism information from ISE partners improved by utilizing their designated ISE Shared Space?

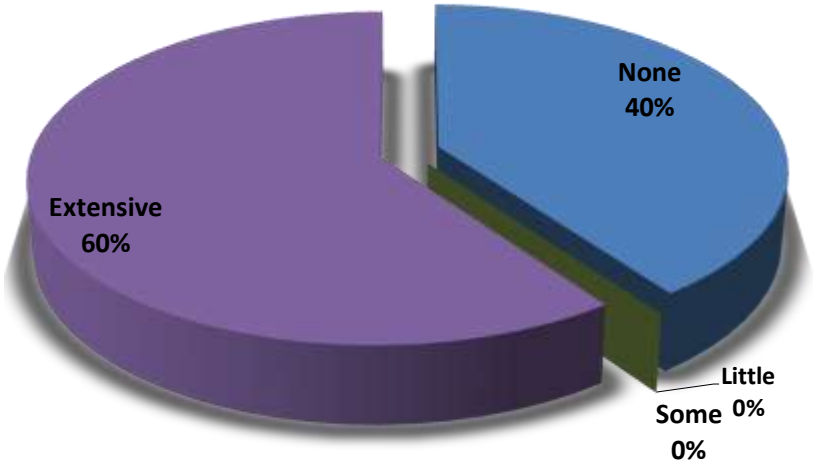


Figure 33. ISE Shared Space Access (% of agency responses) – Maturity Stage 3

Extensive *— Over 360+ DoD installation and facilities globally have access to the ISE Shared Space data via the FBI. -* ***DoD***

Optimizing Mission Effectiveness

Does your agency have a plan to implement a capability to interconnect SBU/CUI networks in order to share terrorism and homeland security information?

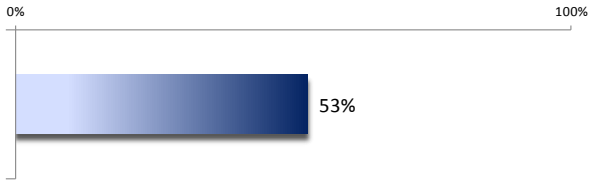


Figure 34. SBU/CUI Plan (% of agencies that answered "Yes") – Maturity Stage 1

The DHS SBU/CUI networks are interconnected through the use of standards that allow interoperability among networks. HSIN PMO is developing an SBU Interoperability Profile based on established and developing standards for identity, secure service exchanges, and access privileges, which will be NIEM-conformant. - ***DHS***

The DOI's Incident Management, Analysis and Reporting System (IMARS) is in the process of initial requirements gathering to develop an interface with the FBI's e-Guardian system which will be used as the Shared Space for reporting suspicious activities. - ***DOI***

The Department currently provides shared data on its third party shared space provider on ODNI's Intelink-U, which is part of the ISE SBU/CUI Interoperability initiative. - ***DoS***

From a Cyber Security perspective, we have no plan to implement a capability to interconnect SBU/CUI networks in order to share terrorism and homeland security information. However, OIA has been trying to facilitate an interconnection between DNI/U and the DO LAN for over two years without much progress. - ***Treasury***

Optimizing Mission Effectiveness

To what extent has your agency implemented interconnection plans for SBU/CUI networks supporting ISE-related missions?

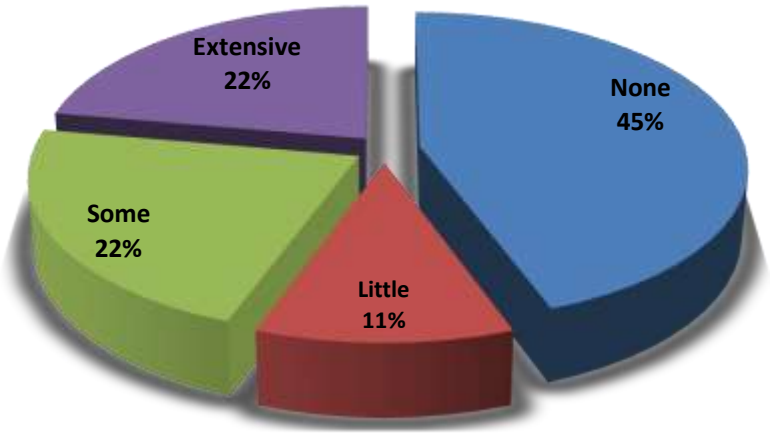


Figure 35. SBU/CUI Implementation (% of agency responses) – Maturity Stage 1

Extensive *— DHS has implemented levels of interoperability across all of its SBU/CUI networks. -* ***DHS***

Some *— Internally, our law enforcement bureaus are all interconnected via IMARS for rapidly sharing ISE-related information. -* ***DOI***

Extensive *— Internal portals have been established within the Office of the Secretary as well as component Operating Divisions for coordination and communication of emergency, crisis, or terrorism information as well methods for coordinating and communicating with other federal agencies, but a Service Level Agreement of interoperability between SBU/CUI networks supporting ISE-related missions has not been established or initiated. -*

Standards Development and Implementation

To what extent has your agency incorporated Common Information Sharing Technical Standards into your architectures?

(Please refer to Information Sharing Environment Enterprise Architecture Framework Version 2.0, September 2008, page 110 - 115)

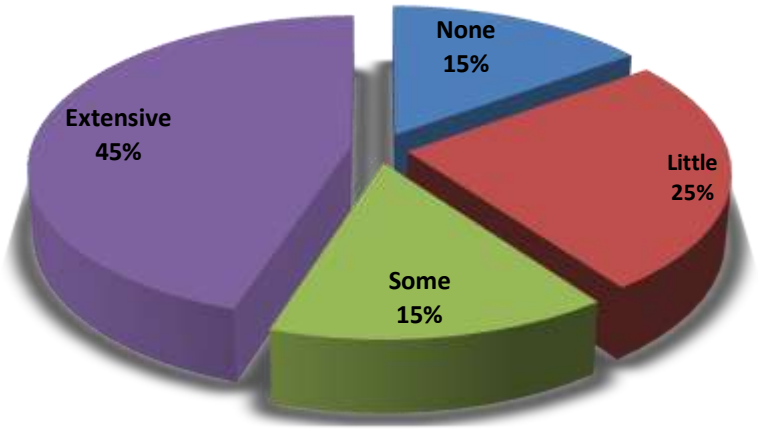


Figure 36. Common Technical Standards (% of agency responses) – Maturity Stage 2

Extensive *— DHS has incorporated standards in to the Homeland Security EA standards profile corresponding to each OSI layer. -* ***DHS***

Extensive *— The Department has implemented numerous IEPDs across many platforms including N-DEx, SAR, NGI, and many others. -* ***DoJ***

Extensive *— DOT has recently stood up a SAR database which is compliant with Common Information Sharing Technical Standards. -* ***DoT***

Extensive *— DIA's architecture and investment management lifecycles implement IC approved technical standards which are compatible with the Common Information Sharing Technical Standards. -* ***DIA***

Standards Development and Implementation

How often does your agency reference 'mission segment architectures' (e.g. SAR) when implementing ISE mission business processes?

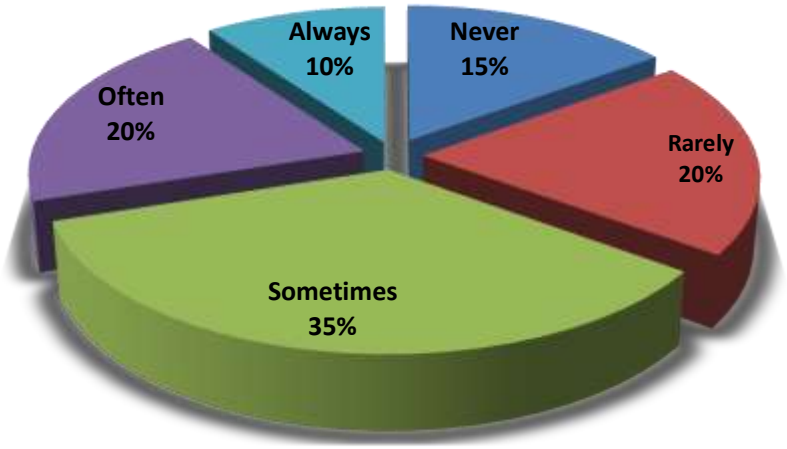


Figure 37. Segment Architecture (% of agency responses) – Maturity Stage 2

Often *— The FBI Enterprise Architecture Office often references mission segment architectures in system upgrades that support ISE mission business processes. Within the FBI mission segment architectures, the ISE core business processes for Suspicious Activity Reporting (SAR), Terrorism Watch List (TWL), and Alerts, Warnings, and Notifications (AWN) are continually addressed to the Law Enforcement and Intelligence Communities through secure interfaces such as Law Enforcement Online (LEO), Foreign Terrorist Tracking Task Force (FTTTF), and the Terrorist Screening Center (TSC). -* ***FBI***

Often *— The Department has a number of segment architectures related to Information Sharing including the information Sharing Segment architecture (ISSA) and Justice Information Sharing Segment architecture (JISSA). -* ***DoJ***

Often *— The Department of Defense has consistently used Information Sharing Standards and Secure Information Sharing strategy, design concepts, and implementation guidance as identified in the DoD Information Sharing Segment Architecture when implementing all ISE mission business processes. –* ***DoD***

Standards Development and Implementation

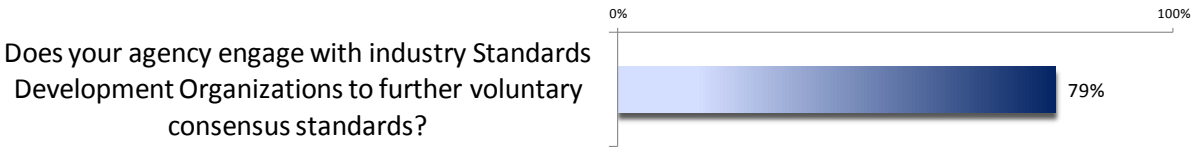


Figure 38. Federal IT Security Certification (% of agency responses) – Maturity Stage 1

During CY2011, the Bureau either chaired or had voting membership in the following Voluntary Industry Standards Development Organizations: American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) Information Technology Laboratory (ITL) Board, to include the National Information Exchange Model (NIEM) Biometrics Domain Working Group and the XML Encoding Working Group; NIEM Program Management Office (PMO), to include the NIEM Business Architecture Committee (NBAC) and the NIEM Technical Architecture Committee (NTAC); Global Justice Information Sharing Initiative XML Structure Task Force (XSTF); International Committee for Information Technology Standards (INCIT), to include participating on the INCITS/M1 Biometrics Technical Committee; and the Interpol Automated Fingerprint Identification System Experts Working Group (IAEWG). - ***FBI***

DoD Is an active member of, and leader in, the Object Management Group (OMG) and the International Standards Organization (ISO). DoD has, in partnership with OMG, developed the UPDM exchange standard.

Military Service Intelligence CIO's and USD(I) participate in the ODNI's IC CIO Council; the Undersecretary of Defense for Intelligence is leading the DI2E Framework to specify the standards, specification, reference implementation and processes necessary to bridge DoD and Intelligence Community information sharing; the DoD Senior Architect Engineer is the current Chair of the Information Integration Standards Working Group, under the White House Information Sharing and Access Interagency Policy Committee; and DoD partnered with NIST to develop the Cloud Strategy and Cloud Reference Architecture. - ***DoD***

The FBI manages the Advisory Policy Board (APB) which is the authoritative council for standards development related to the FBI's Law Enforcement systems. In addition, the FBI currently chairs or provides membership on the following working groups related to United States Government (USG) biometric standards: Electronic Biometric Transmissions Specification (EBTS) Working Group; FBI-Department of Defense (DoD) EBTS Harmonization Working Group; DoD Biometric Standards Working Group (BWG); DoD Biometric Data Sharing (BDS) Community of Interest (COI); Department of Homeland Security (DHS) Biometric Coordination Group; Facial Identification Scientific Working Group (FISWG); and the Iris Experts Group. - ***FBI***

Standards Development and Implementation

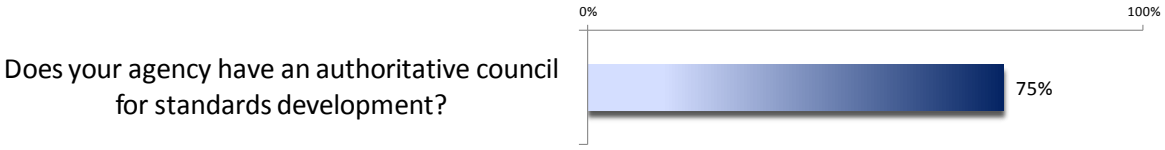


Figure 39. Standards Authoritative Council (% of agencies that answered "Yes") – Maturity Stage 2

Yes. Under the CIO Steering Committee (CIOSC), the NGA Architecture Standards Board provides a governance structure which directs and coordinates all layers of NGA architecture and standards activities and ensures consistent implementation and enforcement across NGA in support of enterprise-wide architecture and development requirements. - ***NGA***

The CIO Council and the ISSGB are the two senior councils that oversee standards development. - ***DHS***

The FBI Advisory Policy Board (APB) serves as the authoritative body for standards development for the Bureau's law enforcement (LE) systems. The APB is chartered by legislation to review policy, technical, and operational issues related to LE IT Programs and Services and make recommendations to the FBI Director. In addition, the FBI has established a Technology Development and Deployment Board (TDDB) chaired by its Chief Technology Officer (CTO) to serve as an authoritative council for standards development for FBI systems in the terrorism, counterintelligence, and intelligence core mission areas. - ***FBI***

Yes. The formal DoD Standards Program is overseen by the DoD IT Standards Committee (ITSC). The ITSC is a formal part of the DoD CIO governance structure. - ***DHS***

Standards Development and Implementation

To what extent has your agency incorporated ISE Functional Standards into the management and implementation of its ISE-related mission business processes?

