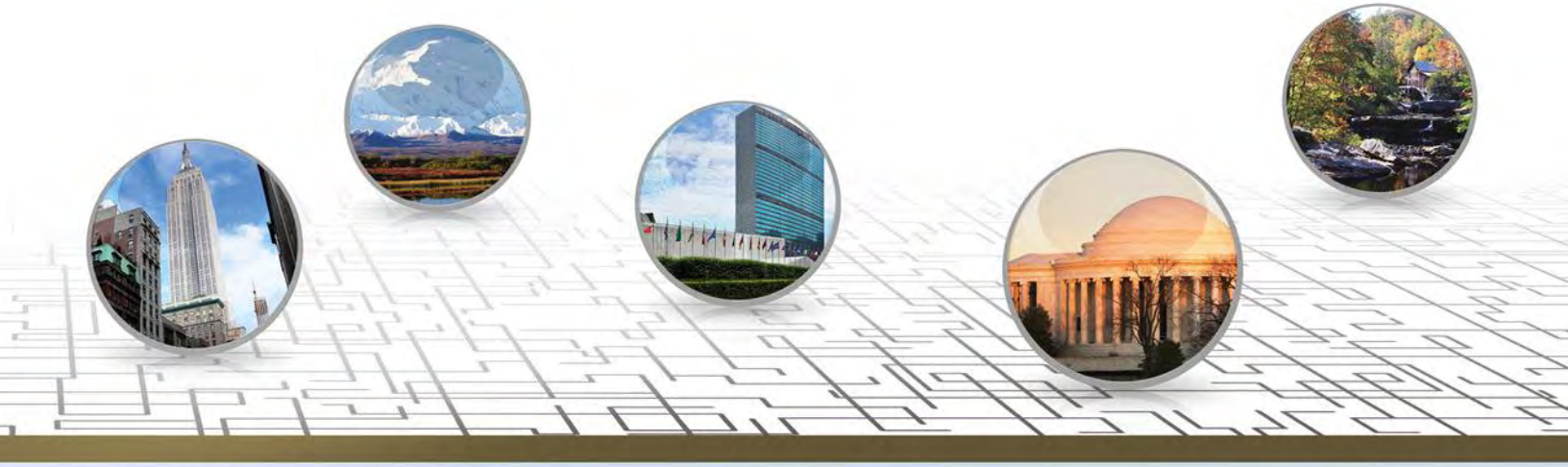


INFORMATION SHARING ENVIRONMENT

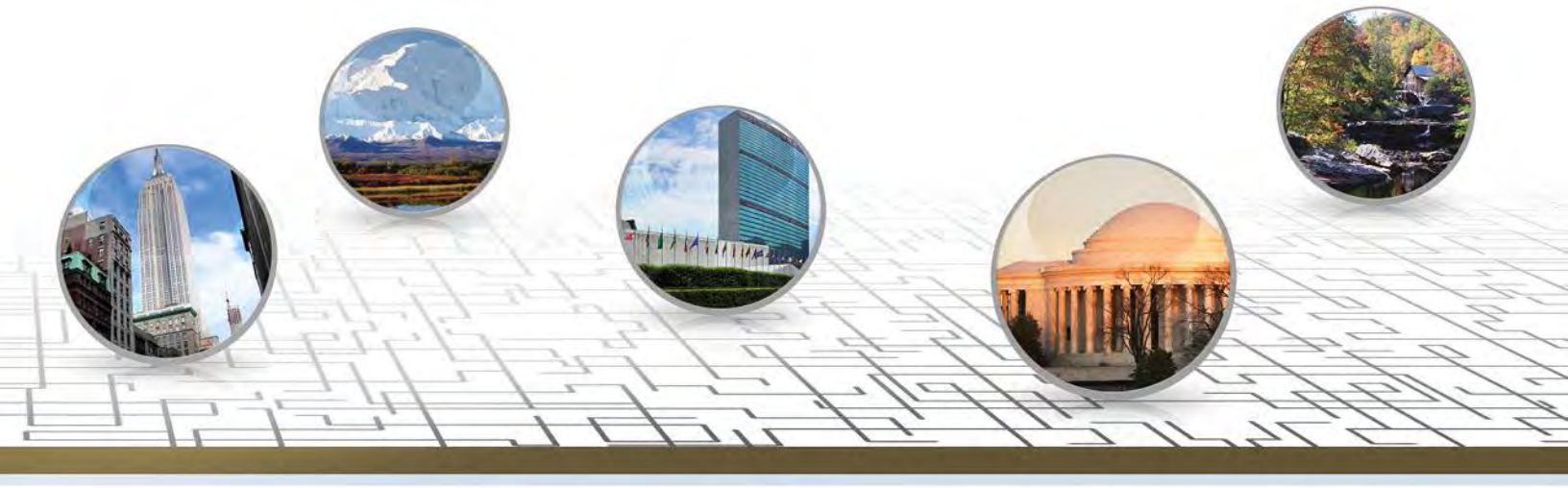
ANNUAL REPORT TO THE CONGRESS

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

Prepared by the

Program Manager, Information Sharing Environment

30 June 2013



INFORMATION SHARING ENVIRONMENT

ANNUAL REPORT TO THE CONGRESS

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

Prepared by the

Program Manager, Information Sharing Environment

30 June 2013

This page intentionally left blank.

FOREWORD

In April, when terrorists detonated two bombs at the Boston Marathon, we were all reminded of what is never far from our minds—the persistent threat of terrorism that our nation is facing. When, a couple of months later, our nation's security was compromised because an insider disclosed classified information to the news media, we were also reminded of the importance of strengthening information sharing and safeguarding in tandem.

In the National Strategy for Information Sharing and Safeguarding (National Strategy), released in December 2012, the President succinctly sets the context for our responsible information sharing challenge:

> Since the September 11, 2001 terrorist attacks, we have seen great improvement in information sharing. Today, our analysts, investigators, and public safety professionals are sharing more information and cooperating more effectively than ever before. Unfortunately, we also have had instances when critical information was not shared quickly or widely enough, or when unauthorized disclosures of classified and sensitive information damaged our national security.
>
> This National Strategy for Information Sharing and Safeguarding aims to strike the proper balance between sharing information with those who need it to keep our country safe and safeguarding it from those who would do us harm. While these two priorities—sharing and safeguarding—are often seen as mutually exclusive, in reality they are mutually reinforcing.

This report, submitted to the Congress on behalf of the President, provides a transparent assessment of the progress and performance of the departments and agencies charged with responsibly sharing information, offering accountability to those who own and operate the Information Sharing Environment. In this report we highlight progress toward the goals and vision of the National Strategy. We end the report with the Way Forward, describing our government-wide processes and plans for the coming year.

Our role, as the national office for responsible information sharing, is to plan for, coordinate the development of, and monitor progress towards development of the distributed and decentralized Information Sharing Environment (ISE) across our federal, state, local, tribal, territorial, private sector, and international partners. We exercise these responsibilities via our three part mission.

ADVANCE RESPONSIBLE INFORMATION SHARING TO FURTHER COUNTERTERRORISM AND HOMELAND SECURITY MISSIONS

Since 2001, we have made significant progress toward effectively sharing information with the right people, at the right time, and in the right way. After the Boston Marathon bombing, law enforcement officials, while recognizing and developing opportunities for improvement, highlighted the effectiveness of post-9/11 innovations like the National Network of Fusion Centers, Joint Terrorism Task Forces, and interoperable systems that allow analysts and investigators to gain access to relevant information in a way that maintains privacy protections, while promoting a culture of information sharing.

We are continuing to work on transforming our domestic information sharing architecture to realize greater efficiencies, to strengthen alignment across various information sharing initiatives, and to better identify, respond to, and prevent terrorist acts and other priority threats. We are exploring opportunities to leverage our nation's investments in counterterrorism and homeland security information sharing to accelerate progress with responsible cybersecurity information sharing.

IMPROVE DECISIONMAKING BY TRANSFORMING INFORMATION OWNERSHIP TO STEWARDSHIP WITH ISE STAKEHOLDERS

The publication of the National Strategy was one of the key milestones achieved this year; it focuses on treating information as a national asset that is valued and responsibly shared within existing laws and policies. Further, the National Strategy reminds us of the central role information plays in decisionmaking across levels and sectors of government.

This year we continued to press for greater interoperability through common standards, and for improving identity access and management capabilities across all stakeholders. We also understand the importance of protecting privacy, civil rights, and civil liberties, and are continuing to pursue automated multi-lateral agreements that will build protections and facilitate automation at each level of the information lifecycle.

We are partnering and collaborating with the information technology industry and standards development organizations to support broad adoption of ISE interoperability frameworks, based on existing standards. In addition, we support increasing use of standards-based acquisition as the way to achieve efficiencies and deploy effective support for responsible information sharing.

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

The 9/11 Commission Report addressed the need to change culture in order to improve information sharing. Our work since then is now reinforced by the National Strategy and builds on the recommendations of the 9/11 Report, placing emphasis on an important clarification: that sharing and safeguarding information are two sides of the same coin. Improvements in safeguarding information—through controls over access and discovery, while considering both security and privacy requirements—engender trust and legitimacy, and enable policy-compliant information sharing.

Effective governance regimes link internal agency, program management, and community decisionmaking efforts, rather than having after-the-fact advocacy for established positions. These regimes bring together the dual goals of sharing and safeguarding information—and encourage shared risk management. We continue to clarify the requirements and strengthen the frameworks needed to promote and conduct effective governance across our stakeholder communities.

In 2013 terrorism-related information sharing remained on the Government Accountability Office's (GAO) High Risk List. Along with our agency partners, we have made substantial progress integrating GAO's recommendations and are committed to solving the remaining challenges. Our partners are using the office of the PM-ISE as a platform from which to expand government-wide best practices to both broaden and institutionalize responsible information sharing.

In conclusion, as stated in the National Strategy:

> As President, I have no greater responsibility than ensuring the safety and security of the United States and the American people. Meeting this responsibility requires the closest possible cooperation among our intelligence, military, diplomatic, homeland security, law enforcement, and public health communities, as well as with our partners at the State and local level and in the private sector. This cooperation, in turn, demands the timely and effective sharing of intelligence and information about threats to our Nation with those who need it, from the President to the police officer in the street.
>
> PRESIDENT BARACK OBAMA

National security through responsible information sharing—our vision—is an increasing reality each and every day. We will continue to mature the ISE, using the National Strategy as our guiding framework, to support and further strengthen our mission partners in their efforts to keep Americans safe.

Kshemendra Paul
Program Manager, Information Sharing Environment

CONTENTS

EXECUTIVE SUMMARY XI

BOSTON – PATRIOTS' DAY 2013 XVII

INTRODUCTION 1
- Scope 2
- Meeting the Legal Requirements for ISE Performance Management Reports 2
- Primary Sources 3

SECTION 1: COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY 5
- Law Enforcement and Homeland Security Information Sharing 7
  - Joint Terrorism Task Forces (JTTFs) 7
  - National Network of Fusion Centers 8
  - Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) 12
  - Joint Counterterrorism Assessment Team 17
  - Domestic Information Sharing Environments 18
  - Tribal Law Enforcement Information Sharing 21
  - Combating Human Trafficking 22
  - Joint CT Coordination Cell (JC3) 23
  - FBI Next Generation Identification System (NGI) 23
  - FBI Sentinel 25
  - Standardizing Requests for Information 25
  - DHS Analytical Framework for Intelligence 25
- Aligning International Identity Frameworks 26
  - Preventing and Combating Serious Crime (PCSC) 26
  - North American Day (NAD) Pilot Programs 26
- Private-Sector Information Sharing 28
  - Addressing the 2012 NIAC Report Findings 28
  - Homeland Infrastructure Threat and Risk Analysis Center 31
  - Addressing Economic and National Security Challenges 33
  - All Hazards Consortium 36
- Multimodal Information Sharing 37
  - National Maritime Domain Awareness Architecture Plan Implementation 37
  - DHS Coastal Surveillance System 38
  - Air Domain Intelligence Integration Element (ADIIE) 38
  - Air Domain Awareness Portal 39
  - Air Event Information Sharing Service 39
- Securing the U.S. Food Supply at Ports of Entry 40
- The DHS Joint Analysis Center Collaborative Information System (JACCIS) 40

INTERLUDE: FUSION CENTERS IN ACTION 41

SECTION 2: INFORMATION DISCOVERY AND ACCESS THROUGH COMMON STANDARDS 45
Standards Governance 47
ISA IPC Standards Working Group, and the Standards Coordinating Council 47
Standards Implementation 48
National Information Exchange Model (NIEM) 48
Using NIEM to Share Information between the Department of Defense and the Department of Veterans Affairs 51
Standardizing Country Codes across Federal Databases 51
Open Geospatial Standards 51
Standards-based Acquisition for Information Sharing 52
Data Aggregation 54
Data Exchange Tool Kit 55
Data Aggregation Capability Updates and Success Stories 55
Data Aggregation Challenges and Next Steps 59

INTERLUDE: TESTING STANDARDS-BASED COMPLIANCE AND CONFORMANCE – IJIS SPRINGBOARD 60

SECTION 3: OPTIMIZING MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY 61
ISE Interoperability Framework (I^2F) 63
Alignment to Existing Architecture Frameworks 63
A Whole-of-Government Approach to Data Stewardship and Data Correlation 64
Geospatial Architecture Interoperability 64
Geospatial Information as a National Resource 65
Identity, Credential, and Access Management: Coordinating Identity Efforts across the Federal Government 66
Federated Identity Management 66
FICAM Maturity Model 67
Assured Sensitive-but-Unclassified (SBU) – Controlled-Unclassified Information (CUI) Interoperability ... 68
Interoperability – Incremental Progress 69
Federated Attribute Sharing on the Secret Fabric 70
Developing Interoperability, Simplified Sign-On (SSO) and Search Capabilities 71
Advancing Identity Access Management (IDdM) with the Backend Attribute Exchange (BAE) 71
Other Shared Services 72
The DHS Common Operating Picture (COP) 72
Critical Event Deconfliction 72
DHS Information Sharing Segment Architecture v 3.0 73
FBI Law Enforcement Enterprise Portal (LEEP) 74
The DOI Incident Management Analysis and Reporting System (IMARS) 74
DEA's de-confliction and Information Coordination Endeavor (DICE) tool 75

INTERLUDE: BACKEND ATTRIBUTE EXCHANGE OPERATIONAL PILOT 76

SECTION 4: STRENGTHENING SAFEGUARDING OF INFORMATION 77
Threat Environment and Vulnerabilities 79
Establishing Priorities 80
Areas of Progress 80
Remaining Gaps and Emerging Vulnerabilities 81
The Way Forward for Strengthening Safeguarding in 2013 82
Other Key Safeguarding-related Accomplishments 82
Defense 82
Privacy, Civil Rights, and Civil Liberties Protections (P/CR/CL) 85

INTERLUDE: HOMELAND SECURITY AND CRITICAL INFRASTRUCTURE 86

SECTION 5: PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES 89
Strategic Objectives and Priorities Established for the ISE 90
P/CR/CL Governance 90
Development and Implementation of ISE Privacy Policies 91
Compliance Activities 92
Critical Role of the P/CL Official 93
Training and Outreach 94
Privacy, Civil Rights and Civil Liberties – Next Steps 95

SECTION 6: MANAGING AND FOSTERING A CULTURE OF RESPONSIBLE INFORMATION SHARING 97
Improving Governance 98
The ISE Performance Framework 99
Budget-Performance Integration 100
Responsible Information Sharing Training 102
Risk Analysis Courses 102
Specialized Analytic Seminar Series 102
Cyber Analysis Training 103
SAR Analysis Course 103
National Fusion Center Analytic Workshop 103
NSI Training 104
SAR – Maritime Training 104
NIEM Biometrics Domain Training 104
Performance Incentives 105
Building Blocks of the ISE 105

THE WAY FORWARD 107
Managing Implementation of Responsible Information Sharing 108
Institutionalizing a Management Framework 108
Implementation Roadmap 110
Targeting Capabilities Not Yet Achieved 113
PM-ISE Vision, Missions, and Priorities 114
Conclusion 116

ENDNOTES 117

APPENDIX A – ISE PERFORMANCE DATA A-1

APPENDIX B – MISSION-BASED TEST SCENARIOS B-1

APPENDIX C – ISE INVESTMENTS C-1

APPENDIX D – ACRONYMS D-1

EXECUTIVE SUMMARY

ORGANIZATION

The first five sections of the 2013 report are aligned with the five goals outlined in the President's National Strategy for Information Sharing and Safeguarding (National Strategy), which was released in December 2012.