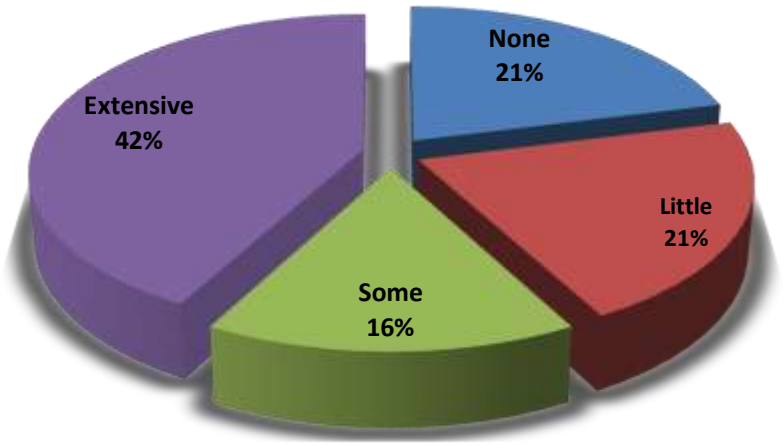


Figure 40. ISE Functional Standards (% of agency responses) – Maturity Stage 2

Extensive *— The Bureau incorporates ISE Functional Standards as new Intelligence Community Directives (ICD) are published and promulgated. During CY2011, the FBI considered new initiatives for the following: ICD 501 (Discovery and Dissemination or Retrieval of Information within the Intelligence Community), ICD 710 (Classification and Control Markings), and ICD 206 (Sourcing Requirements for Dissemination). -* ***FBI***

Extensive *— Common Information Sharing Standards (CISS) functional and technical standards are required for use in RFPs and RFIs for new IT products and services, and CISS standards are also incorporated into the DoD Information Technology Standards Registry (DISR). -* ***DoD***

Extensive *— ISE Standards have been incorporated into the HLS EA Standards Profile. This profile is used as a reference for the DHS Information Sharing Segment Architecture. -* ***DHS***

Standards Development and Implementation

To what extent has your agency incorporated ISE Technical Standards into enterprise architectures and IT capability?

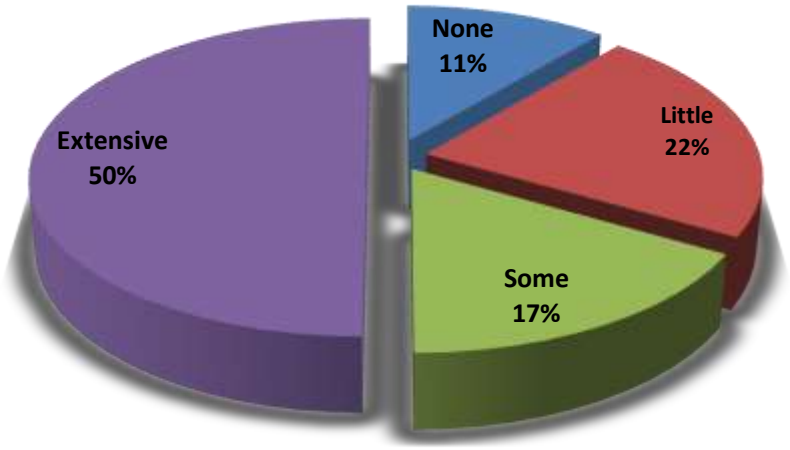


Figure 41. ISE Technical Standards (% of agency responses) – Maturity Stage 2

Extensive *— ISE Technical Standards have been incorporated in Department level information sharing architectures and related IT capabilities and are included in the Department level Information Sharing Segment Architecture (ISSA). -* ***DoJ***

Extensive *— DoD has incorporated ISE Technical Standards into the DoD Standards program and the DoD IT Standards Registry to support cross domain information sharing. All DoD architectures have to conform to the DoD Architecture Framework which is in alignment with the ISE Architecture Framework. -* ***DoD***

Extensive *— ISE Technical Standards are referenced in the Enterprise Standards Profile maintained by the FBI Chief Technology Officer and the Bureau incorporates ISE Technical Standards as part of its IT governance process. As the FBI IT infrastructure is upgraded in phases for all three enclaves, ISE Technical Standards will be incorporated. -* ***FBI***

Does your agency have a single authoritative repository related to ISE Technical or Functional Standards?

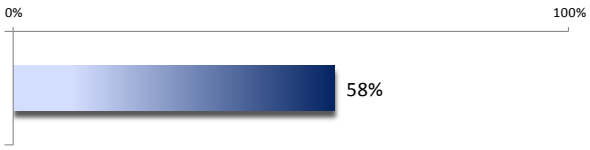


Figure 42. Authoritative Source (% of agencies that answered "Yes") – Maturity Stage 2

DoD has incorporated ISE Technical Standards into the DoD Standards program and the DoD IT Standards Registry where applicable to support cross domain information sharing. The DISR is the DoD single authority Standards Registry for all IT standards which is under the governance of the DoD CIO. - ***DoD***

Yes, an online repository of standards is managed by the DHS Office of Chief Information Officer (OCIO). - ***DHS***

The GEOINT Standards Registry (https://nsgreg.nga.mil) is the Functional Manager's Registry for all GEOINT standards. - ***NGA***

Standards Development and Implementation

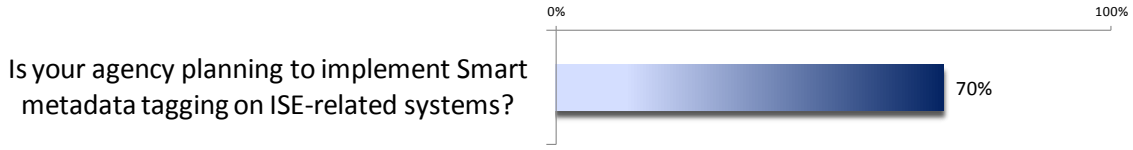


Figure 43. Metadata Tagging Plan (% of agencies that answered "Yes") – Maturity Stage 2

NSA is developing a suite of tools called Smart Data that enables version control, data provenance management, distribution tracking and smart routing. DoD has been coordinating with NSA to assess the applicability of their Smart Data technology for DoD purposes. - ***DoD***

For unclassified systems we participate on the ISE Search and Discovery Team and will implement this wherever possible. For classified systems there is current FBI policy in place that requires tagging of electronically stored information with metadata for systems of records in accordance with the Dublin Core, National Information and Exchange Model (NIEM), and Intelligence Community standards. - ***FBI***

To what extent has your agency implemented Smart metadata tagging on ISE-related systems?

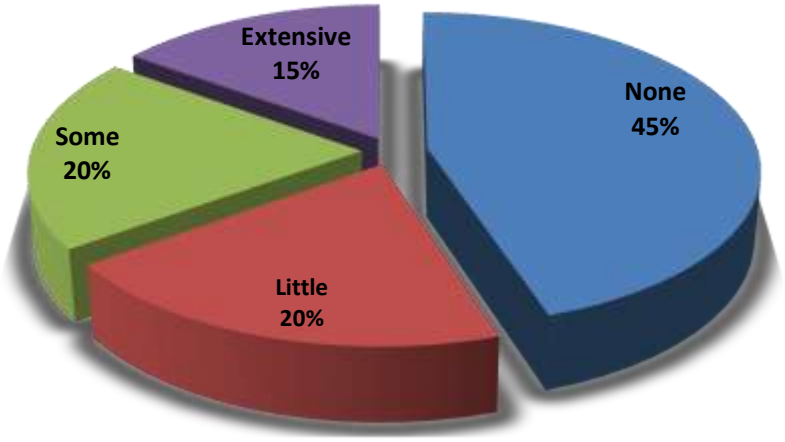


Figure 44. Metadata Tagging Implementation (% of agency responses) – Maturity Stage 2

Some *— For unclassified systems we have implemented the Intelink Intellipedia search into LEO, and will continue to improve on it. For classified systems the FBI IT Program Managers of ISE-related systems continue to have the latitude to consider metadata tagging if there is a requirement identified by users and if there is an enhancement received for system upgrades. For example, most of the metadata in eGuardian already exists in one of the visible data fields displayed to all users. The eGuardian IT Program Manager will consider Smart metadata tagging if users identify a need for it. –* ***FBI***

Some *— NGA has implemented reliable metadata tagging for all imagery delivered to or received from select international partners in the NSG Dissemination Element (NDE) and CURATOR systems. This implementation will be extended to imagery for all international partners, and to non-imagery information, with the implementation of Allied Federated Access starting in CY2013.* ***- NGA***

Standards Development and Implementation

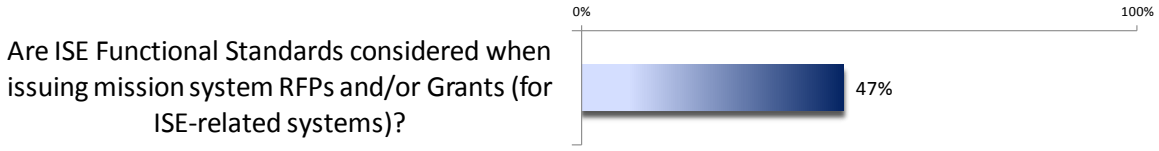


Figure 45. RFP Functional Standards Consideration (% of agencies that answered "Yes") – Maturity Stage 1

Through the Enterprise Architecture Center of Excellence and the System Engineering Lifecycle processes, the NIEM standard is consistently addressed, and others, such as LEXS and GFIPM, are occasionally. Work remains to support the inclusion in the architecture of Enterprise Directory Services, Enterprise Search, Full ICAM implementation, and an Enterprise approach for policy based access controls. - ***DHS***

To the maximum extent possible, ISE Functional Standards are integrated into Agency contracts as compliance or reference documents. - ***CIA***

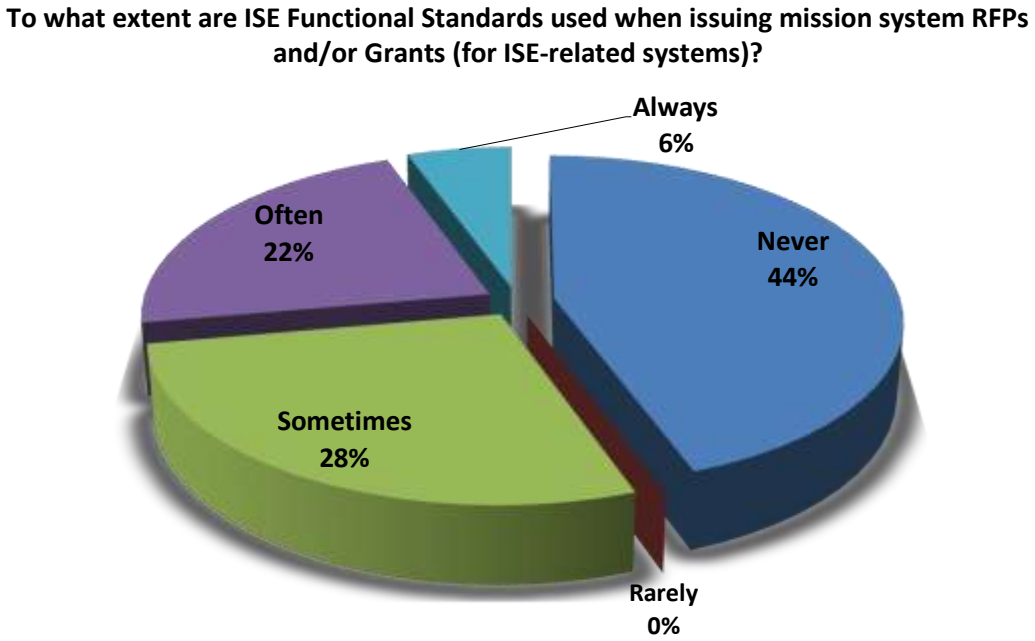


Figure 46. RFP Functional Standards Usage (% of agency responses) – Maturity Stage 3

Sometimes *— Both the ISE Functional and Technical Standards are considered and used in supporting Secure Information Sharing systems, services and applications. The extent to which they are incorporated into RFP is at the decision of the Chief Engineer. However, the Chief Architect and Chief Engineers are guided by the DoD Standards Program and the standards in the DoD IT Standards Registry (DISR) where and when applicable to support cross domain information sharing. -* ***DoD***

Standards Development and Implementation

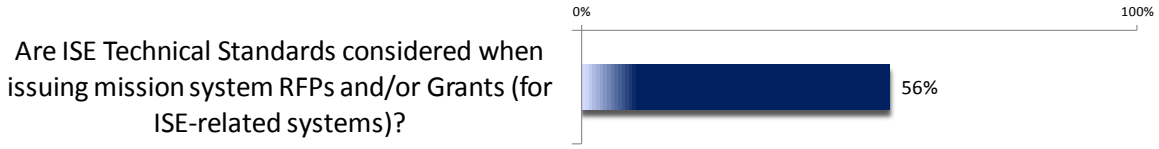


Figure 47. RFP Technical Standards Consideration (% of agencies that answered "Yes") – Maturity Stage 1

The DHS Acquisition process includes language for adherence Enterprise Architecture Center of Excellence and the System Engineering Lifecycle processes which reference formats such as XML, SAML, and XACML. - ***DHS***

ISE Technical Standards are noted on OMB 300s and Exhibit 53s for FBI ISE-related systems. - ***FBI***

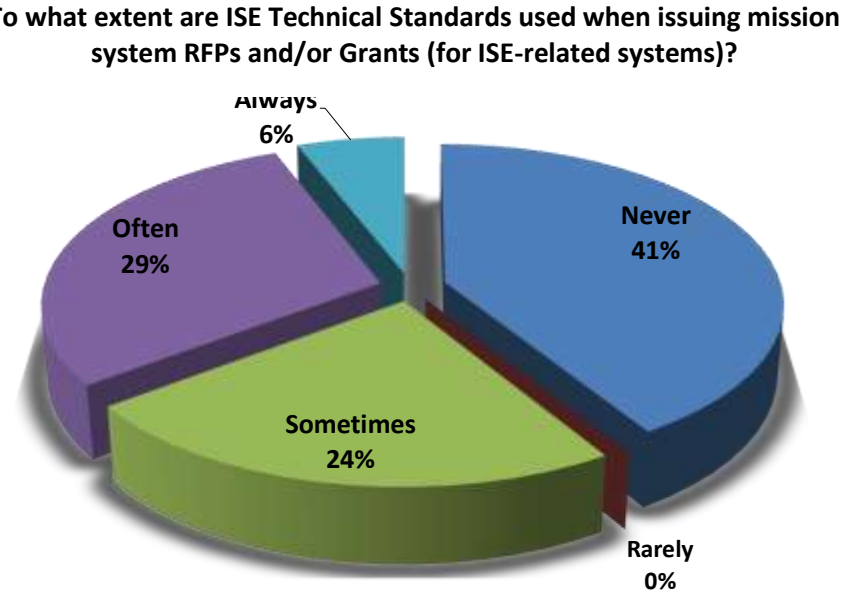


Figure 48. RFP Technical Standards Usage (% of agency responses) – Maturity Stage 3

Often *— ISE Technical Standards are considered and used in supporting Secure Information Sharing systems, services and applications based on mission objectives and are incorporated into DoD RFPs as part of the Acquisition process. -* ***DoD***

Sometimes *— The Department is working to identify all systems that must incorporate ISE functional standards into their architecture and efforts are underway to ensure ISE-related systems are identified and that acquisitions incorporate ISE functional standards into all RFPs. In addition, DHS grant language supports the use of NIEM in its supplemental guidance. -* ***DHS***

Implementing Privacy, Civil Rights, and Civil Liberties Protections

Has your agency submitted an ISE privacy policy to the ISA IPC Privacy and Civil Liberties Sub-Committee?

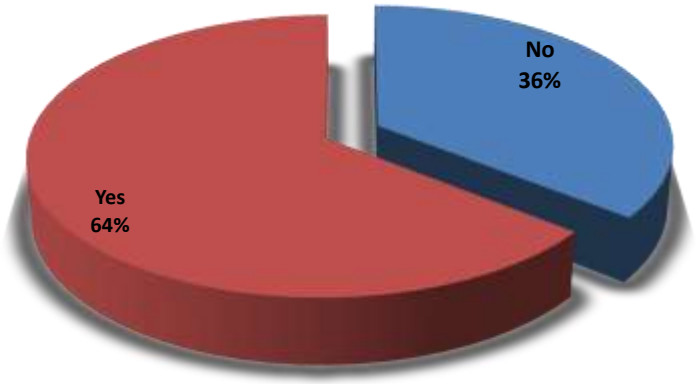


Figure 49. Privacy Policy to IPC (% of agency responses) – Maturity Stage 1

Yes— *"Department of Justice Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment," on January 25, 2010 (DOJ ISE Privacy Policy) was issued. -* ***DoJ***

If your agency has not submitted an ISE privacy policy to the IPC, please indicate where your agency is in the process (not started, under development, etc.).

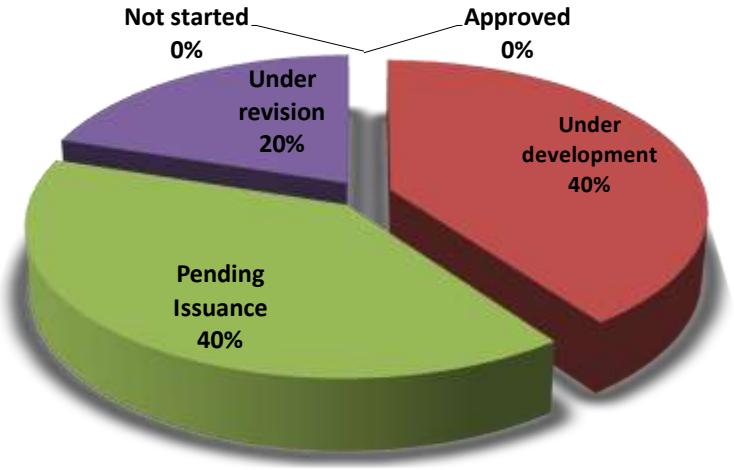


Figure 50. ISE Privacy Policy Status (% of agency responses) – Maturity Stage 1

Under development— *Our policy is in development with ISA-IPC P/CL subcommittee assistance. -* ***HHS***

Implementing Privacy, Civil Rights, and Civil Liberties Protections

What percent of your agency's existing business process(es) have been modified to align with the requirements of your agency's ISE Privacy Policy?

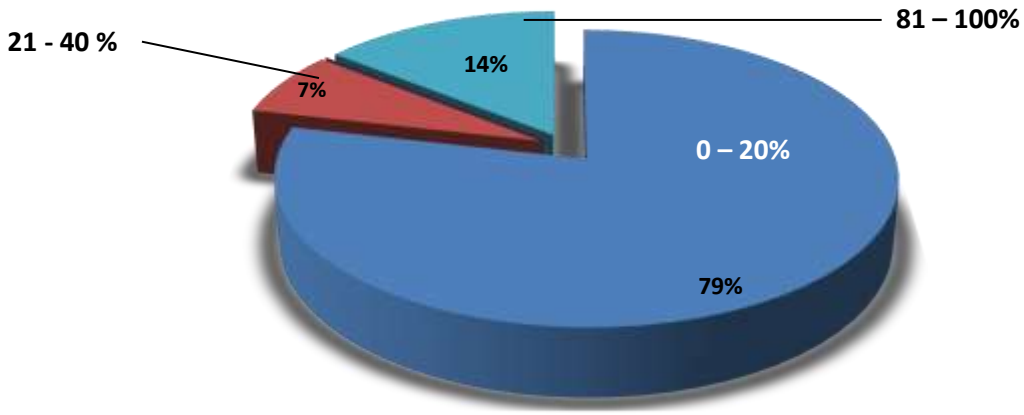


Figure 51. Privacy Policy Process (% of agency responses) – Maturity Stage 2

0 – 20% *— No business processes needed to be modified. Nevertheless, the FBI's Information Sharing Policy Board (ISPB) reviews major information sharing initiatives, a significant portion of which involve sharing terrorism-related information. The DOJ ISE Privacy Policy and other ISE policies are considered during the review of information sharing initiatives, primarily through the review of memoranda of agreement by the FBI Privacy and Civil Liberties Officer and the Office of General Counsel, Privacy and Civil Liberties Unit (PCLU), and by review of other information sharing initiatives, through review by PCLU of privacy impact assessments (PIAs) and privacy threshold analyses (PTAs). -* ***FBI***

0 – 20% *— DOT's ISE related operations have been constructed and implemented in such a manner as to be consistent with the ISE Privacy Policy's requirements. The DOT ISE program privacy risks and controls have been documented in a public facing Privacy Impact Assessment (PIA) and system of records notice (SORN) which can be found at www.dot.gov/privacy. -* ***DoT***

0 – 20% *— The Department does not track modification of business processes directly aligned with the requirements of ISE policy. The DoD net-centric information sharing approach includes ensuring that data and information is collected, used, maintained and disseminated to the greatest extent practicable in accordance with activity that complies with ISE privacy guidelines, the US Constitution and the federal laws of the United States and is consistent with the set of core privacy and civil liberties principles that guide DoD activities. -* ***DoD***

Implementing Privacy, Civil Rights, and Civil Liberties Protections

How frequently are personnel required to review your agency's ISE Privacy Policy?

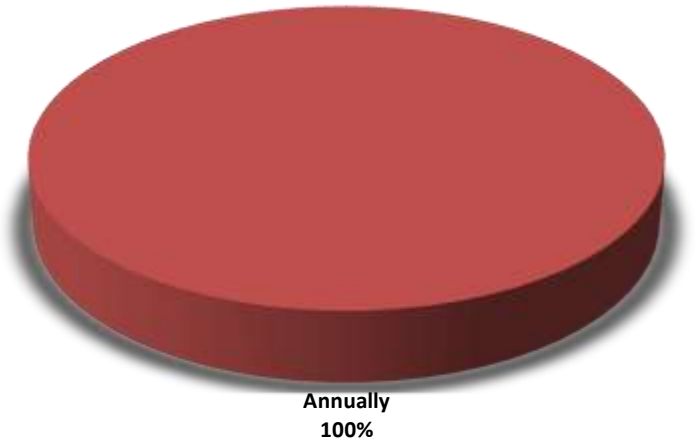


Figure 52. Privacy Policy Review (% of agency responses) – Maturity Stage 1

All DOT personnel receive annual privacy training as required by the Privacy Act and are made aware of their privacy obligations as described in the SAR PIA and SORN. In addition, all staff have direct access to the DOT Chief Privacy Officer to address any privacy related questions or concerns. - ***DoT***

Approximately, how many personnel with information sharing responsibilities received training on your agency's Privacy, Civil Rights, Civil Liberties (P/CR/CL) policies, to include your agency's ISE Privacy Policy? (Maturity Stage 2)

Department employees receive privacy training through the Department's mandatory Computer Security Awareness Training. Under the Department's ISE Privacy Policy, component ISE Privacy Officials develop and conduct training at the component level to ensure compliance. In addition, all eGuardian users are required to receive training before using that system. - ***DoJ***

Since August 2010, 47,360 individuals have completed the FBI's introductory privacy course, of which 1, 793 individuals completed this course in calendar year 2011. - ***FBI***

All DHS employees and contractors are required to take annual training on implementing DHS privacy policy and the Fair Information Practice Principles in DHS operations. - ***DHS***

All Foreign Service and Civil Service employees are required to take the mandatory training regardless of their responsibilities. To date, 11,457 employees have taken this training. - ***DoS***

From February 2011 - February 2012, 75% of the agency (16329 out of 21791 NGA personnel) have completed annual mandatory Privacy Awareness Training. - ***NGA***

Implementing Privacy, Civil Rights, and Civil Liberties Protections

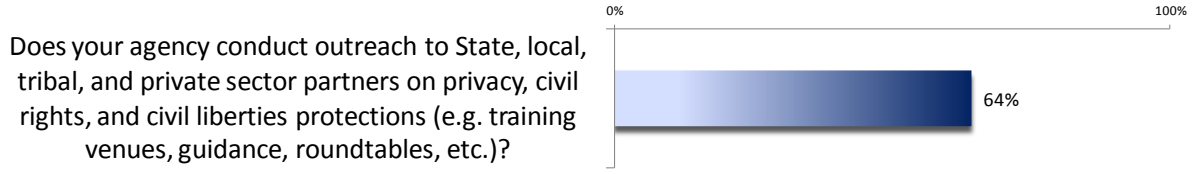


Figure 53. P/CR/CL Outreach (% of agencies that answered "Yes") – Maturity Stage 1

Offerings include an in-person training program delivered on-site to state and major urban area fusion centers; on-line training; and a resources portal for state, local, tribal justice and public safety agencies. DHS personnel also receive training before they are detailed to work at state and major urban area fusion centers. The training includes P/CRCL peer-to-peer exchanges between fusion centers, which are designed to share best practices and lessons learned, as well as P/CRCL training for individual fusion centers and train-the-trainer sessions, which provide fusion center Privacy Officers with the knowledge necessary to train their own staff and partners. - ***DHS***

In 2011, the FBI provided the National Suspicious Activity Reporting Initiative (NSI) Front Line Officer training to approximately 1,561 local, state, tribal and federal law enforcement personnel. This training includes basic privacy and civil liberties modules. Also, the FBI offers basic eGuardian training to our law enforcement partners, which includes privacy modules. - ***FBI***

The Nationwide SAR Initiative, run by the Bureau of Justice Assistance, regularly conducts outreach to SLT and private sector information sharing partners and provides guidance on privacy, civil rights, and civil liberties protections. Additionally, extensive training is also conducted by CJIS regarding privacy and civil liberties across the SLT community. - ***DoJ***

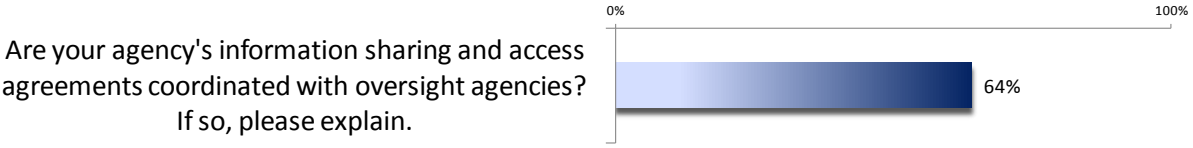


Figure 54. Access Agreements (% of agencies that answered "Yes") – Maturity Stage 2

DHS has altered our departmental information sharing and access agreement (ISAA) review structure to include CRCL, Privacy Office and Office of General Counsel in review of all proposed ISAAs. DHS is developing an IT architecture to support and enhance this review process. - ***DHS***

The Draft DoD Instruction on Support to Fusion Centers was developed in cooperation with the Privacy, Civil Rights and Civil Liberties offices at DHS. The ACLU also participated in the drafting process providing the necessary oversight to ensure all CR/CL concerns were addressed. Additionally, all domestic information sharing and access agreements go through a multi-stage review process, to include a review by the Office of General Council. - ***DoD***

Implementing Privacy, Civil Rights, and Civil Liberties Protections

To what extent has your agency implemented mechanisms that allow you to verify that personnel are compliant with your agency's privacy and civil liberties policies, to include your ISE Privacy Policy?