- **Collective Action through Collaboration and Accountability** – Maturing of foundational ISE mission processes, and new and emerging information sharing initiatives.
- **Information Discovery and Access through Common Standards** – Progress of ongoing efforts and new initiatives in the areas of information discovery and access. Fundamental elements of discovery and access.
- **Optimizing Mission Effectiveness through Shared Services and Interoperability** – ISE initiatives focused on sharing services and achieving interoperability across networks and security fabrics to enable efficiency, reduce duplication, and improve mission success.
- **Strengthening the Safeguarding of Information** – Key achievements in safeguarding capabilities that most directly relate to the advancement of information sharing, and specifically to the relevant characteristics of the ISE.
- **Protecting Privacy, Civil Rights, and Civil Liberties** – ISE initiatives focused on ensuring the protection of privacy, civil rights, and civil liberties (P/CR/CL) through the consistent, government-wide application of protections.

The final two sections address the ongoing implementation of the Information Sharing Environment (ISE).

- **Managing and Fostering a Culture of Responsible Information Sharing** – Progress on oversight and management functions that support information sharing and safeguarding.

- **Way Forward** – A discussion of the Program Manager, Information Sharing Environment's (PM-ISE) management tools, performance framework, and annual planning cycle, and the implementation roadmap and actions in place to achieve ISE mission objectives.

As required by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), this Annual Report provides an assessment of progress achieved in implementing the ISE. To that end, each section provides a summary of major accomplishments made, and also points out existing gaps, ongoing challenges, and opportunities for additional improvements.

COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY

Foundational ISE mission processes—including progress made in existing information sharing procedures between the Federal Government, and state, local, tribal, territorial, private-sector, and foreign partners—continued to mature during the past year. And new and emerging information sharing activities and initiatives that promote collaboration across the ISE have taken hold in both traditional counterterrorism (CT) and homeland security missions.

Significant accomplishments during this reporting period include the Administration's release of three national-level policy directives[1] that reinforce the importance of information sharing with critical infrastructure owners and operators. The National Counterterrorism Center (NCTC), the Department of Homeland Security (DHS), and the Federal Bureau of Investigations (FBI) continued to improve interagency collaboration with the establishment of the Joint Counterterrorism Assessment Team (JCAT), which replaced the Interagency Threat Assessment and Coordination Group (ITACG). Also, the International Association of Chiefs of Police (IACP) and the office of the PM-ISE began work on sponsoring a Unified Message Task Team (UMTT) to enhance Suspicious Activity Reporting (SAR) training, metrics, and policies.

Challenges and opportunities for improvement remain. In spite of the progress noted, work will continue to address the challenges to information sharing between the Federal Government and private-sector owner/operators of critical infrastructure. Also, the PM-ISE released a report in March 2013, *Improving Suspicious Activity Reporting (SAR) Analysis,* and is working with the Information Sharing and Access Interagency Policy Committee (ISA IPC) SAR Subcommittee to address the findings and recommend mitigation strategies.

As noted in last year's report, gaps in tribal information sharing continue to be a concern. PM-ISE and partners across the ISE have identified some of the causes that hinder tribal information sharing and have written a white paper making the business case for improvement with

[1] The National Strategy for Information Sharing and Safeguarding (National Strategy), Executive Order 13636, and Presidential Policy Directive 21 – see p. 30

recommendations for next steps. We are working together with agencies, state and local partners, and Tribes to develop specific plans.

The way forward includes continued focus on expanding the Nationwide SAR Initiative (NSI), as well as on adopting common-exchange processes for Requests for Information (RFIs) and for Alerts, Warnings, and Notifications (AWN).

INFORMATION DISCOVERY AND ACCESS THROUGH COMMON STANDARDS

The National Strategy distinctly defines *discovery* and *access* as two separate concepts. *Discovery* addresses a user's ability to identify the existence of information, while *access* relates to the user's ability to retrieve information. Work by ISE mission partners and the office of the PM-ISE on fundamental elements of discovery and access includes: data-level tagging; data aggregation; the development and incorporation of interoperable industry-accepted technical standards for information sharing solutions; and standards-based acquisition.

Major accomplishments toward promoting discovery and access through common standards have been noted across the Federal Government. This year DHS launched the *Enhanced Overstay Vetting and Biographic Exit Project*, which seeks to increase DHS's capability for identifying immigration violators and prioritizing enforcement. The FBI Criminal Justice Information Services (CJIS) Division expanded the capabilities of the Law Enforcement National Data Exchange (N-DEx) in order to accommodate more records and users, and began sharing its investigative reports in near real-time with its criminal justice partners via N-DEx. And the Department of Defense (DoD) took a major step forward in promoting common standards with their decision to adopt the National Information Exchange Model (NIEM) as the best option for department-wide, standards-based data exchanges.

The challenges to enterprise data correlation noted in last year's report continue to persist and to define the way ahead on the implementation roadmap. Development of a data-aggregation architecture is a priority objective of the National Strategy. Other objectives are adopting metadata standards to facilitate discovery, access, and monitoring across networks and security domains; and defining and implementing common standards to support automated discovery and access. And, while only about 50% of ISE agencies consider ISE functional and technical standards when issuing grants or Requests For Proposals (RFPs) for ISE-related systems, PM-ISE is working with the General Services Administration (GSA) to leverage National Strategy implementation actions to accelerate the use of information sharing standards in acquisition decisions.

OPTIMIZING MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY

ISE initiatives continue to focus on shared services and achieving interoperability across networks and security fabrics to enable efficiency, reduce duplication, and improve mission success. Integral to achieving interoperability is the development of an ISE Interoperability Framework that seeks to align reference architectures—like those for data aggregation and geospatial information—across the ISE. Interoperability is also realized through the adoption and implementation of standard identity and access management (IdAM) practices.

The ISA IPC's Data Aggregation Working Group (DAWG) continues to make progress in developing a reference architecture framework to assist departments and agencies in developing interagency data-sharing requirements. The GSA Federal Identity, Credential and Access Management (FICAM) Program Office is leading the implementation of the FICAM Roadmap across all security domains, which will further interoperability. And the office of the PM-ISE is coordinating an interagency effort with DHS, the Department of Interior (DOI), the National Geospatial-Intelligence Agency (NGA), and the Department of Commerce (DOC) to develop a Geospatial Interoperability Reference Architecture (GIRA) in order to foster the reuse of geospatial services, reduce their information technology (IT) investment costs, and promote information sharing.

Opportunities to optimize mission effectiveness in the way forward include the development of an ISE interoperability framework (I^2F), which the office of the PM-ISE began developing for the purpose of aligning enterprise architecture frameworks used by ISE partners to advance interoperability. Additional opportunities to improve federated identity management continue as PM-ISE and GSA develop an initial test scenario in which an ISE mission partner will use a Backend Attribute Exchange (BAE) to allow the transfer of data as users from one organization login to research cases, intelligence, or other information "owned and protected" by another organization.

Finally, many of the current federal IT budget models do not allow for flexibility, pooling, and extending the availability of funding. Support for removing limits on transferring funding across appropriations and agencies will better allow for provisioning common administrative IT services.

STRENGTHENING THE SAFEGUARDING OF INFORMATION

Protecting and sharing national security and counterterrorism-related information that is stored on—and disseminated electronically from—Federal Government information systems is of increasingly critical importance in ensuring the safety and security of the United States, and of the American people. Sharing and safeguarding information requires enforcement of the controls that are necessary in order to protect sensitive and classified information—as well as the privacy, civil rights, and civil liberties of individuals. At the same time, providing efficient access to mission-

critical information is needed in order to enable analysts, operators, and investigators to effectively perform their jobs.

In November 2012, the Administration disseminated a *Presidential Memorandum on the National Insider Threat Policy* and *Minimum Standards for Executive Branch Insider Threat Programs* in order to provide direction and guidance to help promote the development of effective insider threat programs within departments and agencies. These documents are meant to deter, detect, and prevent actions by employees who may represent a threat to national security.

During this reporting period DHS also expanded its Enhanced Cybersecurity Services (ECS) program, in accordance with Executive Order (EO) 13636 *Improving Critical Infrastructure Cybersecurity,* in order to better assist critical infrastructure owners and operators to improve protection of their systems from unauthorized access, exploitation, or data exfiltrations. DoD is also rolling out a program that will allow users of mobile device—working anywhere in the world, from remote battlefields to the Pentagon—to rapidly and securely share classified information and protected data across all components.

Recent breaches of security and disclosures of classified information highlight the vulnerabilities inherent in the protection of sensitive and classified information. Continued implementation of structural reform and standardized policies will help strengthen oversight as well as align information security best practices.

The work that began under EO 13587 Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, designed to make substantive improvements to the security of our classified networks, is ongoing. The Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) has mapped out goals for the way forward, and a plan for measuring progress with classified information sharing and safeguarding.

PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

ISE initiatives focus on ensuring the protection of privacy, civil rights, and civil liberties (P/CR/CL) through consistent, government-wide application of protections. This year, several agencies have written and adopted privacy policies that are at least as comprehensive as the ISE guidelines. Still, evolving threats and capabilities require that departments and agencies remain vigilant in including P/CR/CL protections in their decisions and that they incorporate effective ways to measure compliance with privacy policies.

The ISA IPC Privacy and Civil Liberties (P/CL) Subcommittee is developing guidelines for information sharing and safeguarding agreements that will both ensure that mission needs are met, and ensure the protection of P/CR/CL. DHS has established a formal process for conducting

compliance reviews for the implementation of DHS-wide P/CR/CL protections. And this year PM-ISE hosted its fourth roundtable outreach event with the P/CR/CL advocacy community in order to build stronger protections in operational programs, training, and guidance materials.

While there have been initiatives to measure and ensure privacy compliance, there currently is not an effective ISE-wide performance measurement for internal agency compliance, oversight, and accountability mechanisms to ensure that P/CR/CL protections are being applied consistently. The development of these measures is a priority for the ISA IPC P/CL Subcommittee.

P/CR/CL objectives in the way forward include continued focus on issuing Fusion Center, SAR, and federal P/CR/CL policy guidelines.

MANAGING AND FOSTERING A CULTURE OF RESPONSIBLE INFORMATION SHARING

Key to the implementation of the ISE are oversight and management functions that support information sharing and safeguarding—including the alignment and harmonization of governance bodies; performance management; training; and information sharing and safeguarding incentives within the ISE. The National Strategy provides a strategic vision and direction for ISE governance—a culture that values responsible information sharing to ensure mission success.

WAY FORWARD

The ISE performance framework consists of a coherent set of management processes that align policy, governance, programmatic guidance, performance, standards, technologies, and architectures. The White House's programmatic guidance, PM-ISE's implementation guidance, and the annual ISE performance assessment make up the ISE performance framework and drive an annual planning and performance measurement cycle which informs ISE agency investments in responsible information sharing initiatives. The performance framework measures progress against milestones and objectives, and is presented in the form of an Implementation Roadmap.

BOSTON – PATRIOTS' DAY 2013

Monday, April 15, 2013 – Patriots' Day. The Boston Marathon started as planned: on schedule, and with great excitement. But at 2:49 pm EDT, about two hours after the winner completed the race, two bombs were detonated on Boylston Street, just before the finish line.

Ongoing investigations will determine the extent of any information sharing gaps that may have existed prior to the bombings. Any success by terrorists is a cause for grave concern. In analyzing what happened in Boston on Patriots' Day, we can also recognize and appreciate the enhanced information sharing capabilities among federal, state, and local law enforcement, intelligence, and public safety agencies that have been mobilized since 9/11. These capabilities were in place and operational in Boston prior to the bombings.

> "The Federal Government provided invaluable assistance both in helping us prepare for and respond to this tragic event. Preparedness training provided through federal funding set a framework for multiple jurisdictions to work seamlessly with one another in a highly effective manner."[2]

For example, the Multi-Agency Coordination Center (MACC) was operational in the State's Emergency Operations Center prior to the start of the marathon. Representatives from Boston's police, fire, and emergency medical services, as well as public safety personnel from seven other cities and towns along the 26.2 mile marathon course were present in the MACC. Also included were representatives from state and federal agencies, including the FBI, DHS, the Federal Aviation Administration (FAA), and the Coast Guard.

[2] Boston Police Commissioner Edward Davis, May 9, 2013, U.S. House of Representatives, Homeland Security Committee, Hearing: Boston Bombing.