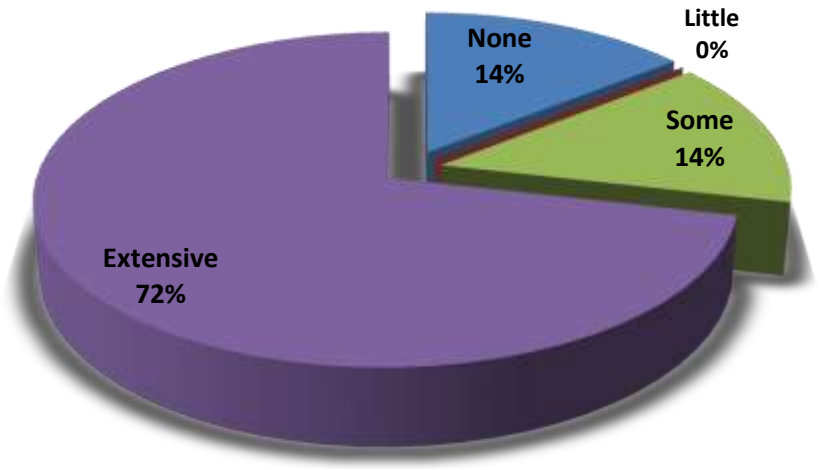


Figure 55. P/CR/CL Verification (% of agency responses) – Maturity Stage 3

Extensive *— DoD has a robust complaint process by which actions that are alleged to be non-compliant with privacy and/or civil liberties policies are reported, investigated and, as appropriate, mitigated. Additionally, organizational inspectors general provide oversight mechanisms. -* ***DoD***

Extensive *— The DHS Offices of Privacy, Civil Rights/Civil Liberties and General Counsel review DHS intelligence products and information reports, proposed information sharing access agreements, and conduct privacy impact assessments of DHS programs and activities. In addition, the Privacy Office Compliance Team conducts compliance reviews of information sharing initiatives to ensure compliance with the terms of those arrangements, including the ISE Policy. -* ***DHS***

Extensive *— The DOI has internal mechanisms to protect privacy and civil liberties through our IMARS system. The Office of Law Enforcement and Security conducts audits of intelligence systems and checks to ensure privacy and civil liberties are appropriately being protected. -* ***DOI***

Extensive *— The FBI has both an Inspection Division and an Office of Integrity and Compliance, which review FBI operational and policy issues, including compliance with privacy and civil liberties requirements. -* ***FBI***

Extensive *— DIA privacy officials ensure personnel pass annual privacy training and report to the Defense Privacy and Civil Liberties Office weekly on any breach information; quarterly on System of Record Notices and privacy and civil liberties complaints; and annually on FISMA-required information. -* ***DIA***

Managing the ISE

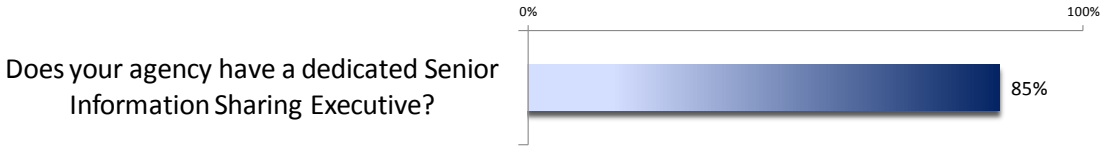


Figure 56. Information Sharing Executive (% of agencies that answered "Yes") – Maturity Stage 1

Yes. The Information Sharing Executive within DHS resides in the Office of Intelligence and Analysis, supported by the Information Sharing and Collaboration Branch. In addition, the Office of the CIO has established and filled an Information Sharing Environment Executive position to ensure focus on the removal of technology barriers associated with the implementation of the ISE. - ***DHS***

The Chief Information Sharing Officer (CISO) is the dedicated Senior Information Sharing Executive and serves as the FBI's designated ISA IPC representative as well as the Senior Official for Information Sharing and Safeguarding as required by EO 13587. - ***FBI***

The CIO is the Senior Information Sharing Executive. – ***DoS***

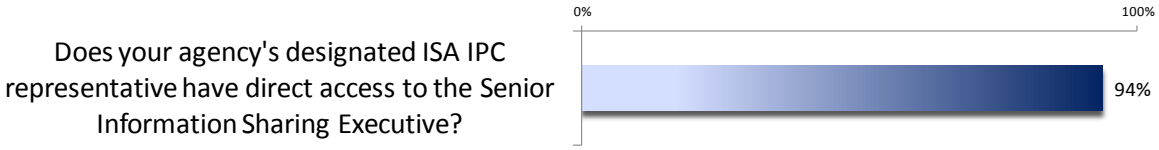


Figure 57. IPC Access (% of agencies that answered "Yes") – Maturity Stage 1

The FBI's dedicated Senior Information Sharing Executive serves as the designated ISA IPC representative. - FBI

The ISA IPC representative regularly communicates with the Senior Information Sharing Executive on ISE issues, as needed. - ***DoS***

The senior information sharing executive is the Director, Office of Intelligence, Security, and Emergency Response (S-60) and the ISA IPC representative is the S-60 Intelligence Division Chief who routinely meets with the S-60 Director on a range of intelligence and security matters. - ***DoS***

Managing the ISE

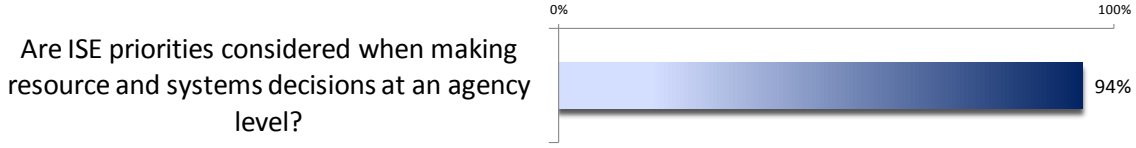


Figure 58. ISE Priorities (% of agencies that answered "Yes") – Maturity Stage 2

Yes, ISE priorities are taken into consideration at the Department level and DOJ works closely with the PM-ISE to ensure that we remain current on new initiatives. - ***DoJ***

The Department's Information Sharing and Safeguarding Governance Board (ISSGB) communicates its priorities throughout the Department's Planning, Programming, Budgeting and Execution (PPBE) process. In April 2010 Department directed the development of an information sharing "roadmap" to use as both a plan of action and a management tool to ensure information sharing activities enable the achievement of the Homeland Security Vision and the Quadrennial Homeland Security Review's (QHSR) missions, goals, and objectives. - ***DHS***

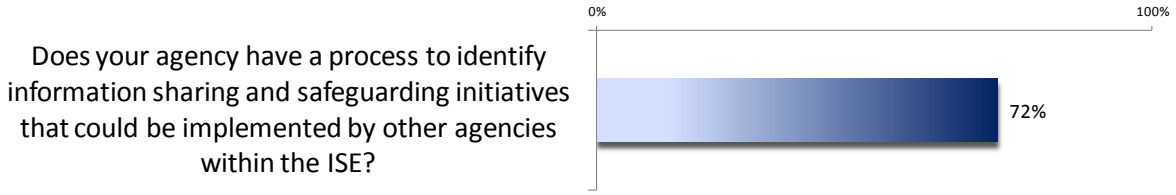


Figure 59. Identify ISE Initiatives (% of agencies that answered "Yes") – Maturity Stage 1

The FBI Information Sharing Policy Board identifies initiatives from across the agency related to information sharing and safeguarding. These initiatives are communicated through the Senior Information Sharing and Safeguarding Steering Committee and the ISA IPC and associated subcommittees. - ***FBI***

The Department's representatives at interagency information sharing and safeguarding fora regularly report and participate at the Information Sharing and Safeguarding Governance Board. - ***DHS***

Managing the ISE

Does your agency have a process to communicate its own information sharing and safeguarding initiatives to the ISA IPC?

Figure 60. IPC Communication (% of agencies that answered "Yes") – Maturity Stage 1

The FBI has a longstanding presence in the ISA IPC and communicates regularly with the IPC membership about FBI initiatives that might be helpful to the interagency. - ***FBI***

Yes, a process to communicate information sharing and safeguarding initiatives exists via direct communication and participation in PM-ISE and sub-working groups. - ***DoJ***

The Department's representatives at interagency information sharing and safeguarding for a regularly report and participate at the ISSGB. The Information Sharing Executive's Deputy regularly attends the ISSGB and communicates information sharing and safeguarding initiatives to the ISA IPC. - ***DHS***

DoD provides representatives to ISA IPC meetings and events consistent with their respective areas of responsibility. These representatives communicate DoD information sharing initiatives to the ISA IPC and its working groups. - ***DoD***

Managing the ISE

To what extent has your agency communicated its own information sharing and safeguarding initiatives to the ISA IPC? Please explain.

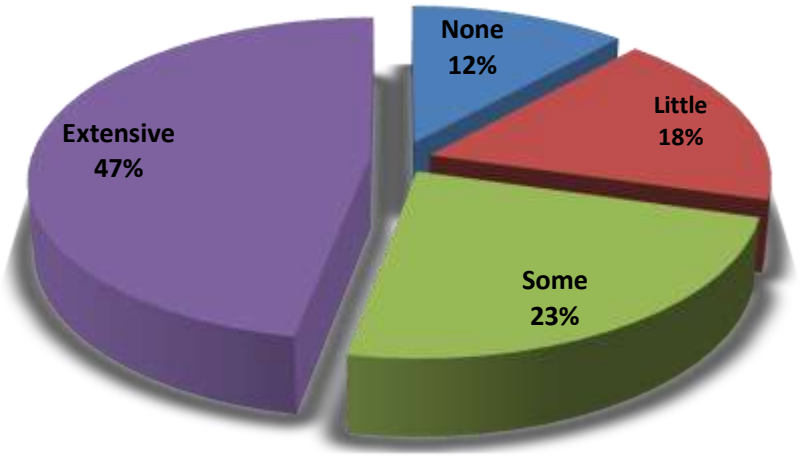


Figure 61. Extent of IPC Communication (% of agency responses) – Maturity Stage 2

Extensive *— The Department's representative regularly participates on behalf of the Information Sharing Executive in the ISA IPC meetings. Prior to attending the meeting, the Department's representative is fully briefed on information sharing and safeguarding initiatives within the Department that are relevant to the ISA IPC discussions. Individual offices within the Department also participate actively in the process. The Department's State and Local Program Office (SLPO) for instance uses the Fusion Center Subcommittee of the ISA IPC routinely to communicate fusion center information sharing and safeguarding initiatives with the ISA IPC. The U.S. Coast Guard also has an observer seat on the ISA IPC and coordinates concerns. -* ***DHS***

Some *— CIA has representatives to multi-agency forums, to include the WikiLeaks SISSSC, the ISA IPC, the ISSC, CNSS, etc., at which we share best practices with regard to information sharing and safeguarding best practices. -* ***CIA***

Extensive *— The Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs is represented at the ISA IPC and the sub-IPCs regularly to share information sharing and safeguarding initiatives with the other agencies of the ISE. DoD and DHS regularly exchange information on the procedures adopted to facilitate the sharing of DoD secure information with the State and Major Urban Area Fusion Centers. -* ***DoD***

Managing the ISE

What degree has your agency implemented any mission-specific training that supports information sharing and collaboration? Please provide examples.

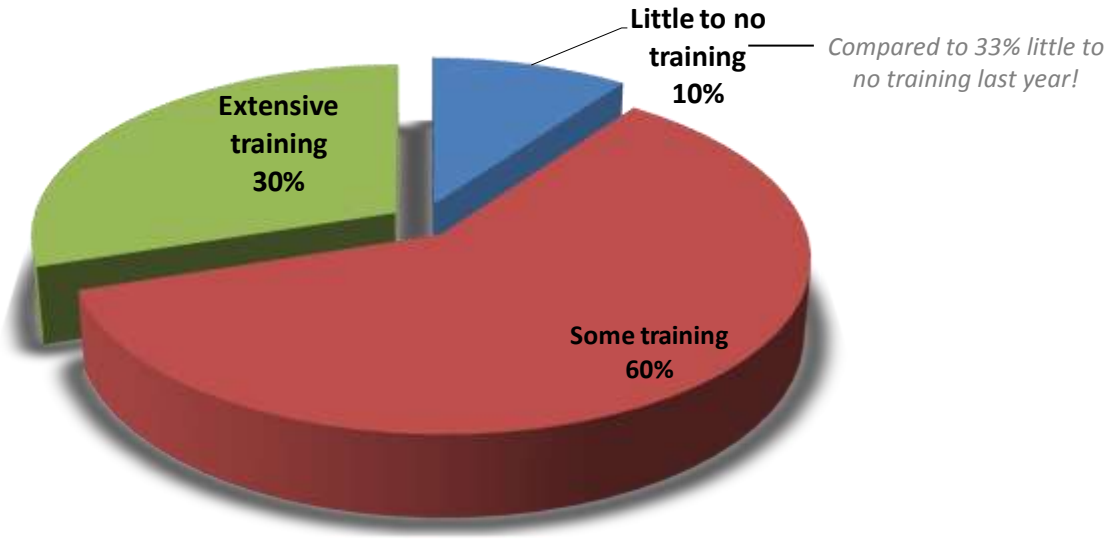


Figure 62. Information Sharing Training (% of agency responses) – Maturity Stage 1

Some training *— All DHS government and contract employees occupying mission-critical information sharing positions are required to complete the ISE Core Awareness Training. In addition, DHS uses the National Information Exchange Model (NIEM) training curriculum for IT resources. -* ***DHS***

Extensive *— The N-DEx Program Office offers self-paced Computer Based Training and training events with local state, regional, tribal, and federal criminal justice agencies to fully expand the footprint of N-DEx as the only nationally-scaled information sharing system. -* ***DoJ***

Extensive *— ODNI, through the Intelligence Learning Network, has developed three new programs for IC-wide participation. All three programs stress information sharing either through integration of intelligence or collaboration. -* ***ODNI***

Some training *— HHS developed a cadre of private sector liaison officers (LNOs) from among our critical infrastructure protection partnership. These individuals have received training on emergency response operations, including relevant ICS (Incident Command System) courses and tailored training related to HHS and ESF-8 emergency response. The LNOs serve as a conduit for information sharing with the private sector as a whole. -* ***HHS***

Managing the ISE

What degree of success has mission specific trainings produced improvements to information safeguarding and stewardship?

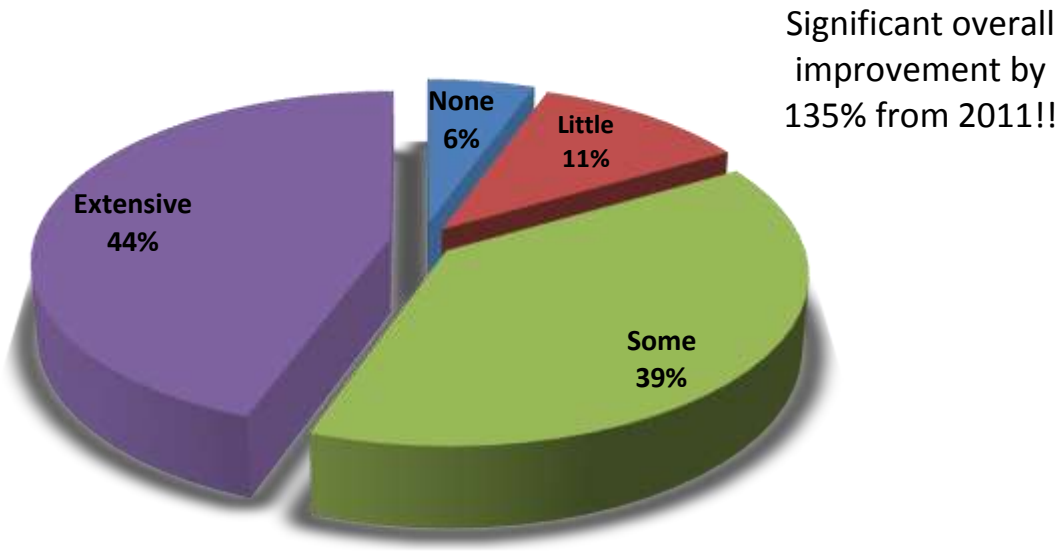


Figure 63. Training Success (% of agency responses) – Maturity Stage 2

Extensive *— The TSC Outreach training has resulted in agencies creating standard operation procedures for contacting the TSC during an encounter with a potential terrorist and for obtaining pertinent watchlisting information and sharing this information with the TSC. The TSC was recognized as the first recipient of the Fusion Center Information National Award based on the TSC's information sharing within the Law Enforcement environment. -* ***FBI***

Extensive *— The [Protected Critical Infrastructure Program] PCII Program has helped us to conduct several information collection projects with the private sector that would not have been possible without it. The LNOs have shown their value in increasing information sharing, especially during the 2009-H1N1 influenza response. In addition, HHS developed departmental NSI policy and handbook that covers information safeguarding and appropriate sharing. -* ***HHS***

Extensive *— The Privacy Awareness Training Course is required across the Department to ensure that personnel are adequately protecting US person information. In addition, for all I&A staff, Intelligence Oversight is a required training seminar in order to safeguard the handling of US persons information. -* ***DHS***

Managing the ISE

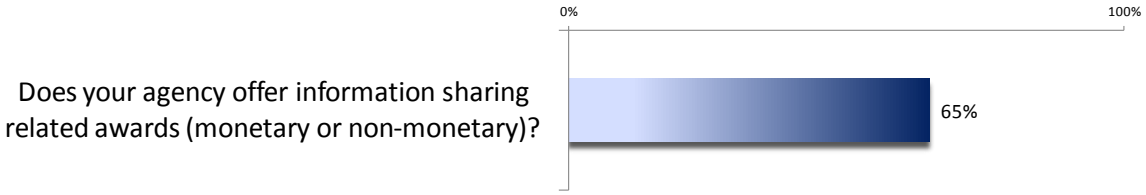


Figure 66. Awards (% of agencies that answered "Yes") – Maturity Stage 2

NGA employees may be nominated for and receive a variety of monetary and non-monetary awards. include, but are not limited to, Individual or Group Special Act or Service awards, or Time Off awards. - ***NGA***

Although there is no special emphasis award for information sharing, information sharing plays a prominent role in nominations submitted for most of the awards in the DNI's National Intelligence Community Awards (NICA) program. - ***ODNI***

DOI has a performance award system that allows supervisors to give an award to an employee for excellent information sharing. Such awards can be monetary or non-monetary. - ***DOI***

The Secretary's Award for Outstanding Achievement in Information Sharing (currently in final approval) is designed to assist in encouraging, adding value, and developing a culture where the responsibility to provide information is understood and practiced consistently throughout the Department. In addition, individual components recognize their employees for information sharing accomplishments. In addition, both the annual US-VISIT Awards Ceremony and the Assistant Director for Program Integration and Mission Services offer rewards related to information sharing. - ***DHS***

How many candidates were nominated in 2011? Please provide examples. (Maturity Stage 1)

All seven members of the Intelligence Division were nominated for and received monetary awards for superior performance in information sharing and collaboration. - ***DoT***

CBP nominated and recognized during CBP's annual Award Ceremony at least 266 employees for their efforts in information sharing and collaboration with CBP partner agencies at all levels of government and private sector. - ***DHS***

In 2011, 5 individuals were so recognized. In one case, 3 FBI analysts worked with the California State Terrorism Threat Assessment Center (STTAC) to help identify regional threats. The STTAC Commander personally commended the analysts and the FBI for dramatically enhancing law enforcement domain awareness in California and neighboring states. - ***FBI***

The DoD CIO recognizes persons and teams throughout DoD for exceptional performance in eight critical IT areas, including Information Sharing. In 2011 the DoD CIO's office received more than 70 nominations for this award, several of which, cited outstanding achievement in information sharing as part of excellence in information management and information technology performance. - ***DoD***

APPENDIX B – MISSION-BASED TEST SCENARIOS

PM-ISE formalized the concept of test scenarios to help leadership determine if the ISE is achieving its desired capabilities. The test scenarios are designed to put these capabilities into a mission context. PM-ISE also encourages agencies to create scenarios independently and provided a "cookbook" to assist with their development. This allows agencies to possess and develop their own compatible performance frameworks to further their respective capabilities. These performance frameworks will help guide ISE performance metric development; development that will expand as the ISE collectively matures. Test scenarios are a key component of the ISE Performance Framework, as they reflect the mission impacts of responsible information sharing to the ISE community of operators, investigators, and analysts.

In the fall of 2011, PM-ISE and ISE agencies developed the following test scenarios:

1. Improving role-based access to ISE-SAR and underlying case file content – implementation of privacy policy automation
2. Improved law enforcement maritime response to a WMD threat by enhancing first responders' situational awareness
3. Improving cross-domain access to distributed information through federated search
4. Removing impediments to federal acquisition and enabling out-of-the-box future interoperability through standards
5. Enabling event deconfliction through common standards to promote officer safety
6. Incentivizing information sharing of insider threat information within agencies and throughout government
7. Using machine generated SARs to aid detection of threats to CIKR
8. Using NIEM as an enabler to share international counterterrorism data on gang-related activity for watchlisting and screening
9. International humanitarian aid and disaster relief coordination efforts
10. Improving public health response to biological threats with increased information to first responders

These test scenarios illustrate government response to a public safety, law enforcement, counterterrorism, or homeland security situation over three time horizons, now, two to three years in the future, and five to seven years hence. Each response demonstrates the analysts', operators', and investigators' improved ability to execute their mission objectives based on investments toward information sharing. For each response point, assumptions are provided to highlight the work required to bridge the capability gap from the previous response, and metrics are shown to concretely demonstrate the improved capability of the ISE community. Each scenario is illustrated in the following pages.

This page intentionally left blank

Scenario #01: Improving Role-Based Access to ISE-SAR and Underlying Case File Content – Implementation of Privacy Policy Automation

Situation

An analyst working in the State X Fusion Center ["XFC"] analyzes a series of possible terrorism related arson incidents occurring near a number of CIKR facilities. A witness from one of the incidents reports seeing a red pickup truck near the scene of one of the incidents carrying a State Y license plate: JC354. Several reports from other arson scenes also note witnesses saw a red vehicle.XFC analyst conducts a Federated Search in the NSI and determines that State Y fusion center's ISE-SAR database has an entry indicating arson activity with similar circumstances as the arson incidents occurring in State X.

The arrows below represent expected increase (⇧) or decrease (⇩) for a particular measure as the capability matures.

Operating Environment

Now	2-3 Years	5-7 Years
 Manual approval to access data based on unreliable, un-standardized 'need to know'	 Policies and procedures in place to allow expedited sharing	 Role-based access to ISE SAR, including privacy policy automation
Assumptions & Measures	**Assumptions & Measures**	**Assumptions & Measures**
• Privacy policies incorporate redress • P/CL/CR officers handle all cases ad-hoc • 100% NSI members trained • XX hrs Sharing Cycle Time • XX% Access Status Error Rate • XX% Cases Require Adjudication • # Reported Violations • # Audit-Discovered Violations • % Redress Mech. Compliance	• 100% NSI members trained ⇧ 50% of privacy policies harmonized • Info sharing policy agreement guidance in place ⇩ P/CL/CR officers handle 50% cases ad-hoc ⇩ XX hrs Sharing Cycle Time ⇩ Access Status Error Rate ⇩ % Cases Require Adjudication ⇩ # Reported Violations ⇩ # Audit-Discovered Violations ⇧ % Redress Mech. Compliance	• 100% NSI members trained ⇧ 95% of privacy policies harmonized • Sharing info system in place • Role-based access in place ⇩ Sharing done on trusted network backbone ⇩ XX hrs Sharing Cycle Time ⇩ Access Status Error Rate ⇩ % Cases Require Adjudication ⇩ # Reported Violations ⇩ # Audit-Discovered Violations ⇧ % Redress Mech. Compliance
Maturity	**Maturity**	**Maturity**
Community *Awareness* Process *Exploration* Technology & Standards *Awareness*	Community *Involvement* Process *Adoption* Technology & Standards *Exploration*	Community *Integration* Process *Harmonization & Compliance* Technology & Standards *Integration*