> "… what I saw in action in Massachusetts was effective leadership, true collaboration, and trusting partnerships. This gave [Boston], the surrounding area, and the country, the confidence that law enforcement was working together and using everything at their disposal to bring this incident to a swift close."[3]

In the days after the attack, Boston's designated fusion center, the Boston Regional Intelligence Center (BRIC), the Massachusetts Commonwealth Fusion Center, and fusion centers across the country tirelessly supported the Boston investigation. And the National Network of Fusion Centers supported requests for information (RFIs) to enhance the BRIC's support of the FBI's Joint Terrorism Task Force (JTTF).[4]

> "… we have seen an extraordinary effort by law enforcement, intelligence, and public safety agencies."[5]

While collaboration among federal, state, and local agencies leading up to and after the Boston bombings certainly illustrates progress in implementation of the information sharing environment since 9/11, the event also painfully reinforces our need to continue advancing the goals of the National Strategy and our responsible information sharing capabilities.

---

[3] http://theiacpblog.org/2013/04/24/one-team-one-fight-vast-improvements-in-information-sharing-and-cooperation
"One Team, One Fight: Vast Improvements in Information Sharing and Cooperation," Posted April 24, 2013, iacpblog, Bart R. Johnson, International Association of Chiefs of Police (IACP) Executive Director.

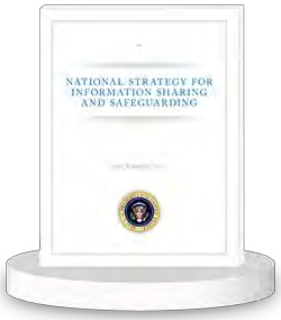
[4] http://ise.gov/blog/mike-sena/fusion-center-staff-boston-and-across-country-tirelessly-support-boston-investigation
"Fusion Center Staff in Boston and across the Country Tirelessly Support Boston Investigation", Posted April 26, 2013, Mike Sena, President of the National Fusion Center Association.Posted by Mike Sena, President of the National Fusion Center Association (NFCA), April 26, 2013.

[5] FBI Director Robert S. Mueller, April 19, 2013, statement on the arrest of the Boston bombing suspect.

INTRODUCTION

This 2013 Annual Report to Congress examines the extent to which the mandate for terrorism-related information sharing, as directed in IRTPA, is being implemented by federal departments and agencies that have stewardship over terrorism-related information; that operate systems within the Information Sharing Environment (ISE);[6] or that otherwise participate in the ISE.[7]

This Report assesses how agencies have fared against established performance measures and contains examples of progress toward information sharing goals specified in the IRTPA; Presidential guidelines and requirements; the 2007 National Strategy for Information Sharing;[8] and most recently, the 2012 National Strategy for Information Sharing and Safeguarding (National Strategy), which outlines 16 priority objectives for implementation by ISE departments and agencies. These priority objectives are the foundation for the future of the Information Sharing Environment.



This Report acknowledges remaining gaps in effective information sharing and safeguarding as identified through the ISE performance management framework and the findings of the Government Accountability Office (GAO). The activities detailed herein are products of National Strategy implementation plans under the oversight of the ISA IPC. While implementation planning and performance management are focused on the National Strategy and its associated priority objectives, GAO's High Risk List areas of concern are being addressed along with National Strategy implementation.

---

[6] For the purposes of this Report, the term Information Sharing Environment, or ISE, refers to the national level ISE defined in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, P.L. 108-458 (Dec. 17, 2004), §1016(b). All other mentions of information sharing environments, such as those at the state level, will be defined by their scope, which is included in their title.

[7] IRTPA, as amended, P.L. 108-458 (Dec. 17, 2004), §1016 (h)(i).

[8] The 2007 National Strategy for Information Sharing remains in effect, and is complemented by the 2012 National Strategy for Information Sharing and Safeguarding.

Finally, as in previous years, this Report includes the PM-ISE's reporting responsibilities associated with what was formerly known as the Interagency Threat Assessment and Coordination Group (ITACG).[9] Effective April 2013, the ITACG was succeeded by the Joint Counterterrorism Assessment Team (JCAT). Details of this succession are contained in Section 1 of this Report.

SCOPE

The ISE is a partnership for sharing and safeguarding terrorism-related information among the law enforcement, public safety, defense, intelligence, homeland security, and diplomatic communities, and includes Federal Government departments and agencies; state, local, tribal, and territorial (SLTT) governments; private-sector partners; and foreign partners and allies. This 2013 ISE Annual Report to the Congress incorporates input from mission partners,[10] represents each of these communities, and uses their initiatives and the office of the PM-ISE's management activities to provide a narrative assessment on the state and progress of terrorism-related information[11] sharing and safeguarding. This includes an assessment of our collective ability to secure the nation and our national interests. The reporting period covered in this Report is July 1, 2012 through June 30, 2013.

Throughout the Report, narratives, performance data, and illustrative examples provide an assessment of the maturity and progress of responsible information sharing activities, and communicate the ways in which both progress made and remaining gaps are impacting missions across the ISE.[i] Relevant activities are referenced to IRTPA requirements in the Endnotes to the Report. Interludes between the main sections further illustrate how mission partners are implementing the ISE through their use of technology, standards, and common processes to improve responsible information sharing inside and outside of the counterterrorism domain.

A classified supplement to this Report, under separate cover, provides the Congress with additional information on progress made, as well as continuing gaps and challenges.

MEETING THE LEGAL REQUIREMENTS FOR ISE PERFORMANCE MANAGEMENT REPORTS

Section 1016(h) of the 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 in the Endnotes to the Report, and all reporting requirements are addressed. In addition, reporting which corresponds to the ISE

[9] 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).
[10] IRTPA Section 1016 (i)(4).
[11] 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).

attributes listed in Section 1016(b) is cited in order to show alignment between ISE activities and the mandatory attributes of the ISE.

PRIMARY SOURCES

In order to provide the best possible assessment of progress made on implementation of the ISE, this Report contains data sourced by office of the PM-ISE's coordinators through daily interaction with our partner agencies, as well as data provided by the agencies that are responsible for executing information sharing and safeguarding initiatives. Agency performance data comes from responses to the annual ISE Performance Assessment Questionnaire (ISE PAQ), other direct agency input,[12] and from the ISA IPC subcommittees and working groups.

[12] IRTPA Section 1016(i)(4).

This page intentionally left blank.

SECTION 1:

COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY

This section addresses the maturation of foundational ISE mission processes, including progress made on existing information sharing procedures between the federal, state, local, tribal, and territorial governments, private-sector, and foreign partners and allies. Many of these activities were called out in the 2007 National Strategy for Information Sharing, which remains in effect and continues to guide ISE activities.

This section also examines new and emerging information sharing initiatives in both traditional terrorism and homeland security missions, and other missions that collect and maintain data to support traditional ISE mission processes. Many of these activities are identified as priorities in the National Strategy for Information Sharing and Safeguarding (National Strategy), or have been the focus of recent reporting by the GAO. Where this is the case, it is noted in this section.

The following list of findings highlights both accomplishments and opportunities for additional improvement. Further detail is provided in the pages that follow.

ACCOMPLISHMENTS

- The Administration released three national-level policy directives that reinforce the importance of information sharing with private-sector critical infrastructure owners and operators, and that boost security and resiliency as a national priority;
- NCTC, DHS, and the FBI established the Joint Counterterrorism Assessment Team (JCAT) as the successor organization to the Interagency Threat Assessment and Coordination Group (ITACG);

- The FBI added the National Palm Print System (NPPS) and Enhanced Latent Functionality to its Next Generation Identification System (NGI). With its deployment, NGI users immediately benefited from accuracy three times greater than that of pre-deployment levels;
- DHS established the Field Analytic Support Task Force (FAST) to advocate for state, local, tribal, and territorial (SLTT) government agencies' intelligence requirements, and to collaborate with federal agencies to share intelligence products with SLTT government partners;
- DHS Office of Intelligence and Analysis (I&A) hosted the first exercise under the Fusion Center Performance Program (FCPP), a performance management framework designed to measure the impact and value of individual fusion centers and the National Network of Fusion Centers;
- DHS migrated the Homeland Security Information Network (HSIN) and its Critical Infrastructure Community of Interest to a new platform in order to improve private-sector partners access to sensitive but unclassified information;
- The International Association of Chiefs of Police (IACP) and the PM-ISE are sponsoring a Unified Message Task Team (UMTT) to enhance Suspicious Activity Reporting (SAR) training, metrics, and policies;
- The Global Justice Sharing Initiative (Global) put out a call to action challenging governors, sheriffs, chiefs of police, and other Global Advisory Committee (GAC)[13] members to adopt strategic solutions to transform the nation's justice and public safety information sharing activities—the tenets of which are being used to build state and regional information sharing environments; and
- The office of the PM-ISE is working closely with the U.S. Chief Technology Officer (CTO) and the Council on Women and Girls to support efforts to utilize innovative technology and advanced intelligence analysis to better target criminal investigations of human traffickers.

OPPORTUNITIES

- Resource constraints, especially among SLTT law enforcement agencies, have necessitated 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. The Global call to action to SLTT partners and the PM-ISE-sponsored nationwide deconfliction strategy are seeking to address this.
- Many of the challenges noted in last year's report with respect to information sharing between the Federal Government and private-sector owner/operators of critical infrastructure persist, but there has been a concerted effort on the part of the Federal Government over the past twelve months to address the findings of the National

[13] http://it.ojp.gov/default.aspx?area=globalJustice&page=1021

Infrastructure Advisory Council (NIAC). Details of these activities are included in this section of the Report, under the heading, "Private Sector Information Sharing."

- Gaps continue in information sharing with tribal law enforcement agencies. This year the office of the PM-ISE, in coordination with the Department of the Interior (DOI), DOI's Bureau of Indian Affairs (BIA), the Department of Justice (DOJ), DOJ's Office of Tribal Justice (OTJ), NCTC, the FBI, DHS, and the IACP convened the Tribal Information Sharing Working Group (TISW), which identified eight major findings that hinder tribal information sharing, and subsequently has developed recommendations for improvement.

- The 2013 PM-ISE report, "Improving Suspicious Activity Reporting (SAR) Analysis," finds there are opportunities to further integrate SAR information into federal, state, and local intelligence analytic processes. PM-ISE is working with the ISA IPC SAR Subcommittee to address the findings and recommendations in the report.
- Federal Operation Centers need to adopt a common Request for Information (RFI) exchange process, and develop a common Alerts, Warnings, and Notifications (AWN) information exchange process, as well as information exchange protocols.

LAW ENFORCEMENT AND HOMELAND SECURITY INFORMATION SHARING

JOINT TERRORISM TASK FORCES (JTTFs)

The tactical edge of counterterrorism within the U.S. homeland remains the FBI's JTTF—a small cell of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists drawn from federal, state, local, and tribal law enforcement and intelligence organizations.

The first JTTF was established in New York City in 1980, but the years since 9/11 have seen a dramatic growth in the numbers and capabilities of JTTFs. Today, the JTTFs in 103 cities include more than 4,200 members—more than four times the pre-9/11 total—hailing from nearly 600 state and local agencies and 50 federal agencies, most notably including the DHS, the U.S. military, Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA).

JTTFs are a major counterterrorism asset as a result of the collaborative work, pooled knowledge, and specialized capabilities of their varied membership. They demonstrate the value that results from an environment in which information is shared freely, and in which action is supported by information drawn together from many sources.

NATIONAL NETWORK OF FUSION CENTERS

Located in states and major urban areas throughout the country, fusion centers empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection owners and operators, and private-sector security personnel to understand local implications of national intelligence findings, enabling local officials to better protect their communities. As of March 2013, 78 designated state and major urban area fusion centers make up the National Network of Fusion Centers (National Network). Agency responses to the 2013 ISE Performance Assessment Questionnaire (ISE PAQ)[14] indicate that 57% of federal agencies participate in the National Network; and that 68% incorporate fusion center information into their own products and services.

CONTINUED PROGRESS IN ENHANCING THE CRITICAL OPERATIONAL CAPABILITIES OF THE NATIONAL NETWORK OF FUSION CENTERS

In accordance with national strategies and policy, the Federal Government has formalized processes for guiding support to fusion centers and evaluating their capabilities.[15] In particular, DHS, in collaboration with fusion center directors and federal partners, has instituted a repeatable annual assessment process[16] to measure the progress made by the National Network in maturing state and local intelligence processes and analytic capabilities.[ii] This assessment aims to objectively evaluate information sharing by fusion centers and the National Network as a whole, while simultaneously providing valuable feedback on support provided by the Federal Government to help further develop and sustain the network.

TERRORIST SCREENING CENTER (TSC)

The TSC reported that in a three-month period ending in August 2012 there were 214 cases of actionable or investigative intelligence developed and 60 new service requests generated through information provided by fusion centers to the TSC. By October 2012, there were 489 cases of actionable or investigative intelligence developed and 152 requests generated through information provided by fusion centers to the TSC.

[14] See Appendix A for a list of responding agencies.

[15] The four identified Critical Operational Capabilities which reflect the National Network priorities identified jointly by Fusion Center Directors and the Federal Government and are now identified in the National Strategy as a priority objective are: **COC 1**—Receive: The ability to receive classified and unclassified information from federal partners; **COC 2**—Analyze: The ability to assess local implications of threat information through the use of a formal risk assessment process; **COC 3**—Disseminate: The ability to further disseminate threat information to other SLTT and private-sector entities within their jurisdiction; and **COC 4**—Gather: The ability to gather locally-generated information, aggregate it, analyze it, and share it with federal partners, as appropriate.

[16] The DHS assessment methodology can be found in the 2011 Fusion Center Assessment, available here: https://www.dhs.gov/annual-fusion-center-assessment-and-gap-mitigation-activities

Progress has increased steadily since 2010. As of 2012, 97% of fusion centers identified counterterrorism as a core mission focus; 96% indicate that they apply an all-crimes approach; and 70% indicate they apply an all-hazards approach.[17] In addition, as detailed in Figure 1, 100% of designated fusion centers at the time of the assessment had approved privacy, civil rights, and civil liberties policies in place;[iii] and more than 92% of fusion centers have documented and approved plans, policies, or standard operating procedures for the four identified Critical Operational Capabilities (COC).[iv]

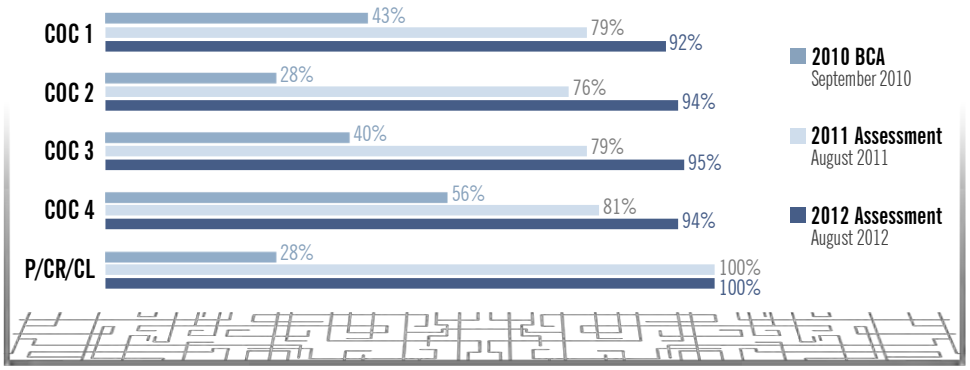


Figure 1. Continued Progress in Enhancing the Critical Operational Capabilities of the National Network of Fusion Centers.

To assist fusion centers in fully achieving and maintaining the four COC, DHS I&A has deployed more than 90 personnel, including Intelligence Officers and Regional Directors, to the field. I&A has worked aggressively to deploy the Homeland Secure Data Network (HSDN) to more than 65 fusion centers,[v] enhancing information sharing at the SECRET level. In addition, the FBI strategy for fusion center engagement has resulted in 90 FBI personnel deployed to fusion centers and FBINet connectivity in approximately 45 of them.[vi] DHS also established a maturity model for the National Network as part of the assessment program. This model identifies four stages—*fundamental, emerging, enhanced*, and *mature*—through which the National Network will progress as it moves towards full capability and operational integration as a unified system. As of February 2013, the National Network is in the second stage of the maturity model, with ongoing efforts to build and achieve full capacity.[vii]

[17] The 2012 FEMA National Preparedness Report, http://www.fema.gov/library/viewRecord.do?id=5914, finds that the National Network of Fusion Centers are effectively bringing together federal, state, and local law enforcement, as well as other public safety officials and private-sector partners to share intelligence and information.

PARTNER ACTIVITIES

FUSION CENTER PARTNERSHIPS

In line with the recommendations in the recently released report, *Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities (GAO-13-471)*, DHS continues to emphasize the importance of ongoing coordination and collaboration between fusion centers; FBI Field Intelligence Groups (FIGs); the High Intensity Drug Trafficking Areas (HIDTA) Program's Investigative Support Centers (ISC); the Regional Information Sharing Systems (RISS) Program's Centers; and major city and county intelligence units to support implementation of the statewide fusion process. To support these coordination efforts, DHS has sponsored 19 analytic exchanges between analysts from fusion centers, HIDTA ISCs, city and county intelligence units, and RISS centers since January 2012. The analytic exchanges promoted collaboration between analysts to share information, including state and local Requests for Information (RFI). Furthermore, the exchanges provided an opportunity to increase the quality of analytic products.[viii]

FUSION LIAISON OFFICER PROGRAMS

On March 15, 2012, the National Fusion Liaison Officer (FLO) Program convened a workshop to facilitate the sharing of best practices and lessons learned between FLOs[18] across the National Network. The workshop provided opportunities for facilitated discussion on ways to implement a bottom-up approach to standardize liaison officer programs across the National Network. The workshop findings included a recommendation that FLO program coordinators conduct regular conference calls, the first of which occurred on January 24, 2013. This national conference call was established to discuss current trends, best practices, and lessons learned from FLO programs across the National Network. This coordination not only improves communications between FLO program coordinators, but also provides opportunities to discuss common and consistent approaches to the operation of FLO programs.[ix]

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

Fusion centers develop, implement, and enforce P/CR/CL safeguards to protect constitutional rights, and to ensure that they are addressing their ethical and legal obligations while engaged in the fusion process. Their commitment to these safeguards builds trust with partners and the community, and fosters increased information sharing, which is vital to executing the fusion process. Fusion centers work to ensure that their personnel understand the importance of protecting P/CR/CL, and that intelligence systems are used in a manner that conforms to appropriate P/CR/CL protection protocols and regulations. For details on National Network P/CR/CL compliance and training, see Section 5 of this report.

[18] Per department or agency policy, FLOs are also known as terrorism liaison officers, intelligence liaison officers, or field intelligence officers.

JOINT PRODUCT DEVELOPMENT ASSISTANCE PROGRAM

In 2012, as part of the DHS/DOJ Fusion Process Technical Assistance Program and Services, DHS facilitated the development of nine joint intelligence products between fusion centers that address cross-jurisdictional homeland security issues such as border-related crime, transnational organized crime, critical infrastructure assessments, and other strategic issues.[19, x] The collaboration necessary to develop joint products improves communication between fusion centers and partners in their areas of responsibility, including private-sector and public-safety entities. Furthermore, the relationships established during these projects build the foundation for future partnerships, which strengthens the fusion center network.

FIELD ANALYTIC SUPPORT TASK FORCE

On October 1, 2012, DHS I&A established the Field Analytic Support Task Force (FAST). FAST is led by senior personnel from I&A, and the State and Local Program Office (SLPO), and supported by analysts who are experienced in analysis and production from across I&A. FAST advocates for the intelligence requirements of SLTT government agencies, and collaborates with federal partners to identify, develop, and share intelligence products with SLTT partners. It also manages and sponsors joint analysis and production efforts with fusion centers, with an emphasis on improving tailored, regionally-focused analysis. FAST ensures coordination with the NCTC, including access to intelligence community (IC) products and education of IC analysts on SLTT needs and requirements, promotes collaboration among analysts, and manages system advocacy and requirements generation.[xi]

BUILDING COMMUNITIES OF TRUST (BCOT)

The BCOT initiative is designed to encourage and improve information sharing among police officers, fusion centers, and the communities they serve—particularly immigrant and minority communities—to address the challenges of crime control and terrorism prevention. The knowledge and insight that comes from trust-based relationships between law enforcement and the community are critical because they allow law enforcement to better distinguish between innocent behaviors and behaviors that may be indicative of criminal activity. Through 2012, the Nationwide SAR Initiative (NSI) led implementation of BCOT efforts, culminating in a roundtable in December 2012. In January 2013, DHS, in collaboration with the NSI PMO; the office of the PM-ISE; DOJ's Office of Community Oriented Policing Services; and the U.S. Attorney's Office, took the lead in implementing the BCOT initiative across the country to help facilitate relationships of trust among local communities, local law enforcement, and fusion centers. DHS has committed to sponsoring 25 BCOT engagements across the country in the next year.[xii]

[19] Fusion centers also develop joint products outside of this Technical Assistance Program.

NATIONAL FUSION CENTER EXERCISE (FUSION X)

As a key component of the Fusion Center Performance Program (FCPP), DHS I&A conducts periodic exercises to evaluate the progress of fusion center capability development and performance. I&A hosted the first exercise under the FCPP in August 2012. Federal agencies, including the FBI, and eight fusion centers participated in this exercise, which was called FUSION X. This exercise provided a valuable opportunity for fusion centers to operationally apply, demonstrate, and assess Critical Operating and Enabling Capabilities alongside National Network and federal partners in response to a regional threat scenario.[xiii]

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.[20] The program's continued implementation and expansion beyond the law enforcement community is one of the priority objectives outlined in the National Strategy.

The NSI is a tool to help prevent terrorism and other related criminal activity by creating a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. The NSI coordinates closely with the DHS "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, and to encourage the reporting of suspicious activity to local law enforcement authorities.

Over the past year, the NSI PMO continued to implement the standards, policies, and processes of the NSI across the National Network. As of June 2013, 78 fusion centers have the capability to contribute and share suspicious activity reports, expanding the reach of the NSI to more than 14,000 law enforcement agencies in all 50 states, as well as the District of Columbia, Puerto Rico, and the Virgin Islands.[xiv] To date, more than 35,000 SAR entries have been submitted by stakeholders to the NSI, and tens of thousands of queries have been made by investigators and analysts. The entries have been successfully leveraged from an investigative perspective by the FBI, and analysts are utilizing this information to advance their situational awareness, and to produce intelligence products related to suspicious activity reporting.[xv]

A UNIFIED MESSAGE FOR SAR

This year the NSI PMO worked with the International Association of Chiefs of Police (IACP) and other state, local, and federal partners to develop the Unified Message document, titled *A Call to*

[20] NSI sustainment has been a focus of discussion over the past year, with the leadership of the IACPUMTT taking steps to identify near and long-term sustainability—to include identifying a path to fiscal sustainment and a viable long-term parent organization. With PM-ISE leadership, federal partners are working to address permanent funding issues.

Action: A Unified Message Regarding the Need to Support Suspicious Activity Reporting and Training. This document emphasizes the importance of reporting suspicious activities; stresses the importance of SAR training and tells agencies where they can receive it; discusses the role of fusion centers, FBI Field Intelligence Groups (FIG), and FBI JTTFs in analyzing and investigating SAR; and encourages agencies at all levels of government to work with the DHS on its "If You See Something, Say Something™" campaign.[21] The IACP and PM-ISE are sponsoring a Unified Message Task Team (UMTT), which uses the Unified Message to enhance SAR training for law enforcement agencies. The UMTT is also promoting efforts to incorporate Terrorist Screening Center (TSC) efforts into the unified message, to improve SAR metrics, and to develop and distribute model policies to local law enforcement agencies in order to institutionalize and operationalize the reporting of SAR.[xvi]

IMPROVING SAR ANALYSIS

In late 2012, the office of the PM-ISE, in consultation with the NSI PMO, the FBI, the Federal Government, and SLTT partners, examined the implementation of the current ISE-SAR Functional Standard to identify gaps, challenges, and opportunities in analyzing ISE-SAR information.[xvii] The findings and recommendations of the review are intended to assist program managers with completing implementation of NSI programs across the National Network of Fusion Centers and the Federal Government, and seamlessly integrate ISE-SAR information into analytic processes and potentially subsequent investigations by FBI JTTF personnel.

Overall, the review found that significant progress was made over the past two years to help analysts incorporate ISE-SAR information into their analytic workflow. However, opportunities exist to further leverage ISE-SAR information. For instance, the inability to download or import ISE-SAR data from the NSI Federated Search Tool and eGuardian limits fusion center analysts' ability to seamlessly integrate this information into their analytic processes. This limitation, which is by design, is intended to ensure that originators of ISE-SAR data are able to keep this information up-to-date, as well as to ensure that proper access controls are in place, and that privacy, civil rights, and civil liberties (P/CR/CL) protections are maintained. Any course of action to overcome this limitation would necessarily have to possess at least the same levels of data integrity, access control, and P/CR/CL protections as currently exist.

The review identified other noteworthy challenges. Fusion center analysts recommended that the behaviors listed in Part B of the ISE-SAR Functional Standard should be updated to bring the document up to date with current analysis of behaviors and indicators of violent extremism and mobilization to violence. In addition, several analysts lamented that a lack of a shared understanding of the value that intelligence analysis brings to strategic planning and decisionmaking contributes to analytic capability shortfalls. The review found that intelligence

[21] http://nsi.ncirc.gov/documents/A_Call_to_Action.pdf

analysis processes are not part of the law enforcement agencies' "gold standard" for accreditation.

Based on the findings, PM-ISE made the following recommendations for ISE-SAR analysis:

- The ISA IPC SAR Subcommittee should consider establishing a SAR Analytic Working Group, composed of federal and SLTT analysts, to review the existing overall NSI Concept of Operations (CONOP), and to jointly develop a more focused analysis CONOP to more clearly articulate its roles, responsibilities, and expectations;
- The SAR Subcommittee should explore various solutions that may be offered as shared services for responsibly, reliably, and repeatedly correlating ISE-SAR and other law enforcement and criminal intelligence data through national data exchanges;
- The ISE-SAR analysis training should be enhanced by presenting a menu of approaches for processing, analyzing, and disseminating ISE-SARs, making it a more practical course with components that can be incorporated wholly or in part into the workflow of fusion centers and federal agencies;
- The SAR Subcommittee should conduct a comprehensive stakeholder analysis to identify governance gaps for the NSI; take the necessary steps to fill these gaps; and raise to the attention of the ISA IPC any issues with filling governance shortfalls;
- The SAR Subcommittee should convene a panel of federal, state, and local subject matter experts to review the criteria listed in Part B of the ISE-SAR functional standard to determine if it should be updated;
- The SAR Subcommittee and the P/CL Subcommittee of the ISA IPC should jointly support the NSI PMO efforts for reviewing compliance of ISE-SAR reporting with the functional standard across the entire ISE; and
- The SAR Subcommittee should evaluate the need to develop and implement an end-to-end comprehensive performance framework that enables programmatic decisions by providing key information on an ongoing basis for evaluating ISE-SAR integration into analytic processes and potential subsequent investigation by FBI JTTFs (for those SARs with a terrorism nexus).

eGUARDIAN AND NSI SHARED-SPACE INTEROPERABILITY AND ENHANCEMENTS

The FBI's eGuardian system was developed to help meet the challenges of collecting and sharing potential terrorism-related SARs 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 further investigative action. The FBI enhanced its internal Guardian system to be able to push unclassified Guardian incidents to

eGuardian in 2010. To date, more than 18,534 incidents have been shared with eGuardian and the NSI Shared Spaces.

GUARDIAN SUPPORT TO THE BOSTON BOMBINGS INVESTIGATION

During the investigation following the April 15, 2013 Boston Marathon bombing, the FBI utilized Guardian to facilitate a flow of leads and tips generated by FBI field offices, state and local police forces, and the public. The Guardian system enabled more complete and comprehensive analysis of all the available information in support of national-level decisionmaking.

The FBI Counterterrorism Division's Guardian Management Unit (GMU) monitored and coordinated the flow of information received by the Guardian system, and assured users that pertinent information on the bombing was being shared.

Supporting the investigation, GMU identified and reported 177 Guardian incidents relevant to the investigation; those leads were generated not only from the internal Guardian system, but also from eGuardian. The leads enabled direct reporting of relevant information to the FBI for additional assessment.

Information sharing between the FBI and the public was vital to the Boston Bombings investigation. After a press conference on April 18, the FBI received more than 5,700 tips on that day alone, and approximately 15,000 tips in the days following, which enabled the FBI to generate 119 Guardian leads for assessment.

After the initial investigation, the FBI expanded its review of incidents containing information possibly related to the bombing.