Figure 67. ISE Performance Scenario #01

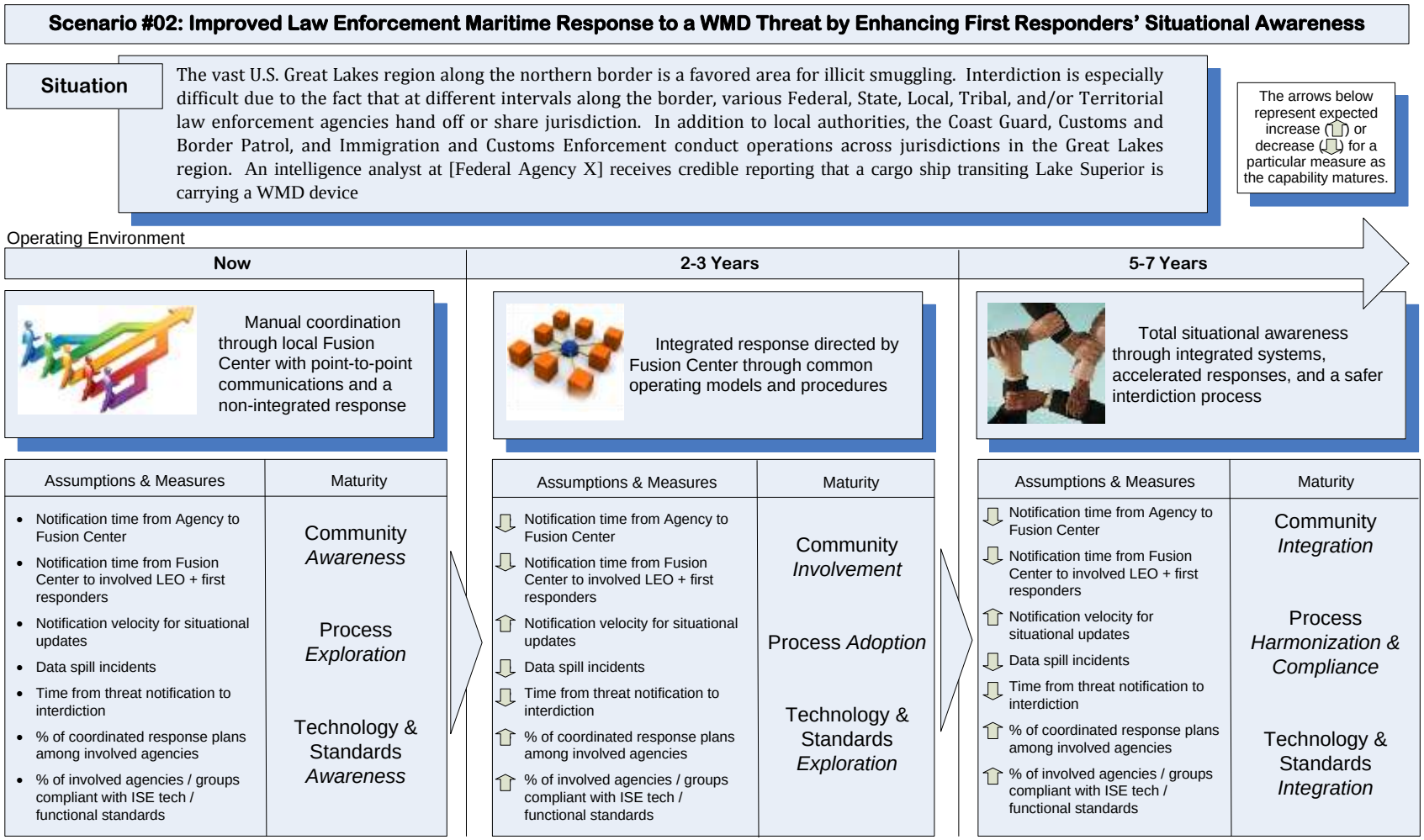


Figure 68. ISE Performance Scenario #02

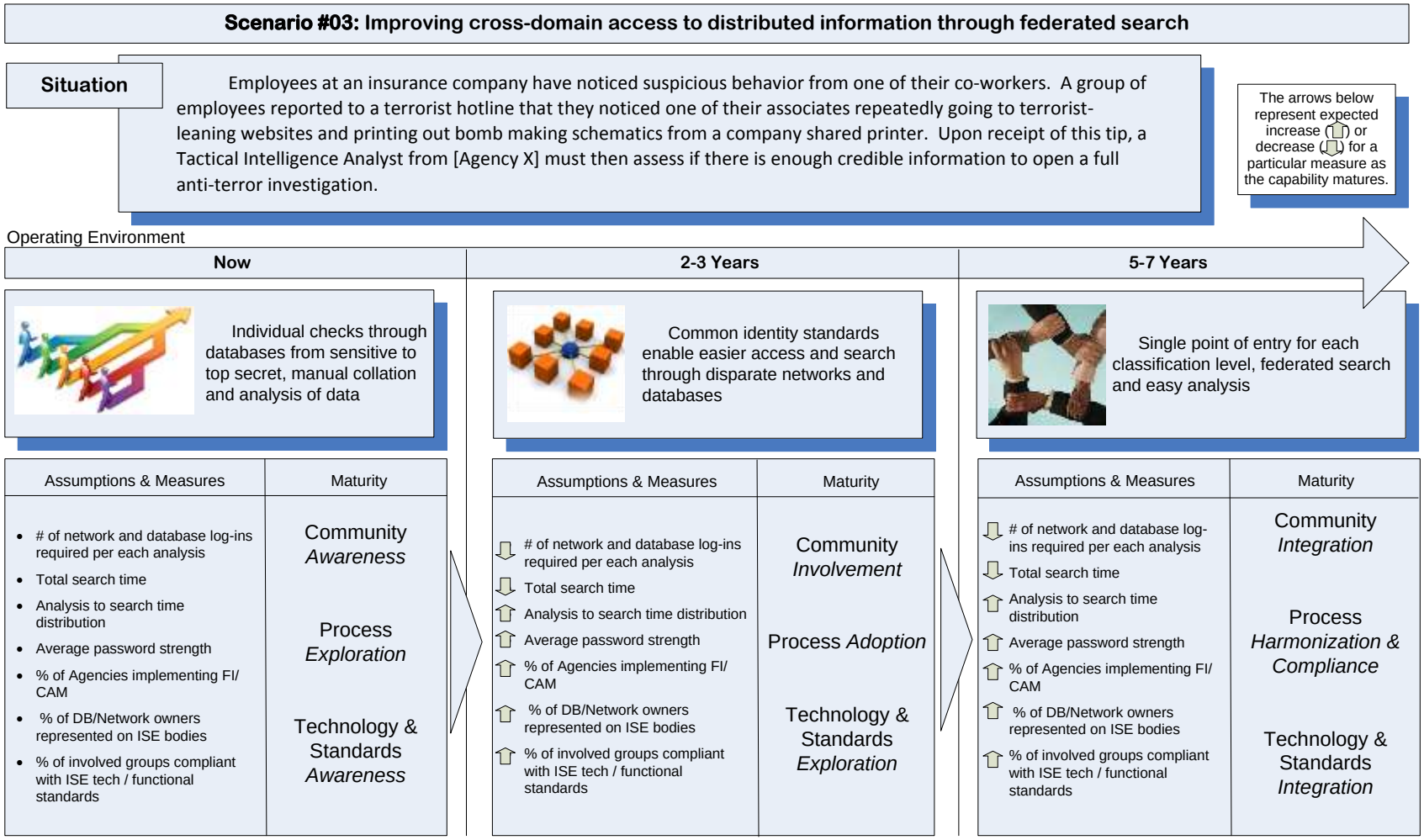


Figure 69. ISE Performance Scenario #03

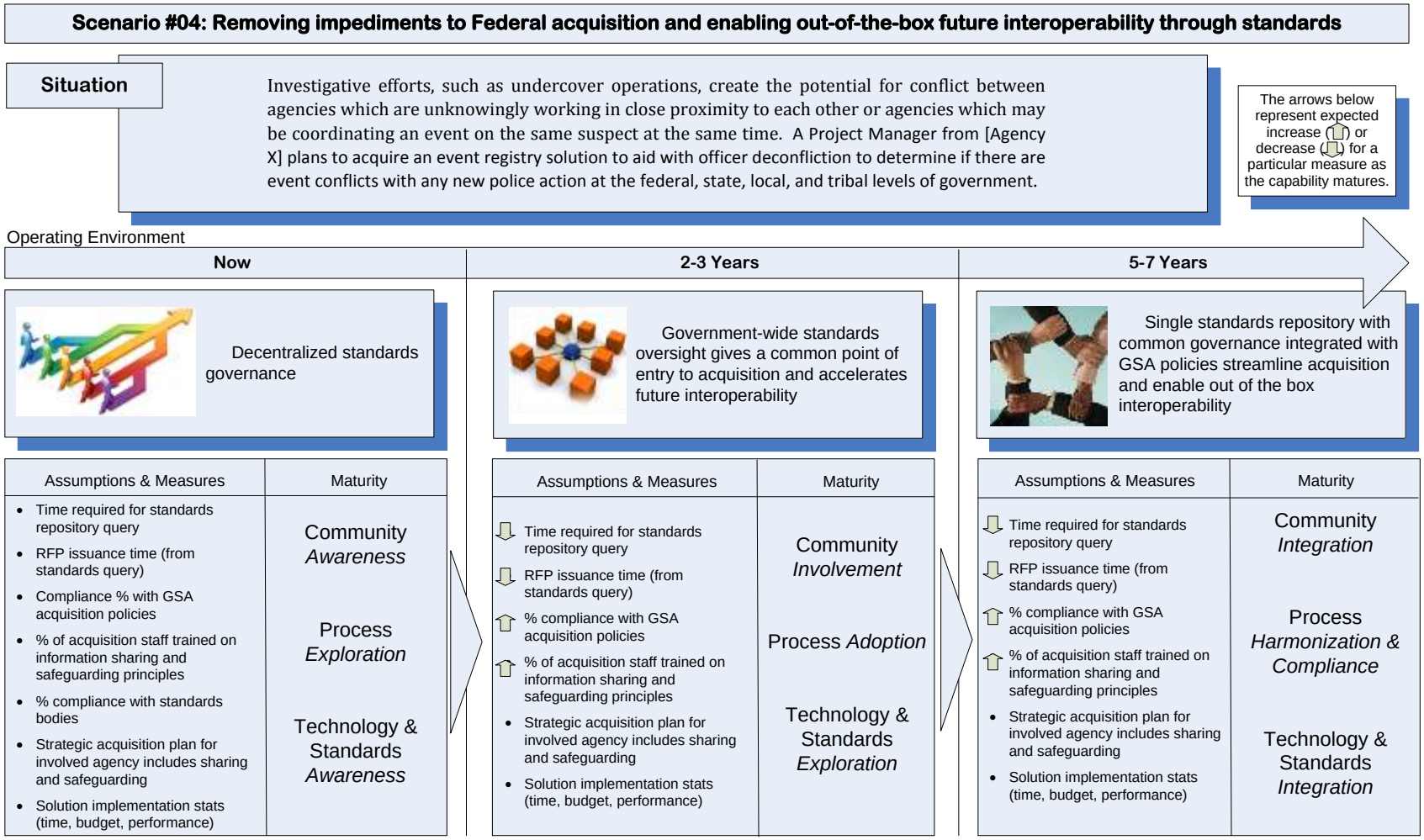


Figure 70. ISE Performance Scenario #04

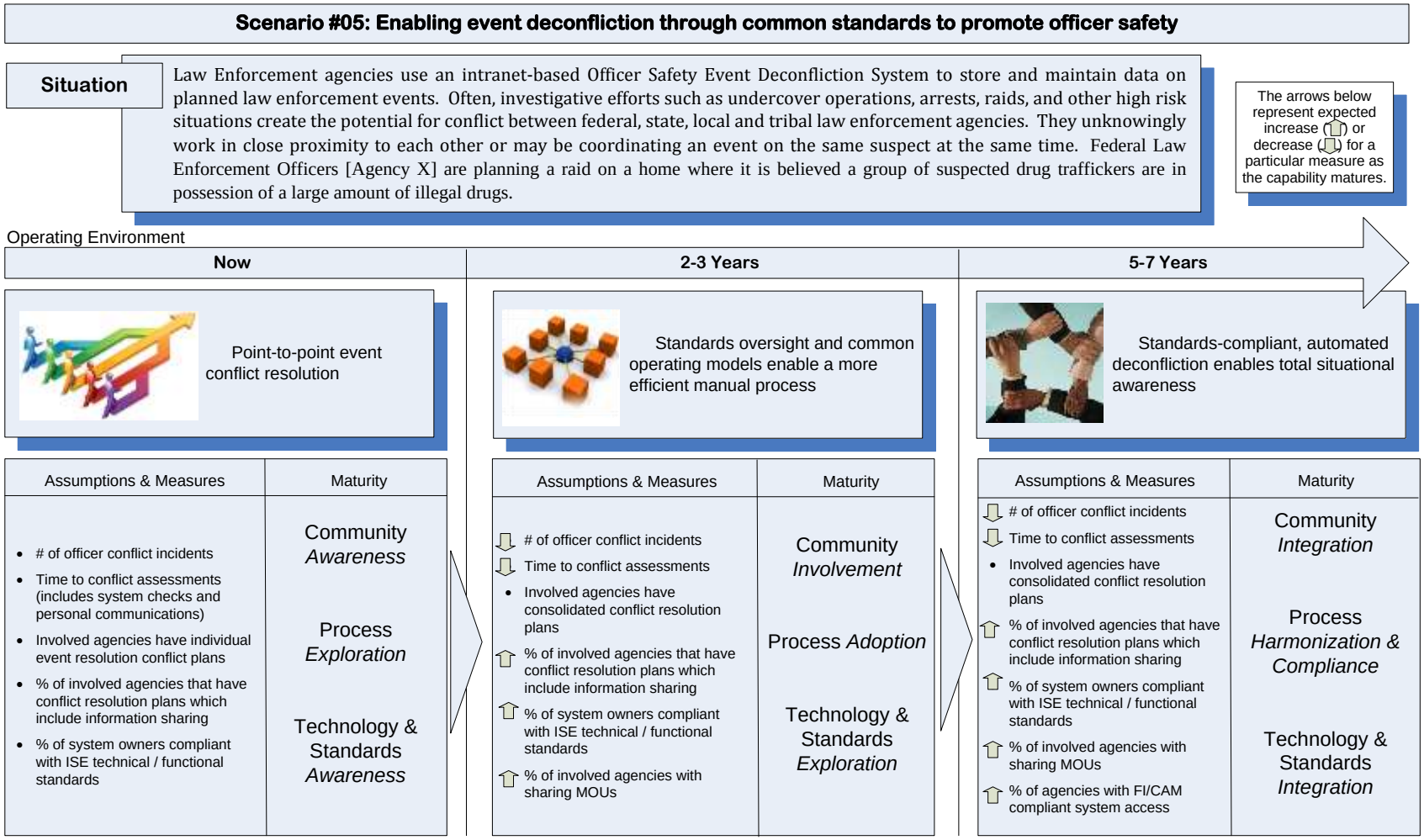


Figure 71. ISE Performance Scenario #05

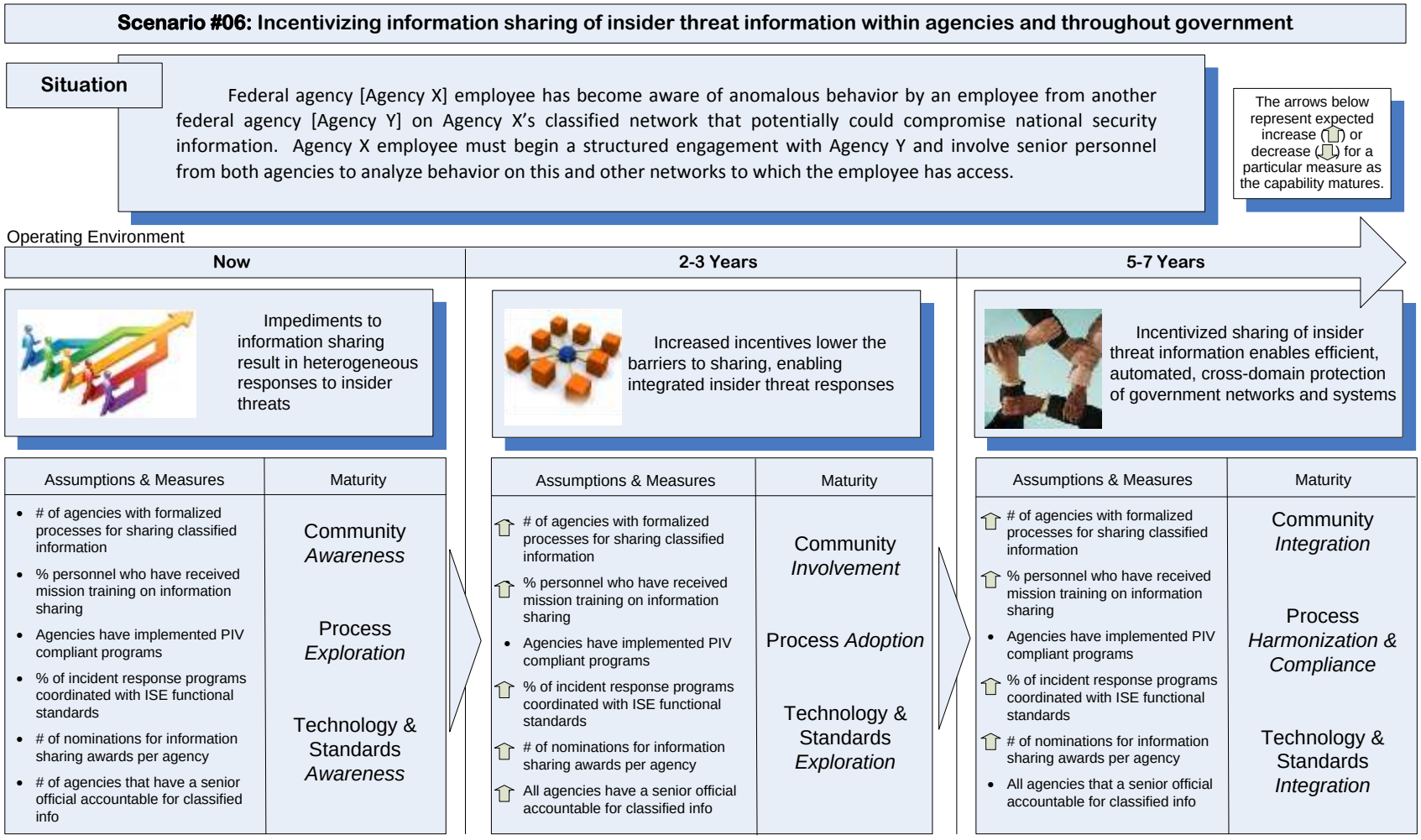


Figure 72. ISE Performance Scenario #06

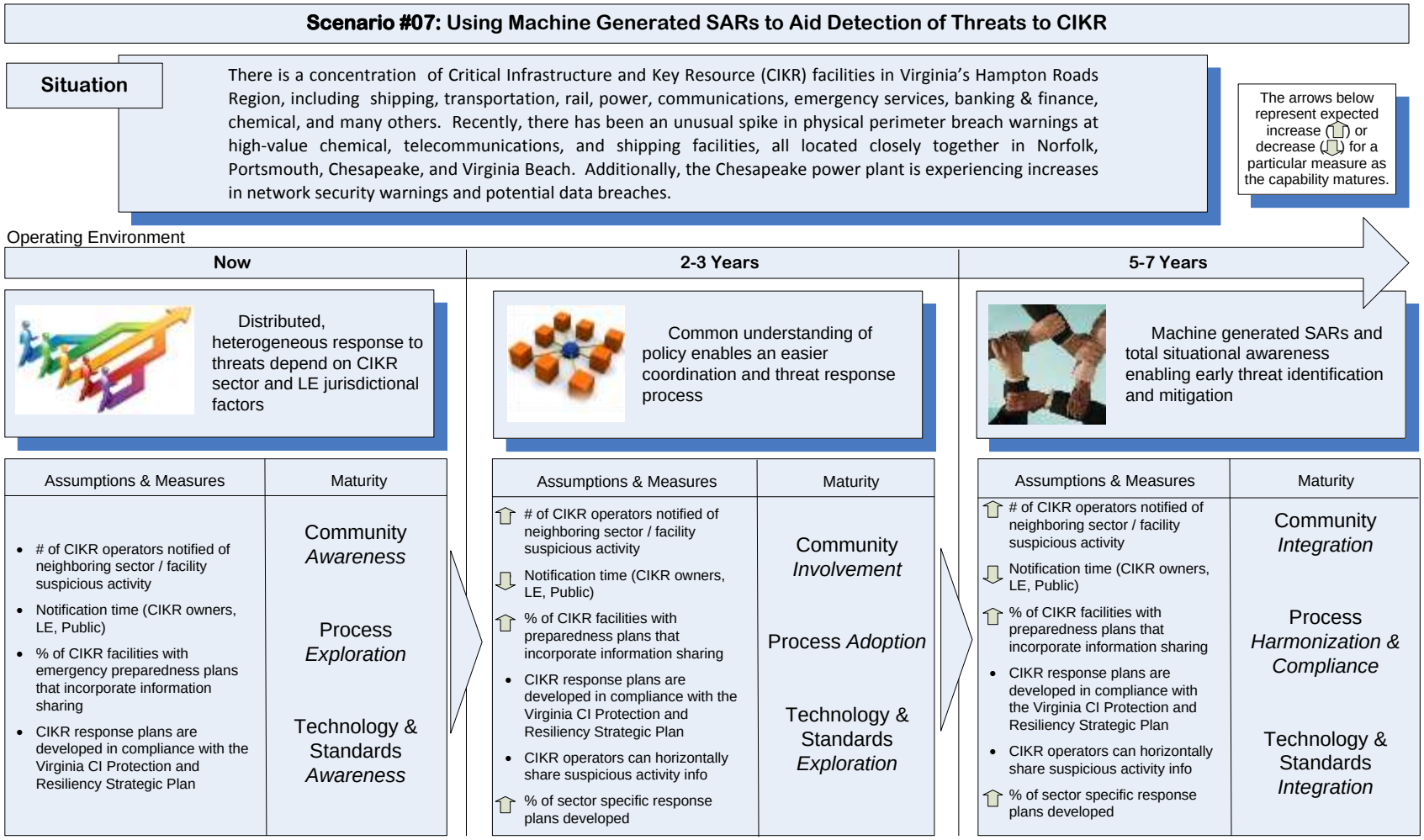


Figure 73. ISE Performance Scenario #07

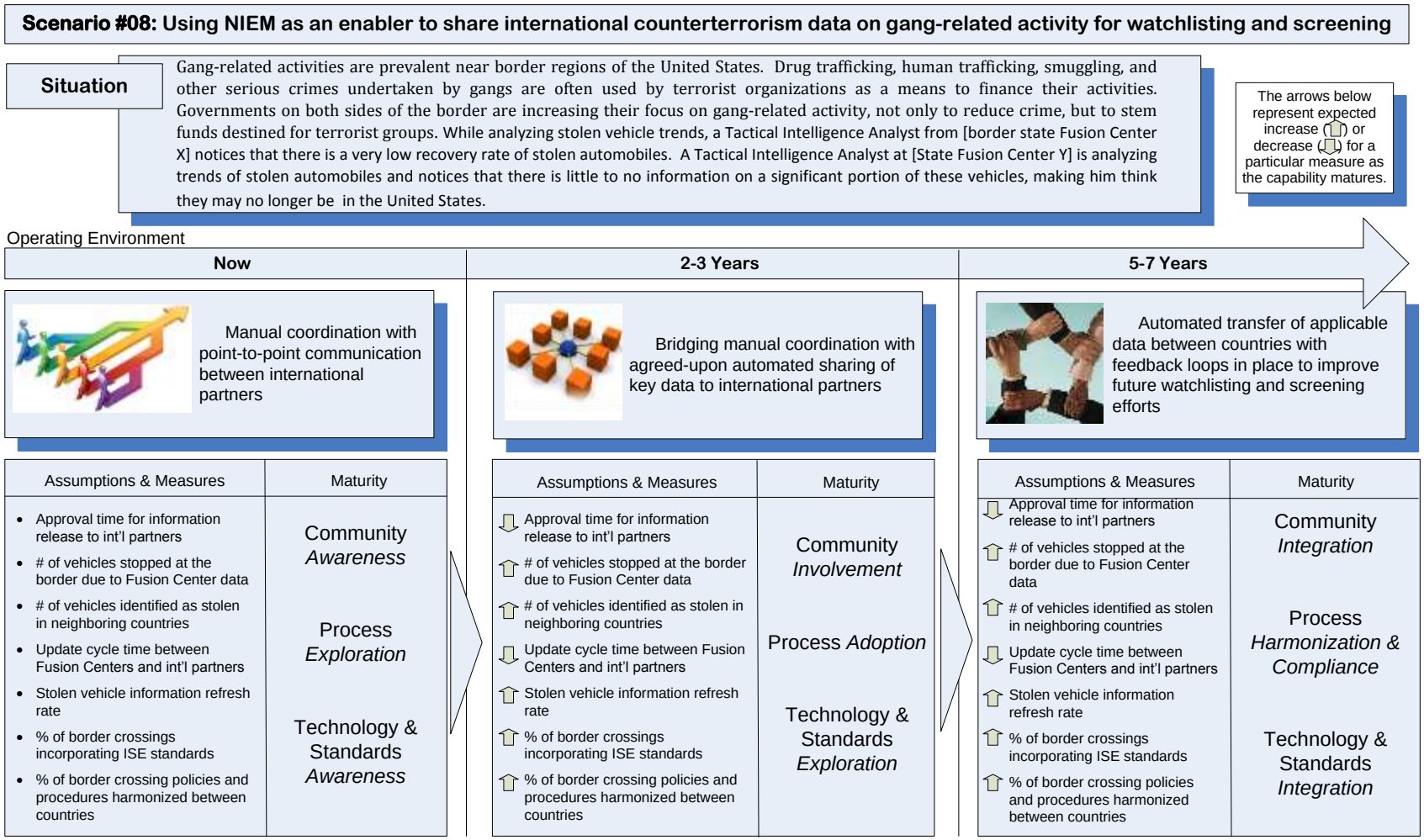


Figure 74. ISE Performance Scenario #08

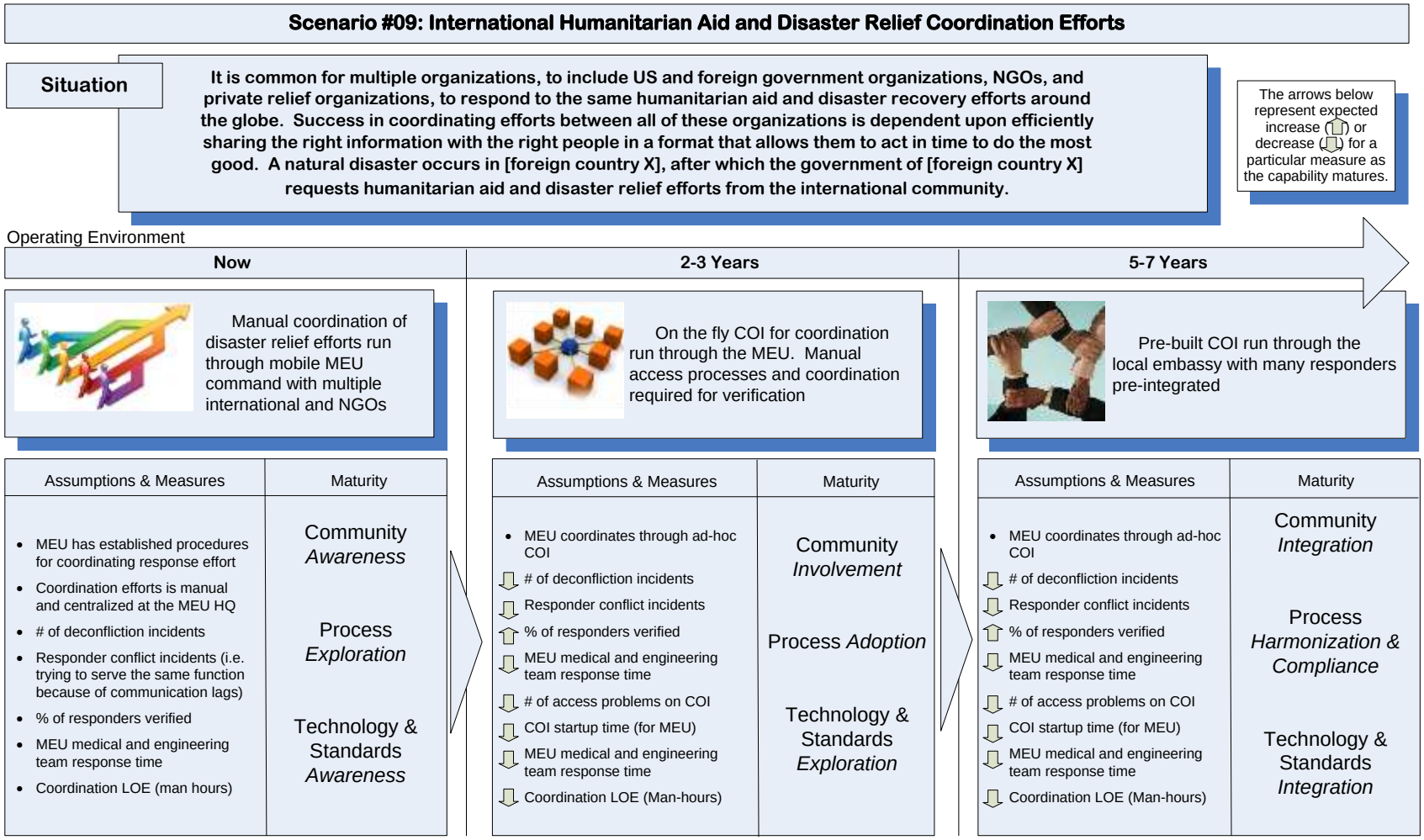


Figure 75. ISE Performance Scenario #09

Figure 76. ISE Performance Scenario #10

APPENDIX C – ISE INVESTMENTS

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 Exhibit 53 reporting is only one step of many used to understand the ISE priority area costs of mission partners.[84] Overall, the data revealed that approximately 14 percent of the Federal Government IT spending is aligned to one or more of the ISE priorities.

As reported by agencies, Figure 76 depicts the percentage of their agency's IT budget that is aligned with at least one of the ISE priority areas. Agencies are increasingly identifying resources dedicated to collaborative efforts.