Shared Space to eGuardian Auto-Push A significant accomplishment this past year was the institutionalization of an automatic transfer of information from the NSI Shared Space to eGuardian. As 50 fusion centers use the Shared Space technology, it is vital to ensure that the information being submitted and shared via the Shared Space is also being actively sent to the FBI for assessment. The NSI PMO technology team worked closely with the FBI and the fusion centers to help realize this goal by the end of March 2013, and the auto-push feature is now employed in all fusion centers using the Shared Space technology.[xviii]

New eGuardian Geospatial Tools Standard map controls were delivered last year. This gives users the ability to zoom and pan on eGuardian's dynamic map display, to click on an incident to display core incident data, and to link to the full incident report. Additionally, a new query capability gives users the ability to filter their incident display by state and incident type.

eGuardian Cyber Incident Update eGuardian users can now submit incidents that contain cyber attack and cyber victim information. These cyber incidents are transmitted to the FBI, similar to the process for transmitting incidents related to terrorism.

SAR IN FEDERAL AGENCIES

A rollout plan to formalize the sharing of SAR information currently taking place between federal agencies is under development. This plan will ensure that federal SAR information sharing processes mirror those within the National Network. The implementation of the federal plan involves the identification of those federal agencies with law enforcement personnel; outreach to the executive management of those agencies to gain the necessary support and participation in the NSI; and the execution of a SAR process. The approach also includes the incorporation of the eGuardian system as the technology solution; NSI Line Officer Training; SAR Analytic Training; and adherence to a privacy policy. As of January 2013, 56 federal agencies, representing 226 individual organizations,[22] are in various stages of participation with the NSI, and four additional agencies that may be able to participate have been identified.

BANK SECRECY ACT SUSPICIOUS ACTIVITY REPORTS

The Bank Secrecy Act (BSA), as amended by the USA PATRIOT Act, establishes important reporting requirements for certain financial institutions to help authorities follow the money when tracking illicit actions. These required reports include BSA Suspicious Activity Reports (BSA SAR). BSA SARs are a specific kind of suspicious activity report, distinct from the NSI, that have proved essential in identifying, investigating, and interdicting terrorist activity in the United States.

Financial institutions file BSA SARs with the Financial Crimes Enforcement Network, a bureau of the Department of the Treasury, which makes the information available to appropriate authorities for their investigative and analytical work. BSA SARs highlight suspicious behavior based on indicators of potential criminal activity. The form includes a section for filers to specify whether the activity is believed to be associated with terrorist financing and can help investigators and analysts detect a terrorist cell.

Another report, the currency transaction report (CTR), is filed by certain financial institutions whenever a customer transaction involves more than $10,000 in cash, including related cash transactions over the course of a day that aggregate to more than $10,000. Rather than a subjective analysis of financial behavior, the CTR documents specific transactions and patterns of activity that may lead to a crucial piece of evidence. The FBI reports that, as of June 2012, 37% of their pending counter-terrorism cases have associated BSA reports, and more than 90% of those counter-terrorism BSA reports are CTRs.[23]

[22] Exclusive of 371 additional organizations within the U.S. Department of Defense, which is already an active participant with 1396 eGuardian accounts in more than 260 global installations and facilities.

[23] Remarks of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, to the Florida International Bankers Association Anti-Money Laundering Conference, Miami, Florida, February 13, 2013.

JOINT COUNTERTERRORISM ASSESSMENT TEAM

On April 1, 2013, NCTC, DHS, and the FBI established the Joint Counterterrorism Assessment Team (JCAT) as the successor organization to the Interagency Threat Assessment and Coordination Group (ITACG). The ITACG was established in 2007 under the Implementing Recommendations of the 9/11 Commission Act to integrate, analyze, and assist in the dissemination of federally-coordinated information within the scope of the ISE, including homeland security information, terrorism information, and weapons of mass destruction (WMD) information. Given the expiration of appropriations for ITACG in FY 2012, NCTC collaborated with its partners to build upon the ITACG model to ensure that NCTC, DHS, and the FBI continue to meet the CT mission needs of SLTT partners.

The JCAT is a joint, interagency activity within the NCTC Directorate of Operations Support (NCTC/DOS), with NCTC, DHS, and the FBI sharing staff and other resources. Unlike the ITACG, which was led by a Senior DHS Officer, the JCAT Director position is a rotational billet that can be filled by an officer from any of the three organizations when appointed by the NCTC Director. An NCTC officer will serve as the first JCAT Director. In addition, there are two deputies, both senior officials from DHS and FBI initially. Under the ITACG, there was a single deputy, a senior FBI officer.

Going forward, the JCAT's primary mission is to research, draft, and collaborate with NCTC, DHS, and the FBI for the joint production of counterterrorism and terrorism intelligence for federal, SLTT, and private-sector partners.[xix] This is a change from the ITACG, which was mandated by law only to integrate, analyze, and assist in the dissemination of federally-coordinated information. The JCAT, like the ITACG, will also advocate for the intelligence requirements of the SLTT partners and the private sector, and will work to foster an understanding of SLTT and private-sector intelligence needs throughout the Intelligence Community (IC).[24, xx]

Table 1. ITACG and JCAT Comparison.

ITACG INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP	JCAT JOINT COUNTERTERRORISM ASSESSMENT TEAM
Led by DHS	Led by NCTC, in partnership with DHS and FBI
DHS-sponsored law enforcement, fire service, and public health billets	Cost sharing of law enforcement, fire service, and public health billets by NCTC, DHS, and the FBI
Integrated, analyzed, and assisted federal partners in dissemination	Integrates, analyzes, and assists federal partners in dissemination and produces intelligence in partnership with federal analysts
Integrated in NCTC's Directorate of Operations Support	Fully integrated across all NCTC elements, and with the National Intelligence Manager for Counterterrorism

[24] To aid in ensuring that SLTT intelligence needs are well represented, the staff will include both law enforcement and non-law-enforcement fellowships from the SLTT community.

In 2013, at the request of the NCTC/DOS, the office of the PM-ISE assisted the JCAT in refining their understanding of SLTT partner information requirements and integrating these requirements into the JCAT's standard operating procedures. JCAT is also working closely with the National Intelligence Manager for Counterterrorism (NIM-CT) to integrate and align with IC-wide counterterrorism management frameworks, including the NIM-CT's annual counterterrorism production guidance and performance reviews.

MEASURING JCAT PERFORMANCE

NCTC leadership requires evaluative information to assist them in effectively managing the JCAT. The information should tell them whether, and in what ways, the JCAT is working well, which ways it is not working well, and in both cases why. The purpose of measuring JCAT performance is to promote increased efficiency and effectiveness of the program and ultimately, improved information sharing and enhanced public safety. The PM-ISE is assisting NCTC in developing a comprehensive framework, which will be in place to support the next full round of ISE performance reporting requirements in the spring of 2014.

DOMESTIC INFORMATION SHARING ENVIRONMENTS

Shrinking budgets, dynamic threats, and exploding amounts of data are all significant challenges for the homeland security and law enforcement communities today. Building efficient and effective information sharing environments at the state and local levels using the tools and lessons learned from federal efforts is helping to solve these challenges. Each state, of course, has unique requirements, but states are realizing good results by building ISEs based on best practices.

The call to action for these efforts is the Global Justice Sharing Initiative's (Global) *Strategic Solutions to Transform Our Nation's Justice and Public Safety Information Sharing*.[25] Released in November 2012, this document challenges governors, sheriffs, chiefs of police, and other Global Advisory Committee (GAC) members to develop single-sign-on (SSO) and federated query capabilities; leverage secure cloud solutions; develop and engage in shared services and systems; ensure interoperability between law enforcement deconfliction systems; advance information sharing to support successful reentry of formerly incarcerated individuals; and collaborate with federal partners to coordinate a consistent approach to federal funding, policy support, and universal adoption of common standards and technologies.

States are responding to the call and are realizing benefits. The New York State Police moved from an antiquated mainframe to a service-oriented architecture, reducing costs and improving response time. New York also employed the National Information Exchange Model (NIEM) to

[25] www.it.ojp.gov/docdownloader.aspx?ddid=1809

standardize their data exchanges and deploy a system that is more interoperable with other public-safety databases. And the Illinois Criminal Justice Information Authority is bringing together practitioners, program managers, and technologists from federal, state, and local governments to establish an Illinois ISE that connects information responsibly and effectively.[xxi]

The following section highlights three ongoing state-based efforts:

NEW JERSEY INFORMATION SHARING ENVIRONMENT

In February 2012, the Integrated Justice Information Systems (IJIS) Institute technology assessment of the New Jersey Regional Operations and Intelligence Center (NJ ROIC) provided recommendations for building an integrated information sharing enterprise that would place the NJ ROIC in a unique position to drive and help sustain an information sharing environment within the state. Coordinated by the Police Institute at Rutgers University, with IJIS involvement in leading the development of the standards-based architecture and technology components, this effort is now underway and is a national model for linking state law enforcement agencies with fusion centers.[xxii]

The New Jersey Information Sharing Environment (NJ ISE) Initiative will ensure the expeditious transmittal and receipt of the information and intelligence needed to make better decisions about public safety challenges by:

Enabling the free flow of information in support of statewide law enforcement, homeland security, and emergency management to prevent, mitigate, respond to, investigate, and recover from manmade and natural or disasters;

Providing secure access to information and actionable intelligence for participating agencies, across the public and private sectors, to better assure the safety and security of New Jersey communities;

Providing network, data, and application services in a trusted, Internet-based federation, in conformance with national standards for information sharing and safeguarding; and

Optimizing investment through the use and reuse of business and technological frameworks that have been effectively implemented in state and national initiatives.

This progression to a statewide ISE puts powerful analytic tools that traditionally were only accessible at the Fusion Center into the hands of remote users and makes data that was once unavailable to those outside of a local precinct office discoverable and retrievable to the enterprise as a whole.

At the heart of the NJ ISE initiative is the intention of sharing critical information with key partners at the local, county, state, and federal levels—in a timely, cost-effective, and design-efficient manner. This solution will provide analysts, field operators, investigators, and chief executives with the information and intelligence they need to enhance overall public safety efforts.

INDIANA DATA EXCHANGE

The Indiana Data Exchange (IDEx) is 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, it seeks to connect data from disparate justice and public safety systems for the purpose of enhanced decisionmaking and increased public safety by leveraging prior investments. Using federal grants, national data sharing models and standards (i.e. NIEM), and reusing common information exchange languages, the state is reducing development costs as more agencies request the same data from a common system.[26]

The state could potentially save approximately $2 million in upfront IT development costs and an additional $3 million annually in business cost avoidance from gained process efficiencies.[27] A return on investment report for IDEx concludes that "*there are significant benefits—both from a true cost savings and from a business process/operational savings—in making this investment. Ultimately, it also increases effectiveness and efficiency of government services by placing the right information in the right person's hands at the right time—all critical elements in ensuring a safe community for residents of the Hoosier state*."[28]

CONNECT SOUTH DAKOTA

South Dakota state law enforcement, city police departments, and county sheriffs have traditionally used a variety of systems to manage records and jail information. Until recently, these systems were largely isolated from each other, preventing statewide information sharing. A low-cost solution for statewide information sharing that could incorporate jurisdictions, many with small budgets and few officers, was required.

Using a grant from the DOJ BJA to build the servers and licenses; standards from Global; and with acquisition assistance from the IJIS Institute, South Dakota built the backbone of *Connect South Dakota*. Their systems now use NIEM to standardize data exchanges—providing a secure login environment using role-based permissions through a RISS implementation of the Global Federated Identity and Privilege Management (GFIPM) project.[xxiii]

---

[26] Report: Indiana Data Exchange (IDEx) Return on Investment www.it.ojp.gov/docdownloader.aspx?ddid=1660
[27] Ibid.
[28] Ibid.

Connect South Dakota plans to continue adding partners from the Departments of Corrections, Parole, and Probation, as well as sworn tribal officers in South Dakota; and will grant access to agencies regardless of whether their jurisdiction submits information. *Connect South Dakota Phase 2* will add a web-based Records Management System (RMS) feature for smaller jurisdictions, many of whom use localized databases or pay for vendor solutions.

TRIBAL LAW ENFORCEMENT INFORMATION SHARING

There are more than 2,300 tribal law enforcement officers in 171 tribal police agencies and 37 Bureau of Indian Affairs (BIA) agencies, for a total of 208 agencies associated with the 564 federally recognized tribes in the United States. As noted in last year's report, through Federal Government support, and in cooperation with state and local partners, tribal law enforcement personnel are integrated into several fusion centers. However, as noted last year, there continue to be recognized gaps in tribal information sharing. The variety of challenges include lack of resources; reluctance of some states to allow tribal law enforcement access to federal and state databases; tribal reluctance to engage with outside law enforcement entities; and insufficient training on the use of fusion center resources.[xxiv]

In 2013, PM-ISE, in coordination with BIA, DOJ's Office of Tribal Justice (OTJ), the NCTC, the FBI, DHS, and the IACP convened the Tribal Information Sharing Working Group (TISW) to examine the challenges that exist in justice and public safety information sharing in Indian Country. As of April 2013, the TISW has identified the following eight major findings that hinder tribal information sharing, and has developed recommendations for improvement:

1) Tribal law enforcement participation in fusion centers is an area for improvement, and can be enhanced in a variety of ways;
2) Some states operate outside the goals of the Tribal Law and Order Act;
3) Tribal access to national and state information databases is hampered;
4) More tribal law enforcement entities should have access to the International Justice and Public Safety Network (Nlets);
5) The NSI program has been effective in tribal law enforcement efforts, and federally recognized tribes currently have full access to SARs with no impediments;
6) Some states do not recognize tribal law enforcement as *bona fide* police departments;
7) There should be a continued effort to upgrade technological capabilities in Indian Country; and
8) The DOI Incident Management Analysis and Reporting System (IMARS) could be an opportunity for improved records management in Indian Country. IMARS will also provide tribal agencies with access to some federal databases.

The Office of State, Local and Tribal Affairs within the Office of National Drug Control Policy (ONDCP) convened preliminary meetings with DOJ, DOJ/FBI, and DHS/Customs and Border Protection, as members of a tribal subcommittee, to establish a framework for information sharing considerations and collaboration of federal law enforcement agencies and tribal law enforcement agencies. The preliminary meetings led to a more comprehensive executive meeting with DOJ, DOJ/FBI, OTJ, BIA, and CBP, to consider action items enhancing information sharing in Indian Country resulting in coordinated law enforcement efforts.

COMBATING HUMAN TRAFFICKING

There has been considerable attention within the domestic and international law enforcement and intelligence communities focused on the probability that international terrorist groups exploit existing criminal trafficking networks. The same ISE capabilities that are being implemented to enable the sharing of terrorism-related information can be leveraged to improve the nation's capacity to combat human trafficking.

DHS, through fusion centers, is helping state and local partners identify and report human trafficking indicators to federal law enforcement. Additionally, the IC is developing an all-source intelligence collection strategy for human trafficking to provide actionable intelligence to increase the number of domestic and international trafficking prosecutions. Through efforts like these, the ISE will continue to make a substantial contribution to improving our capacity to combat modern forms of slavery as well as the potential for terrorist exploitation of trafficking networks.

SOUTHEAST LAW ENFORCEMENT AND HOMELAND SECURITY HUMAN TRAFFICKING SYMPOSIUM

The DHS I&A SLPO, in partnership with the Georgia Bureau of Investigation and the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Atlanta field office, hosted the Southeast Law Enforcement and Homeland Security Human Trafficking Symposium in Atlanta, Georgia, on August 8–9, 2012. Approximately 70 local, state, and federal participants attended and discussed emerging issues related to human trafficking in the southeastern U.S. The symposium provided an important opportunity for local, state, and federal entities involved with combating and preventing human trafficking to discuss issues in their respective areas of responsibility. The symposium encouraged dialogue, facilitated information exchange, accelerated the sharing of best practices, and enabled discussion of next steps among local, state, and federal participants.

INTERAGENCY TASK FORCE ON HUMAN TRAFFICKING

In March 2012, the President tasked the Interagency Task Force on Human Trafficking to identify administrative actions internationally and domestically to combat human trafficking. As part of those efforts, the office of the PM-ISE has worked closely with the U.S. Chief Technology Officer (CTO) and the Council on Women and Girls to support efforts to use innovative technology and advanced intelligence analysis to better target criminal investigations of traffickers, and to facilitate more effective information sharing across jurisdictions to make critical investigative connections.

As part of that effort, in February 2013, the CTO convened a meeting with senior law enforcement officials from the Las Vegas Metropolitan Police Department, the Georgia Bureau of Investigation, and the New Jersey State Police, as well as private-sector partners, to develop ways to bring private-sector innovation to help combat child sex trafficking in these three jurisdictions. As New Jersey will host the 2014 Super Bowl at MetLife Stadium, the New Jersey State Police are specifically focused on creating a protocol to address the trafficking that occurs around major sporting events.

JOINT CT COORDINATION CELL (JC3)

As a method of evolving force protection threat information sharing, military service investigative elements and the Defense Intelligence Agency established a Joint Counterterrorism Coordination Cell (JC3). The JC3 aims to provide focused coordination, de-confliction, and analytic functions for terrorism-related investigations in order to ensure multi-agency information sharing and collaboration, to minimize duplicative effort, and to optimize intelligence support for protecting the Department of Defense (DoD) from terrorism.

JC3 achieved initial operational capability in April 2013, and is working to incorporate ISE-SAR information as a principal data source.[xxv] For incidents that reach the threshold of force protection threat information, the JC3 will coordinate the communication of concise summaries that preserve the integrity of ongoing operations and investigations while ensuring awareness for Combatant, Service, and DoD Installation Commanders.

FBI NEXT GENERATION IDENTIFICATION SYSTEM (NGI)

The Next Generation Identification System (NGI) is incrementally replacing the FBI's existing Integrated Automated Fingerprint Identification System (IAFIS), 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 has already deployed services that provide more accurate fingerprint searches, increasing the true match rate to 99.6%.[xxvi]

NEXT GENERATION FACIAL RECOGNITION

Deployed as a pilot in February 2012 and scheduled for full operational capability in the summer of 2014, the NGI Facial Recognition Pilot permits authorized law enforcement agencies to submit queries for a facial recognition search of the FBI's national repository of approximately 15.3 million criminal mug shots. Query requests are automated, and the results are returned to the submitting agency as an investigative lead in the form of a ranked candidate list. Michigan, Maryland, and Texas are currently using the Facial Recognition Pilot to submit facial recognition searches to Criminal Justice Information Services (CJIS). Memorandums of Understanding (MOU) have been executed with Hawaii, New Mexico, Ohio, South Carolina, Maine, Nebraska, Washington, DC Metro, and Tennessee. Minnesota and the U.S. Secret Service are engaged in the MOU review.

REPOSITORY FOR INDIVIDUALS OF SPECIAL CONCERN (RISC)

The Repository for Individuals of Special Concern (RISC), a national-level mobile fingerprint identification capability, makes possible time-critical searches to assist with the identification of wanted persons, known or appropriately suspected terrorists, sex offenders, and persons of special interest. Since deployment of RISC, more than 530 agencies representing 14 states, have begun participation in the national service, and 7 additional states/agencies are in the process of implementing RISC. More than 900 transactions are processed daily, with a response time of less than 7 seconds, and an average weekly hit rate of 6-10%.

NATIONAL PALM PRINT SYSTEM (NPPS) AND ENHANCED LATENT FUNCTIONALITY

In May 2013, NGI established the National Palm Print System (NPPS) and transitioned IAFIS latent print functionality to the new NGI infrastructure. These upgrades provide all latent print capabilities currently supported by IAFIS, as well as enhanced latent capabilities, including expansion of cascaded searches for ten-print and RISC submissions, and additional repositories for searching palm prints and supplemental fingerprints. The benefits of the increased accuracy and the expansion of cascaded searching to additional repositories are already producing results not available with the previous system. Agencies are now transitioning to full functionality.

FBI SENTINEL

The FBI's next-generation information and case management system, Sentinel, was deployed to all employees on July 1, 2012. Sentinel moves the FBI from a paper-based case management system to a digital record system. Sentinel uses a modern web-based application for entry, review, approval, and research of case and intelligence information. It enhances the FBI's ability to link cases with similar information through expanded search capabilities, and streamlines administrative processes through electronic workflow, making new case information and intelligence available more quickly to agents and analysts.[xxvii] The FBI will continue developing Sentinel's capabilities according to employee feedback and organizational requirements. During 2012, the FBI began to contribute records from its Sentinel system to the National Data Exchange (N-DEx).[xxviii]

STANDARDIZING REQUESTS FOR INFORMATION

DHS is the primary federal source of accurate, actionable, and timely homeland security-related information for its federal, SLTT, and private sector partners. To carry out this mission, the DHS Office of Operations Coordination and Planning (OPS) provides situational awareness and a common operating picture through its National Operations Center, which fuses law enforcement, intelligence, emergency response, private-sector and open-source reporting, and shares this information through the Homeland Security Information Network.[xxix] DHS I&A accesses, receives, and analyzes law enforcement, intelligence, and other information, and integrates it into intelligence products that are shared internally and with DHS partners at all levels.

DHS OPS and I&A have developed a standardized business process, the Single Point of Service (SPS), to ensure that all operational and intelligence RFIs are reviewed, validated, and facilitated to the appropriate DHS organizations, as well as to federal, state, and local partners.[xxx] As part of the DHS-SPS process, OPS and I&A have been working with the Office of the Chief Information Officer to develop and deploy an automated RFI Management Tool (RMT) at the Sensitive but Unclassified level. The RMT will serve as OPS and I&A's system of record for recording, tracking, and facilitating requests, including the associated oversight and review process. RMT will provide users with visibility into the RFI process by enabling them to obtain the status and location of their organization's RFIs, submit feedback, obtain performance management (metrics) reporting, and request access to RFIs submitted by other organizations.

DHS ANALYTICAL FRAMEWORK FOR INTELLIGENCE

In FY 2013, ICE partnered with U.S. Customs and Border Protection (CBP) to replace the capabilities of ICE's Intelligence Fusion System (IFS) with the CBP-run platform Analytical Framework for Intelligence (AFI). AFI allows for increased analytic collaboration, cooperation, and efficiencies by providing a full suite of tools designed to enhance all-source data consolidation,

research, intelligence analysis, reporting, and production management. After AFI was identified as ICE's solution for these capabilities, ICE and CBP began to work together as an integrated team to bring in additional data sources to the AFI platform and deploy the application to approximately 5,000 ICE users at all 26 major field offices. The adoption of AFI by ICE and the consolidation of data sources will result in operations cost savings of nearly $3 million per year.

By extending the AFI platform to ICE, both ICE and CBP will begin to share intelligence and a variety of data sources that have previously only been available in disparate systems. AFI will become the central platform where the data will be available to both components as well as other partners within DHS. Plans to extend AFI to U.S. Citizenship and Immigration Services (CIS), TSA, and the USCG are in progress. As additional components join, the information sharing and collaborative intelligence environment will become more robust, resulting in better intelligence products, research capabilities, and investigative insights.

ALIGNING INTERNATIONAL IDENTITY FRAMEWORKS

PREVENTING AND COMBATING SERIOUS CRIME (PCSC)

The Agreement on Preventing and Combating Serious Crime (PCSC) refers to bilateral agreements between the United States and other countries to share information about individuals to prevent or combat a serious crime.[29] A PCSC agreement provides for the reciprocal exchange of biometric and biographic data, and any relevant underlying information, to prevent or combat an offense punishable by a maximum deprivation of liberty of more than one year, or a more serious penalty. Currently 36 of the 37 Visa Waiver Program (VWP) countries and three non-VWP countries have entered into PCSC agreements with the United States. Most recently, in May 2013, the Government of Chile and the U.S. entered into a PCSC agreement.

NORTH AMERICAN DAY (NAD) PILOT PROGRAMS

The United States, Canada, and Mexico annually participate in the North American Day (NAD) conference to exchange ideas about improving information technology issues of common concern among the three countries. During the July 2011 NAD conference, delegations from each country signed a trilateral MOU, and established information sharing pilot projects to conduct trilateral test data exchanges for public health alerts and stolen vehicle information issues based on common processes and framework standards. The purpose of the pilots was to demonstrate consistent and repeatable information sharing among the three countries without having to rely upon ad-hoc or point-to-point interfaces.

[29] PCSC are agreements entered into pursuant to the 9/11 Commission Act of 2007 which requires VWP countries to enter into information sharing agreements with the United States.

The NAD 2012 Summit provided the CIOs from Canada, Mexico, and the United States with a venue in which to discuss the results of the two trilateral pilot projects for information exchange. The Public Health pilot focused on exchanging aggregated health alerts concerning food-borne illness outbreaks, and successfully exchanged real-time, aggregated, public health alerts among the three countries. Results and lessons learned are currently being documented to share with the public health community and the World Health Organization, as is a roadmap for moving the pilot to full production. The Public Safety pilot is ongoing and is focused on trilateral exchanges of information about stolen vehicles that cross the borders of the three countries.[xxxi] A trilateral working group has conducted a technical demonstration and test exchange between the United States and Canada, and is nearing completion on a text exchange with Mexico.

In addition to exploring approaches to operationalizing the exchanges, the three countries are pursuing opportunities for future collaboration. These include Canada's adoption of or participation in an Open Government Platform (OGPL)—the open-source version of Data.gov software developed by the United States and India—as the basis of its new open data portal, data.gc.ca; identifying and implementing best practices in the three countries' identity management and authentication programs; and a potential NIEM-based pilot to share information on missing children and Amber Alerts.

ALIGNING MULTI-NATIONAL IDENTITY MANAGEMENT SYSTEMS

GSA took the lead in implementing a NAD agreement to align identity management systems across the U.S., Canada, and Mexico, and expanded the collaboration to Denmark, the United Kingdom, Australia, and New Zealand. Each country's national identity experts attended a two-day Identity Summit in February 2013, and will continue to meet regularly to share ideas about identity, credentials, and access management. The participants are exploring consistent approaches to identity management by first coming to agreement on the essential factors that define identity.[xxxii]

PRIVATE-SECTOR INFORMATION SHARING

More than 85% of the nation's infrastructure is owned by the private sector.[30] This infrastructure is vulnerable to manmade threats—as evidenced by the denial-of-service cyber attacks that breached some of the nation's most advanced computer defenses at the largest U.S. banks—as well as natural disasters, as made evident by the effects of Hurricane Sandy on the electric, transportation, and waste water sectors. The importance of responsible information sharing to bolster the security and resiliency of our critical infrastructure cannot be overstated.

As noted in our 2012 Annual Report, in January 2012, the National Infrastructure Advisory Council (NIAC) issued a report to the President on Intelligence Information Sharing with the private sector.[31] The report called attention to seven areas where public-private sector information sharing was lagging:

- authority and policy;
- implementation of authority;
- leveraging the capability of the private sector to reduce risk;
- information content;
- information delivery;
- counterintelligence and counterterrorism; and
- leveraging the National Network of Fusion Centers.

ADDRESSING THE 2012 NIAC REPORT FINDINGS

In 2012 the PM-ISE championed a collaborative effort with DHS and the Office of the Director of National Intelligence (ODNI) to address gaps in intelligence and information sharing with the private-sector critical infrastructure and key resource owners and operators. The initiative began in October 2012, and is focused on integrating private-sector requirements and equities into existing processes of the ISE; increasing participation by the private sector in the ISE; and extending the existing capabilities, frameworks, and approaches that are centered on federal, state, local, and tribal agencies to support improvements in Critical Infrastructure and Key Resources (CIKR) information sharing with the private

2012 NIAC RECOMMENDATIONS

1	Assert the priority of infrastructure protection and resiliency
2	Improve implementation of existing authorities
3	Improve information content by leveraging partner capabilities
4	Improve the value of information products to risk management
5	Build accepted practices for timely information delivery
6	Capitalize on P/S capabilities for counterterrorism product solutions
7	Enhance fusion center capabilities as a mechanism for sharing
8	Develop an action plan to implement accepted recommendations

[30] http://www.dhs.gov/critical-infrastructure-sector-partnerships

[31] 2012 National Infrastructure Advisory Council Report to the President, http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf

sector.[xxxiii] In addition, the Administration has taken a number of steps to address several of the NIAC report findings and recommendations, some of which we highlight below.

NIAC RECOMMENDATIONS 1 AND 2

Assert the priority of infrastructure protection and resiliency in national security; Improve implementation of existing authorities.

FEDERAL GOVERNMENT RESPONSE

The Administration released three national-level policy directives that reinforce information sharing with critical infrastructure stakeholders, and boost security and resiliency as a national priority.[xxxiv] These policies' complementary goals provide the foundation for strengthening the resiliency of the critical infrastructure of the United States through partnership and collaboration between government and the private sector.

The National Strategy for Information Sharing and Safeguarding, released in December 2012, specifies the need to "establish information sharing processes and sector specific protocols with private sector partners to improve information quality and timeliness" as a priority.

Presidential Policy Directive (PPD)-21*,* released in February 2013, establishes national policy on critical infrastructure security and resilience, and establishes a shared responsibility among federal, state, local, tribal and territorial entities as well as public and private owners and operators of critical infrastructure. This directive also seeks to refine and clarify the functions, roles, and responsibility related to critical infrastructure protection across the Federal Government.