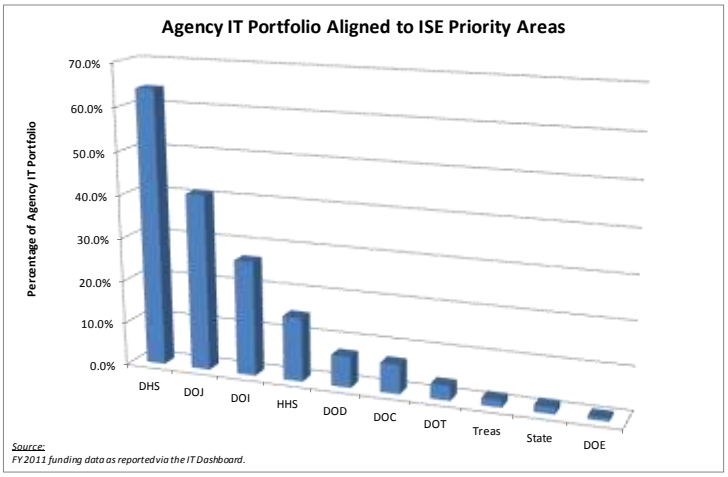


Figure 76. Agency IT Portfolios Aligned to ISE Priority Areas

This graphic illustrates that several agencies—e.g. 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. Compared to last year, DHS and DoJ show the largest increases of 15% and 2 %, respectively (see Figure 77). Fluctuations in other agencies from last year, specifically DoS and DOI are a result of improved reporting.

[84] IRTPA requires PM-ISE to provide an accounting on how much was spent on the ISE in the preceding year.

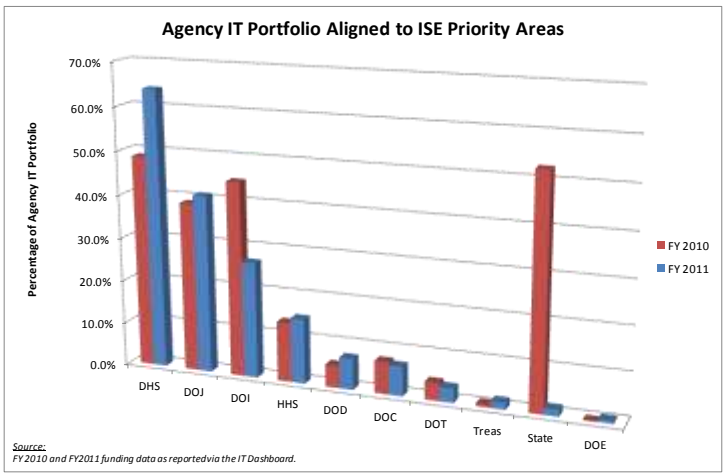


Figure 77. Agency IT Portfolios Aligned to ISE Priority Areas (year over year analysis)

The ISE priority area of SBU/CUI Interoperability accounted for the vast majority of IT spending alignment. This is expected, as investments in this ISE priority area tends to encapsulate larger, agency-wide IT initiatives. More detailed analysis through the Information Sharing and Access Interagency Policy Committee (ISA IPC) sub-committees and working groups 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.

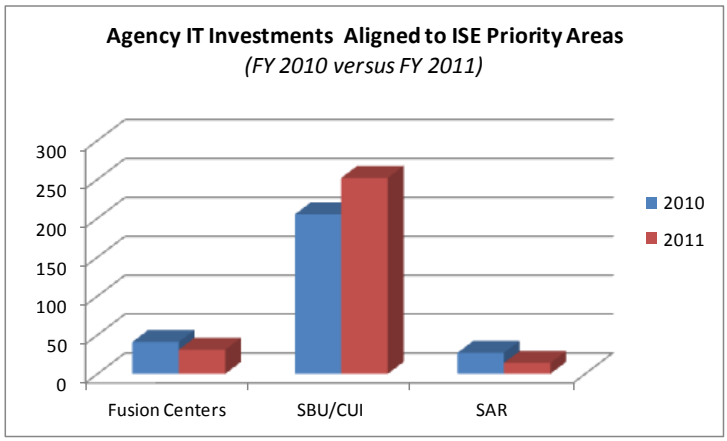


Figure 78. Agency IT Investments Aligned to ISE Priority Areas

Based on agency reporting via the OMB Exhibit 53, depicted in Figure 79, more than three quarters 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.