Executive Order (EO) 13636, released in February 2013, directs increases in the volume, timeliness, and quality of cyberthreat information shared with private-sector entities for the purpose of improving the security and resiliency of our nation's critical infrastructure against evolving physical and cyber threats and hazards.

DHS is the Federal Government's lead agency for coordinating efforts to implement EO 13636 and PPD-21. It has formed an interagency task force comprised of nine working groups to engage the Federal Government, SLTT governments, and private-sector partners in implementing the policies' major deliverables, and plans for these policies to be substantially implemented within one year. The major information sharing objectives and deliverables of these executive policies parallel the findings and recommendations of the NIAC report.

NIAC RECOMMENDATIONS 3, 4, AND 6

Improve information content by leveraging partner capabilities; Improve the value of information products to risk management; Capitalize on private sector capabilities for counter-terrorism product solutions.

FEDERAL GOVERNMENT RESPONSE

The DHS National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) and DHS I&A launched three targeted initiatives designed to incorporate the knowledge and expertise of CIKR owners and operators.

Leveraging Cross-Sector Capability – DHS established a working group of cross-sector representatives to assess the relevance of intelligence data and its usefulness to CIKR owners and operators across multiple sectors. Following a successful pilot, DHS developed a concept of operations to implement the capability.

Increasing Private-Sector Access to Relevant Fusion Center Products – DHS began developing an enterprise-wide approach to efficiently make relevant fusion center analytic products available to the private sector via the Homeland Security Information Network (HSIN) and its Critical Infrastructure Community of Interest.

Leveraging Private Sector Owner and Operator Expertise – In the summer of 2012, DHS and the Department of Energy (DOE) sponsored a classified cyber-threat briefing for Chief Executive Officers of electric utilities from across the nation. This led to a major executive-level industry initiative to identify the requirements and dedicate the necessary resources to address this sector-specific cyber-threat. Additionally, in March 2013, DHS began developing a process to engage appropriate CIKR stakeholders in the development of DHS analytical products prior to their dissemination to private-sector partners. This process is designed to increase the quality and usefulness of strategic analytic products by ensuring that they reflect private-sector requirements and concerns.

NIAC RECOMMENDATIONS 4 AND 5

Improve the value of information products to risk management; Build accepted practices for timely information delivery.

FEDERAL GOVERNMENT RESPONSE

In the last year, DHS NPPD IP migrated the Homeland Security Information Network and its Critical Infrastructure Community of Interest to a new platform to improve private-sector partners' access to sensitive but unclassified information.[xxxv] The Suspicious Activity Reporting Tool for Critical Infrastructure Sectors on HSIN is now deployed to the Chemical, Commercial

Facilities, Oil and Natural Gas, Health and Public Health, and Highway Motor Carrier sectors, more than doubling the number of sectors engaged in suspicious activity reporting.[xxxvi] Each of these sectors can now use this tool to track its own suspicious activity reports and trends, and to identify potential anomalies. Additionally, the ODNI conducted an assessment in February 2013 that confirmed the need to improve the provision of relevant, actionable intelligence threat information to CIKR stakeholders. Working with DHS, efforts are underway to pilot the integration of IC and private-sector analytic capabilities to provide better tailored information to specific sectors and to better reflect sector needs in national intelligence processes.

NIAC RECOMMENDATION 7

Enhance Fusion Center capabilities as a mechanism for sharing.

Specifically, the NIAC Report recommended that to better assist private-sector partners, DHS should sponsor training and/or rotational assignments with fusion center analysts; assist fusion centers with developing analytic products to distribute to relevant sectors; and assist fusion centers and their private-sector partners in becoming active participants in the Nationwide Suspicious Activity Reporting (SAR) Initiative.

FEDERAL GOVERNMENT RESPONSE

DHS NPPD IP, in collaboration with DHS I&A, developed the *Infrastructure Protection Field Resource Toolkit* to enhance critical infrastructure information sharing and analytical capabilities across the National Network. The toolkit is a suite of resources tailored to meet the unique critical infrastructure protection needs of each fusion center. The Toolkit enables fusion center personnel to access analytical training, data, and tools to support critical infrastructure analysis and information sharing capabilities, and to advance fusion center support to the NSI.

At the state and local level, the fusion center stakeholders established a Working Group on Private-Sector Best Practices. The PM-ISE and DHS are supporting the working group's efforts to accelerate the private-sector engagement capabilities of fusion centers.

HOMELAND INFRASTRUCTURE THREAT AND RISK ANALYSIS CENTER

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) is a partnership between DHS I&A and DHS NPPD IP. The HITRAC's analytic program enhances risk-based decisionmaking for steady-state and crisis-response efforts related to homeland security. It focuses on understanding and analyzing strategic-level risks within and across sectors, as well as developing and enhancing modeling capabilities to address current, evolving, and future threats.

In collaboration with other DHS components, the Center provides tailored risk-assessment products for critical infrastructure and key resource sectors. It fuses consequence and

vulnerability information from infrastructure protection communities with threat information from the intelligence and law enforcement communities. HITRAC analytical products support NPPD subcomponents in their engagement with stakeholders and audiences at the national, state, local, and international levels.

UNDERSTANDING THE IMPACT OF CYBER THREATS ON PHYSICAL SECURITY

Holistic thinking about security and risk management is more important today than ever before. Understanding the cascading effects of cyber threats on physical infrastructure assets is the centerpiece of a capability being piloted at DHS through the HITRAC's Integrated Analysis Task Force (IATF). The IATF is comprised of participants from across NPPD components, including the HITRAC Program, Cybersecurity & Communications, and Federal Protective Services.

In 2012, the IATF conducted a proof-of-concept pilot with the city of Charlotte, North Carolina. The IATF worked with stakeholders from the commercial facilities sector, the Charlotte Office of the Chief Information Officer, and the Charlotte-Mecklenburg Emergency Management Office to assess participant cybersecurity postures, and to mitigate the physical consequences flowing from exploited cyber vulnerabilities.

DHS plans to use the findings from the proof of concept to enhance its analytical tools, models, and risk methodologies to provide a greater understanding of how vulnerabilities and consequences associated with emerging threats such as cyber attacks can affect critical infrastructure assets, as well as the interdependency of physical and cyber vulnerabilities.

VALUE GENERATED FROM THE DHS INTEGRATED ANALYSIS TASK FORCE

2012 CHARLOTTE PROOF OF CONCEPT

- Open-source information can facilitate the discovery of system vulnerabilities.
- Geospatial capabilities can inform analytics and support the regional characterization of federal and local critical assets.
- Using the Cybersecurity Self-Evaluation Tool (CSET), participants noticed a significant increase in their situational awareness of cybersecurity threats.
- Participants could link identified cyber-related vulnerabilities to associated physical consequences.
- IATF analytics improved risk-based decisionmaking and mitigation planning.

LEVERAGING HITRAC ANALYTICS TO AID RESPONSE AND RECOVERY EFFORTS

Hurricane Sandy struck the U.S. Atlantic coastline in late October 2012, resulting in severe damage to more than 17 states. The storm was responsible for widespread power outages; massive damage to infrastructure, businesses, and private residences; and significant loss of life.

The DHS HITRAC provided actionable analysis for decision makers before, during, and after Hurricane Sandy.

Before the storm made landfall in the U.S., HITRAC operated 24/7 to provide impact analysis, high-fidelity consequence modeling, and a listing of infrastructure protection priorities based on predictive analytic capabilities. HITRAC produced more than 20 analytic products and updates, which were disseminated to federal, state, and local partners. During the course of Hurricane Sandy, these products were updated based on the evolving situation to help the Protective Security Advisors, FEMA, and others involved in the response better prioritize restoration efforts.

Following the storm, HITRAC provided DHS leadership with analysis of the impacts of closures of New Jersey fuel terminals and petroleum pipelines and New Jersey/New York port damage. It also supported prioritization of fuel distribution for backup power generation at specific critical infrastructure facilities, and deployed personnel to support the New York and New Jersey Joint Field Offices. During their time in the field, HITRAC representatives provided critical infrastructure analysis capabilities and supported FEMA's infrastructure recovery support function as part of the national disaster recovery framework.

ADDRESSING ECONOMIC AND NATIONAL SECURITY CHALLENGES

Private-sector organizations face a tremendous challenge in securing their classified information, proprietary data, and technology. According to the Office of the National Counterintelligence Executive, foreign adversaries are using advanced means to acquire this information to gain political, military, and economic advantage over the United States.[32] And foreign intelligence services are leveraging the placement of individuals from all walks of life in a broad range of professions to achieve their objectives: as employees at U.S. firms, students and researchers at universities, and scientists at national laboratories. Foreign intelligence service collection efforts target nearly every entity involved in classified and unclassified high-end research throughout the United States.

THE FBI's NATIONAL SECURITY BUSINESS ALLIANCE COUNCIL

The National Security Business Alliance Council (NSBAC), under the FBI Counterintelligence Division's Counterintelligence Strategic Partnership Program, is a partnership between the FBI and leading companies in the defense industrial base and IT/telecommunications sectors, whose members are the cleared Chief Security Officers from more than 30 of the top national security and IT/telecom business leaders. Together, the NSBAC and Strategic Partnership Coordinators

[32] The Office of the National Counterintelligence Executive (ONCIX), "Foreign Spies Stealing US Economic Secrets In Cyberspace", November 2011, available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

from each of the FBI's 56 field offices collaborate on measures for effectively hardening the target around technologies deemed valuable to the U.S. government. These efforts provide a first line of defense inside facilities where research and development is occurring, and where foreign intelligence services are focused; foster information exchange with U.S. Government agencies on the foreign intelligence threat; and promote use of the counterintelligence vulnerability assessment tool, which can assist the FBI and business alliance partners in identifying and mitigating vulnerabilities.

During FY 2012, Strategic Partnership Coordinators conducted more than 7,000 briefings, meetings, and presentations to promote counterintelligence awareness of economic espionage, protection of trade secrets, espionage, insider threats, and acquisition of sensitive technologies by foreign actors. In addition, the program provided nearly 4,000 Counterintelligence Vulnerability Assessments to assist cleared contractors, private businesses, and academia in conducting self-assessments of their counterintelligence programs. As a result, more than 180 organizations either created a counterintelligence program or hardened their current counterintelligence security policies and practices, and the FBI initiated hundreds of investigations and threat assessments based on information shared with the Strategic Partnership Coordinators.

PROTECTING INTELLECTUAL PROPERTY

The 2013 Joint Strategic Plan on Intellectual Property Enforcement calls upon law enforcement to improve public outreach on intellectual property matters. In FY 2012, the National Intellectual Property Rights Coordination Center, an ICE-led multi-agency coordination and deconfliction center for intellectual property investigations, conducted more than 400 trainings and outreach sessions for more than 20,000 individuals.

DOMESTIC SECURITY ALLIANCE COUNCIL

The Domestic Security Alliance Council (DSAC), a strategic partnership between the FBI, DHS, and the U.S. private sector, was established to promote the timely and effective exchange of information. The DSAC advances the FBI's mission to prevent, detect, and investigate criminal acts, particularly those affecting interstate commerce, while enhancing the ability of the private sector to protect its employees, assets, and proprietary information.

The DSAC maintains a secure web portal—www.dsac.gov—for delivery of unclassified intelligence products, contact information, training material, and other information to DSAC members. The portal is a collaborative platform that allows members to work jointly to solve common problems. The portal also includes a discussion board so that members can share information trends and best practices.

The DSAC continuing education opportunities include the Domestic Security Executive Academy (DSEA) and the Intelligence Analyst Symposium (IAS).

The DSEA, a one-week program, is a strategic outreach program for corporate chief security officers, chief information security officers, and federal law enforcement senior executives, including FBI Field Office Special Agents in Charge. In 2012, more than 40 executives, the majority from the private sector, attended the DSEA.

The IAS is a strategic training outreach program for sector-security analysts, FBI intelligence analysts, and other federal law enforcement partners. It is designed to teach analytical trade craft, share methodologies, discuss best practices, provide networking opportunities, and generate greater collaboration and cooperation. In 2012, more than 100 analysts, the majority from the private sector, attended IAS training sessions.

FBI INFRAGARD

InfraGard is a two-way information sharing exchange between the FBI and more than 55,000 members of the public and private sector. With InfraGard, the FBI has successfully recruited technology and security professionals from the private sector to assist in the protection of the critical infrastructure of the U.S. through information sharing in a controlled-access environment. InfraGard provides members access to law enforcement sensitive (LES) analytical threat products pertaining to their areas of expertise. In turn, these members assist the FBI by initiating and/or enhancing FBI investigations and intelligence products.

In 2012, InfraGard members initiated 163 FBI investigations, enhanced 435 ongoing FBI investigations, and disseminated intelligence used in 339 FBI reports to the IC. Through InfraGard activities, the FBI identified 100 U.S. banks that had been victimized by unauthorized ATM withdrawals in Romania, and as a result, 18 Romanian citizens were charged, 8 of whom were extradited to the U.S. for prosecution.

InfraGard members will soon have access, via the InfraGard network, to iGuardian, a new portal that will provide tools to mitigate and prevent serious cyber-threats, scheduled for deployment in the summer of 2013. The FBI is adding iGuardian to its Guardian program and is developing it specifically for trusted industry partners within the critical infrastructure sectors.

The InfraGard Network is scheduled to host a pilot test of the iGuardian portal with approximately 90 trusted industry partners. Upon successful completion of the pilot, a malware investigator tool will be piloted via iGuardian, adding the ability to submit suspected malware for analysis to the FBI. iGuardian is scheduled to officially become available via the InfraGard Network in July 2013. Future enhancements will include the ability to submit terrorist events, suspicious activity reports, and suspected counterintelligence espionage threats via the portal.

ALL HAZARDS CONSORTIUM

The evolving threat to critical infrastructure has stimulated the creation and maturation of a variety of trusted partnerships, whether established under government auspices or through self-organizing initiatives of private-sector partners. Through these partnerships, critical infrastructure stakeholders leverage the collective expertise of their networks to improve risk management practices for identifying and mitigating threats, as well as response and recovery efforts.

An example is the All Hazards Consortium (AHC), a 501(c)(3) non-profit organization founded in 2005 that includes representatives of all levels of government in the mid-Atlantic region, along with stakeholders from higher education, business and industry, non-profit and volunteer organizations, research firms, and trade associations. Focusing on homeland security, emergency management, and business continuity issues, the AHC's footprint represents more than 60 million citizens, a significant percentage of the nation's critical infrastructure, and more than 50% of all FEMA grant dollars issued to states, urban areas, and maritime ports in the United States.