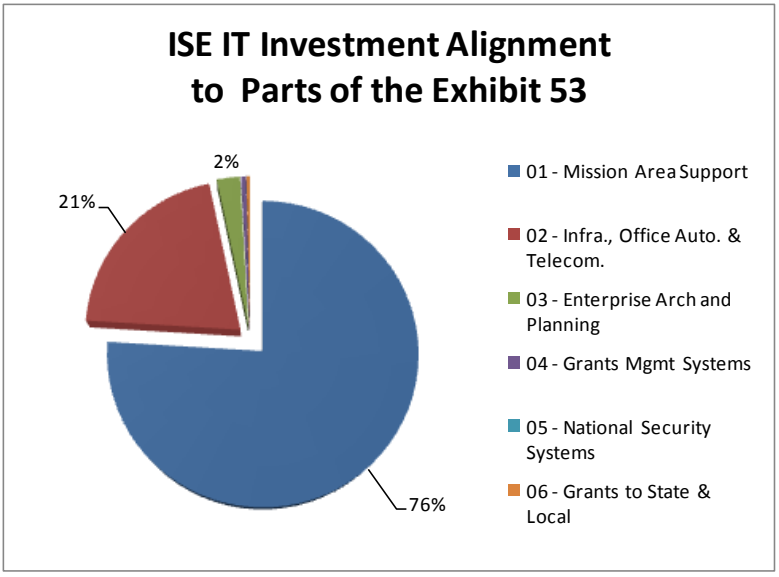


Figure 79. ISE IT Investment Alignment to Parts of the Exhibit 53

The Exhibit 53 reporting allowed analysis of federal agency IT spending aligned to the ISE priority areas focused 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 Infrastructure Maintenance LOB (38 percent), as depicted in Figure 80 below.

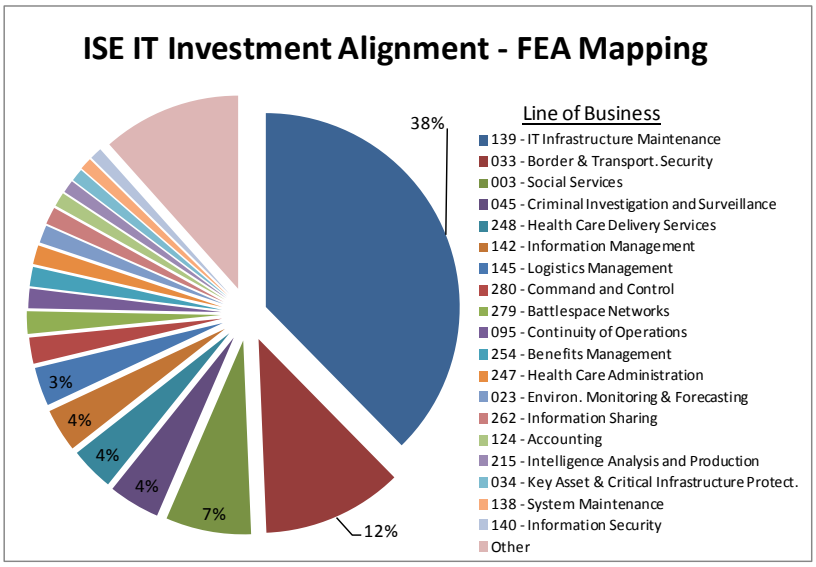


Figure 80. ISE IT Investment Alignment – FEA Mapping

IT infrastructure is broad; it captures the coordination of information and technology resources and systems to support or provide a service. However, the analysis also revealed significant primary mapping to other mission LOBs such as Border & Transportation Security (12 percent), Social Services (7 percent), Criminal Investigation and Surveillance (4 percent), Health Care Delivery Services (4 percent) , demonstrating a focus of these investments

toward advancing agency mission areas consistent with their position in the Mission Area Support portion of the Exhibit 53. Further analysis and improved data quality in future reporting will help to identify potential opportunities for investment decisions in these areas.

Continued collection of this data year-after-year will allow for trend analysis of programmatic efficiencies to better understand and account for ISE spending. 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 SBU/CUI, standards, data aggregation, case and event deconfliction 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.

APPENDIX D – ACRONYMS

ACT-IAC	American Council for Technology - Industry Advisory Council
ADIS	Arrival Departure Information System
AKIAC	Alaska Information and Analysis Center
ARJIS	Automated Regional Justice Information System
ASNI	Assured Secret Network Interoperability
AWN	Alerts, Warnings, and Notifications
BAE	Backend Attribute Exchange
BCOT	Building Communities of Trust
BJA	Bureau of Justice Assistance (DoJ)
CAC	Common Access Card
CBP	U.S. Customs and Border Protection (DHS)
CBSA	Canadian Border Security Agency
CIA	Central Intelligence Agency
CIAC	Colorado Information Analysis Center
CICC	Criminal Intelligence Coordinating Council
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CISS	Common Information Sharing Standards
CISSO	Classified Information Sharing and Safeguarding Office (PM-ISE)
CJIS	Criminal Justice Information Services (FBI)
CNCI	Comprehensive National Cybersecurity Initiative
CNSS	Committee on National Security Systems
COC	Critical Operational Capabilities
COI	Community of Interest
CONOPS	Concept of Operations
COP	Common Operating Picture
COTS	Commercial Off-The-Shelf
CSAM	Cyber Security Assessment and Management
CT	Counterterrorism
CTDL	Counterterrorism Data Layer
CUI	Controlled Unclassified Information
CVE	Countering Violent Extremism
DAWG	Data Aggregation Working Group
DEA	Drug Enforcement Administration (DoJ)
DHE	Domestic Highway Enforcement
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DICE	DEA Internet Connectivity Endeavor

DIIV	Data Integrity Identification Validation
DIVS	Data Integration and Visualization System
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
DPICS2	DHS Pattern and Information Collaboration Sharing System
DSAC	Domestic Security Alliance Council (FBI)
DSI MG	DHS SAR Initiative – Management Group
EA	Enterprise Architecture or Executive Agent
EAIR	Enterprise Architecture Information Repository
EC	Enabling Capabilities
EDM	Enterprise Data Management
EDS	Enterprise Directory Service
EDXL	Emergency Data Exchange Language
EIAS	Enterprise Identity Attribute Services
ELP	Electronic Learning Portal
EO	Executive Order
EPOC	European Pool against Organised Crime
EUROJUST	European Union's Judicial Cooperation Unit
FAQ	Frequently Asked Questions
FBI	Federal Bureau of Investigation
FBINet	Federal Bureau of Investigation Secret Domain Network
FCAP	Fusion Center Assessment Program
FEA BRM	Federal Enterprise Architecture Business Reference Model
FICAM	Federal Identity, Credential, and Access Management
FIG	Field Intelligence Groups
FISTT	Federated Identity Standards Tiger Team
FLETC	Federal Law Enforcement Training Center (DHS)
FLO	Fusion Liaison Officer
FPPS	Federal Personnel and Payroll System
FSLT	Federal, State, Local, and Tribal
FTTTF	Foreign Terrorist Tracking Task Force (FBI)
FY	Fiscal Year
GAC	Global Advisory Committee
GAO	Government Accountability Office
GBI	Georgia Bureau of Investigation

GFIPM	Global Federated Identity and Privilege Management
GISAC	Georgia Information Sharing & Analysis Center
GJXDM	Global Justice XML Data Model
Global	Global Justice Information Sharing Initiative
GML	Geospatial Markup Language
GNDA	Global Nuclear Detection Architecture
GPS	Global Positioning System
GRA	Global Reference Architecture
GSA	General Services Administration
HHS	Department of Health and Human Services
HIDTA	High Intensity Drug Trafficking Area
HRA	Human Resources Administration
HS SLIC	Homeland Security State and Local Intelligence Community of Interest
HSDN	Homeland Security Data Network (DHS)
HSIN	Homeland Security Information Network (DHS)
HSIN-CS	Homeland Security Information Networks-Critical Sectors
HSPD	Homeland Security Presidential Directive
I&A	Office of Intelligence and Analysis (DHS)
IACP	International Association of Chiefs of Police
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
ICAM SC	Identity Credential and Access Management Subcommittee
ICD	Intelligence Community Directive
IdAM	Identity and Access Management
IDEx	Indiana Data Exchange
IEC	International Electrochemical Commission
IEPD	Information Exchange Package Description
IISC	Information Integration Subcommittee
IJIS	Integrated Justice Information System
IJP	Integrated Criminal Justice Portal
IMARS	Incident Management, Analysis, and Reporting System
INTERPOL	International Criminal Police Organization
IPC	Interagency Policy Committee
IPT	Integrated Project Team
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA	Interconnection Security Agreement
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISAC	Information Sharing and Analysis Centers
ISC	Information Sharing Council or Investigative Support Center
ISE	Information Sharing Environment or Information Sharing Executive (ODNI)
ISE PAQ	Information Sharing Environment Performance Assessment Questionnaire
ISGB	Information Sharing Governance Board (DHS)

ISO	International Organization of Standardization
ISSA	Information Sharing and Safeguarding Architecture
ISRMC	Information Sharing and Risk Management Council (DHS)
ISSGB	Information Sharing and Safeguarding Governance Board (DHS)
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
JAB	Joint Authorization Board
JISSA	Justice Information Sharing Segment Architecture
JTTF	Joint Terrorism Task Force
KISSI	Key Information Sharing and Safeguarding Indicators
KST	Known or Suspected Terrorist
LEGAT	Legal Attaché
LEISI	Law Enforcement Information Sharing Initiative
LEO	Law Enforcement Online (FBI)
LEO-EP	Law Enforcement Online-Enterprise Portal
LES	Law Enforcement Sensitive
LEXS	Logical Entity Exchange Specification
LInX	Law Enforcement Information Exchange
LOB	Lines of Business
MDA	Model Driven Architecture
MI2	Maritime Identity Intelligence
MOU	Memorandum of Understanding
MSSIS	Maritime Safety and Security Information System
N-DEx	Law Enforcement National Data Exchange (FBI)
NAD	North American Day
NARA	National Archives and Records Administration
NASCO	National Association of Security Companies
NCTC	National Counterterrorism Center (ODNI)
NFCA	National Fusion Center Association
NGI	Next Generation Identification
NIAC	National Infrastructure Advisory Council
NICA	National Intelligence Community Awards
NIEF	National Information Exchange Federation
NIEM	National Information Exchange Model
NIEM-M	National Information Exchange Model-Maritime
NIST	National Institute for Standards and Technology
NJTTF	National Joint Terrorism Task Force
Nlets	The International Justice and Public Safety Network
NMIO	National Maritime Intelligence-Integration Office
NPPD	Directorate for National Protection and Programs (DHS)
NSA	National Sheriff's Association or National Security Agency
NSI	Nationwide Suspicious Activity Reporting (SAR) Initiative

NSS	National Security Staff
NTAC	Nevada Threat Analysis Center
NVPS	National Virtual Pointer System
OASIS	Organization for the Advancement of Structured Information Systems
ODNI	Office of the Director of National Intelligence
OGC	Open Geospatial Consortium
OJP	Office of Justice Programs
OMB	Office of Management and Budget
OMG	Object Management Group
ONDCP	Office of National Drug Control Policy
OPM	Office of Personnel Management
OSPIE	Office of Security Policy and Industrial Engagement (DHS)
PAC	Provisioning and Access Control System
P/CL	Privacy and Civil Liberties
P/CR/CL	Privacy, Civil Rights, and Civil Liberties
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Interoperable
PKI	Public Key Infrastructure
PM-ISE	Program Manager, Information Sharing Environment
PMO	Program Management Office
PMP	Prescription Monitoring Program
PNR	Passenger Name Record
RAC	Resource Allocation Criteria
RCR	Roll Call Release
RFI	Request for Information
RFP	Request for Proposal
RIDE	Records and Information from DMVs for E-Verify
RISC	Repository for Individuals of Special Concern
RISS	Regional Information Sharing System
RISSNET	Regional Information Sharing System Network
ROIC	Regional Information and Operations Center (New Jersey)
SAR	Suspicious Activity Report(ing)
SCC	Standards Coordinating Council
SBU	Sensitive But Unclassified
SDO	Standards Development Organization
SIEM	Security Information and Event Management
SILO	Single Integrated Look Out
SIMAS	Security Incident Management and Analysis System
SIPRNet	Secret Internet Protocol Router Network
SISSC	Senior Information Sharing and Safeguarding-Steering Committee
SLIC	State and Local Intelligence Community of Interest

SLPO	State and Local Program Office
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
SOP	Standard Operating Procedures
SP	Service or Special Publication
SSC	Shared Services Center
SSO	Simplified Sign On
SSP	Service Specification Profile
STTAC	California State Terrorism Threat Assessment Center
SWG	Standards Working Group
TLO	Terrorism Liaison Officer
TIDE	Terrorist Identities Datamart Environment
TOD	Tips of the Day
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TSS	Terrorist Screening System
TWL	Terrorism Watchlist
UCore	Universal Core
UML	Unified Modeling Language
USAO	U.S. Attorney's Office
USCG	U.S. Coast Guard (DHS)
USCIS	U.S. Citizenship and Immigration Services (DHS)
USD(I)	Under Secretary of Defense for Intelligence (DoD)
USIA	Under Secretary for Intelligence and Analysis (DHS)
VBC	Virtual Biosecurity Center
VFC	Virginia Fusion Center
WIS3	Workshop for Information Sharing & Safeguarding Standards
WSFC	Washington State Fusion Center
WMD	Weapons of Mass Destruction
XML	Extensible Markup Language


fusion
mission
securi
standards
government
state
Department
across
Agency
Technology
policies
privacy
interoperability
infrastructure
areas
guidance
Office
effort
law
NIEM
Services
Maritime
Criminal
key
ISE.

Program Manager, Information Sharing Environment
Washington, D.C. 20511

202.331.2490

www.ise.gov

@shareandprotect

fb.me/informationsharingenvironment

http://lnkd.in/zaCB97

youtube.com/shareandprotect

ise.gov/blog

ise.gov/email