The AHC addresses issues related to managing natural and manmade hazards by regularly hosting regional meetings and conference calls that bring government and private-sector partners together to focus on specific issues. When participants identify a common need or priority, the AHC conducts a regional workshop in cooperation with the state sponsoring the issue. The needs, issues, best practices, lessons learned, and recommendations emerging from the workshop are memorialized in a "regional consensus" white paper that serves to create awareness and to attract funding and in-kind donations to help the states address the issues at hand.

During emergencies the AHC activates its trusted relationships to assist in sharing critical recovery information between government and the private sector. For example, in the aftermath of Hurricane Sandy, the AHC realized the need to work with out-of-state entities to obtain assistance, and quickly turned to its private-sector partners to provide data, support, and services. The AHC organized this information into daily Private Sector Resource Reports, which showed potential "open and closed" locations for necessities such as fast food, fuel, hotels with available rooms, and pharmacies, and then emailed the information to tens of thousands of public and private stakeholders.

AHC believes that three key best practices make the AHC's model successful.

- It develops relationships with partners during normal operations so that in times of an event, participants comfortably and efficiently work together through established, trusted relationships.
- Consortium members identify issues collaboratively, ensuring that there is broad buy-in to the AHC agenda.

- The AHC's engagement with DHS and FEMA headquarters and the Regional Offices' technical assistance and resources maintains the Consortium's alignment with the National Infrastructure Protection Plan.

Going forward, the AHC plans to improve upon and expand its existing model to include all FEMA regional offices and emergency response units, and to develop and implement a formal multi-state planning and information sharing process.

MULTIMODAL INFORMATION SHARING

Every year, millions of tons of cargo cross our nation's land borders or arrive 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 combination of environments 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 both federal and SLTT agencies.

NATIONAL MARITIME DOMAIN AWARENESS ARCHITECTURE PLAN IMPLEMENTATION

The National Maritime Domain Awareness (MDA) Architecture Plan describes a National Maritime Information Sharing Environment (MISE) that is implemented through common data standards and architectural understanding; defines a framework that enables information sharing through use of a common vocabulary; and seeks to reduce cost by leveraging existing programs and systems. The architecture plan, implemented through the MISE, and the vocabulary, defined in the NIEM – Maritime, provides a proven, repeatable process for sharing maritime information.

The first successful evaluation of the National MDA Architecture Plan was with international partners during the 2011/2012 DoD Trident Warrior exercises. Standardized unclassified data sets were successfully shared between the United States, France, and the United Kingdom. Based on how Trident Warrior successfully facilitated the sharing of standards-based information between international partners, the National Maritime Intelligence-Integration Office (NMIO) partnered with the office of the PM-ISE to replicate the sharing of maritime data between domestic partners.

In 2012, NMIO and the PM-ISE proposed the first operational implementation of the National MDA Architecture Plan, known as the Domestic Common Maritime Picture (DCMP). The DCMP is

an unclassified, multi-agency information sharing effort in the port of Baltimore that improves maritime security and builds port partnerships. Through re-using the data exchanges successfully demonstrated in Trident Warrior, the DCMP has successfully integrated data from DoD, DHS, Department of Transportation (DOT), and the Maryland Natural Resources Police into the MISE.

The National MDA Architecture Plan has proven successful. Organizations that choose to participate in the MISE are finding that sharing information through common missions of federal, state, and local government, as well as private-sector organizations can be a low-cost, clearly-defined process. Trust and understanding will continue to grow among participating organizations as implementation of the National MDA Architecture expands. As implementation efforts expand, safety and situational awareness within ports will increase, resulting in strengthened national security.

DHS COASTAL SURVEILLANCE SYSTEM

The DHS Directorate of Science and Technology (S&T) Directorate plans to leverage existing and new sensor capabilities to give DHS a new capability called the Coastal Surveillance System (CSS). CSS is being built on a service-oriented architecture (SOA) framework and uses NIEM-Maritime standards to provide enhanced Maritime Situational Awareness by enabling affordable, persistent, and pervasive detection, classification, identification, tracking, and surveillance of afloat vessels. This system is being prototyped in partnership with the DHS Customs and Border Protection (CBP) Office of Air and Marine, at the Air and Marine Operations Center, and is being integrated with other CBP maritime domain awareness capabilities. The DHS S&T effort started in FY 2013, and will result in full operational capability in FY 2016.

AIR DOMAIN INTELLIGENCE INTEGRATION ELEMENT (ADIIE)

ODNI established an Air Domain Intelligence Integration Element (ADIIE) in May 2012 to coordinate and advocate for the Global Air Domain Community of Interest (Global Air Community) and its intelligence needs.[33] ADIIE was developed as the catalyst for enhancing intelligence integration and facilitating information sharing among all air domain stakeholders. The ADIIE Director serves as the IC's primary national-level representative for aviation-related intelligence integration and information sharing issues, and is the chair of the Organization for Economic Cooperation and Development High-Level Risk Forum, fostering the international development of risk management capabilities for, and the mitigation of, high-level risks to the air domain.

In January 2013, ADIIE completed development of a five-year strategic plan with the primary goals of developing the global air community; improving aviation information sharing; and advocating

[33] Director of National Intelligence, Air Domain Intelligence Integration Element (ADIIE) Strategic Guidance and Priorities, E/S 00462, U.S. Government, 2012

for aviation intelligence analysis. In addressing these goals, ADIIE has met with more than 250 federal, state, local, tribal, private-sector, and international organizations; has created a directory of federal air intelligence organizations;[xxxvii] is mapping the inter- and intra-organizational flow of intelligence and information across the air domain by constructing flow maps and tracking specific air domain products from production to dissemination; and is participating in the development of national intelligence priorities for air domain issues.

In addition, ADIIE is conducting two pilot projects to help SLTT law enforcement and private-sector partners eliminate barriers to air domain intelligence sharing and information exchange. Through these pilots, ADIIE will identify partner information sharing gaps and needs; work with partners to find solutions by leveraging existing resources when possible; and streamline processes for disseminating federal information and intelligence products to the SLTT community and the private sector.

AIR DOMAIN AWARENESS PORTAL

The ODNI ADIIE and the DHS HSIN-Critical Sectors engineers are developing an Air Domain Awareness (ADA) portal to provide an online venue for Global Air Domain Community of Interest interaction and information sharing across DHS's HSIN, the FBI's LEO, and the DSAC's web portal.

AIR EVENT INFORMATION SHARING SERVICE

North American Aerospace Defense Command (NORAD) and the U.S. Northern Command (USNORTHCOM) have developed a web application for tracking, collaborating, and sharing air-track and decision-support data among U.S. and Canadian joint, intergovernmental, interagency, and multinational agencies in near real time. Initially operational in December 2012, the Air Event Information Sharing Service (AEISS) is a secure, web-enabled collaboration tool designed to improve situational awareness for senior leaders and air defense and security mission partners across North America.

As of April 1, 2013, there were more than 1,300 AEISS account holders in more than 40 operations centers across the United States and Canada, with new mission partners added each day. NORAD and USNORTHCOM are currently working with the DoD CIO and the Joint Staff on sustainment of the new capability. Additionally, the CBP Office of Air and Marine's Air and Marine Operations Center and USNORTHCOM have partnered to establish a technical infrastructure to create shared air-domain awareness with Mexico. This has resulted in tactical coordination of a Mexican response to more than 400 suspect air targets approaching the U.S. border thus far in FY 2013.

SECURING THE U.S. FOOD SUPPLY AT PORTS OF ENTRY

The U.S. Food and Drug Administration (FDA) works closely with CBP to protect the public from terrorist attacks on the U.S. food supply, and to prevent food that may be contaminated with biological, chemical, or radiological agents from entering the U.S. Personnel from each organization are collocated at CBP's National Targeting Center – Cargo, where CBP provides FDA analysts with direct access to several databases and information systems[34] that are essential to carrying out the FDA's food defense responsibilities. This partnership facilitates information sharing between these organizations, and rapid response to potential vulnerabilities or threats to the U.S. food supply through the daily flow of information about imported shipments that raise concerns.

Daily reports generated by CBP allow the FDA to cross reference potential persons of concern. FDA analysts perform regular searches of CBP's Automated Targeting System for potentially high-risk food shipments, which provide the FDA with early targeting of these shipments prior to receiving filed notices. For shipments of concern, and at the FDA's request, CBP places shipments on hold under the Bioterrorism Act, giving the FDA time for further examination and analysis.

THE DHS
JOINT ANALYSIS CENTER COLLABORATIVE INFORMATION SYSTEM (JACCIS)

JACCIS is the DHS Domestic Nuclear Detection Office's (DNDO) information technology system. It receives, manages, analyzes, and reports on data from the Global Nuclear Detection Architecture (GNDA). JACCIS facilitates the sharing of radiation and nuclear detection data among mission partners, and allows users to evaluate and categorize detection events. It incorporates information from multiple sources and allows analysts to collaborate, share, and correlate data. In June 2012, JACCIS implemented a NIEM standard message router, allowing real-time system interconnections with fixed and transportable radiation portal-monitoring equipment and mobile radiation detection equipment. In February 2013, it established connection with the Department of Energy's Triage system, providing local authorities with the ability to directly elevate alarms to the national level; thereby decreasing the time required to adjudicate alarms, and providing a central repository of alarm data to facilitate trending, fusion, and analysis.

[34] These systems include TECS—formerly the Treasury Enforcement Communication System—a controlled-access law enforcement system that contains temporary and permanent enforcement, inspection, and intelligence records relevant to the anti-terrorism and law enforcement mission of CBP, and the numerous other federal agencies that it supports; Automated Targeting System - a CBP targeting system that compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments; Automated Commercial System – a legacy CBP system for processing importer data and transactions; Automated Commercial Environment - a commercial trade- processing system with rail and sea manifest capabilities, and future replacement for ACS; and the Homeland Secure Data Network.

INTERLUDE: FUSION CENTERS IN ACTION

The value of fusion centers is best seen through the successes they have had in protecting their communities, in informing decisionmaking, and in enhancing information sharing 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 CENTERS COLLABORATE TO LOCATE AND APPREHEND A WANTED FUGITIVE

In January 2013, Alaska State Troopers informed the Alaska Information Analysis Center (AKIAC) that a fugitive wanted for multiple felony charges in Alaska, including sexual assault, kidnapping, and assault, was at large and may have departed the state. Working with the TSA, AKIAC analysts determined that the subject had departed Anchorage on a commercial flight and was currently en route to Memphis via Minneapolis. Coordinating through the Tennessee Fusion Center (TFC) and the Memphis TSA, the AKIAC worked directly with the Memphis International Airport Police Department, providing an extraditable warrant and National Crime Information Center (NCIC) information concerning the subject. Within two hours of AKIAC's notification, the subject was in custody at the Memphis International Airport Police Department.

This example demonstrates the importance of connectivity between the National Network of Fusion Centers and their federal, state, and local partners. Through the sharing of information in real time, these partners were able to locate and apprehend a wanted fugitive.[xxxviii]

FUSION CENTER COORDINATES NEW JERSEY HURRICANE SANDY DISASTER RESPONSE

Prior to and throughout Hurricane Sandy, the New Jersey Regional Operations and Intelligence Center (ROIC) and New Jersey's State Emergency Operations Center used the ROIC's systems and networks to issue detailed situation reports with up-to-the-minute information about the locations of shelters, road closures, the status of public transportation vehicles, and the overall state of the disaster. Following the storm, the ROIC provided updated law enforcement-related information, maps, and other general public safety information—valuable data used in the protection and rehabilitation of communities severely impacted by the storm. Through the chiefs of police network, New Jersey ROIC personnel were deployed into the field and began the process of

collecting information related to the condition of various municipal government buildings and other infrastructure. The reports were developed to share with FEMA and the U.S. Army Corps of Engineers to assist with prioritizing recovery efforts.[35, xxxix]

FUSION CENTER SUPPORTS THE OAK CREEK SIKH TEMPLE ACTIVE SHOOTER INCIDENT

In August 2012, the Southeastern Wisconsin Threat Analysis Center (STAC) and its host agency, the Milwaukee Police Department (MPD), provided analytic support in response to the Oak Creek Sikh Temple active shooter incident. Members of the STAC and the Joint Intelligence Operations Center (JIOC) determined that the suspect was a known affiliate of a white supremacist group, and the shooting was handled as a domestic terrorism matter by the FBI's Milwaukee Division, which assumed the investigative lead. Both the FBI and MPD relied on STAC's intelligence and investigative support throughout the incident. The STAC led development of joint FBI fusion center products to further share information regarding the event, and leveraged the expertise from across the National Network to identify any additional leads or information pertaining to the suspect and the incident. Following the incident, the STAC infrastructure and training personnel provided recommendations for instituting a security framework for other infrastructure in the area and led efforts to raise awareness of threat indicators, including the importance of reporting suspicious activity to the proper law enforcement authorities.[xl]

FUSION CENTERS SUPPORT MONEY LAUNDERING INVESTIGATION

In July 2012, a South Dakota law enforcement officer discovered, during a traffic stop, that two foreign nationals were in possession of more than 100 stored value cards and a credit card reader. This raised suspicions because criminal organizations are known for stealing credit cards or credit card numbers and transferring money from them to stored value cards in order to circumvent customs reporting requirements. The officer reported this to the South Dakota Fusion Center (SDFC), which conducted state and federal records checks in coordination with the North Dakota State and Local Intelligence Center (NDSLIC) and Immigration and Customs Enforcement (ICE). Records revealed that the individuals were identified in an active ICE transnational organized crime money laundering investigation involving stored value cards. The SDFC and NDSLIC were able to inform ICE of the officer's report, which was used to document the suspects' involvement in the ongoing criminal investigation.[xli]

[35] Additional detail about the ROIC's role in supporting Hurricane Sandy is located at http://ise.gov/blog/col-rick-fuentes/fusion-center-coordinates-new-jersey-hurricane-sandy-disaster-response

FUSION CENTERS COLLABORATE TO SUPPORT ARREST OF INDIVIDUAL CHARGED WITH PRODUCTION OF CHILD PORNOGRAPHY

In June 2013, several phone calls across the Southeastern United States were made from a telephone belonging to an individual wanted for production of child pornography by an ICE office in Fort Lauderdale, Florida. ICE provided details of the wanted individual to the Central Florida Intelligence Exchange (CFIX) in Orlando and asked them to widely disseminate the information. Based on the location where the phone calls were being made, the CFIX notified the Tennessee Fusion Center and the Georgia Information Sharing and Analysis Center that the suspect might be in their area. These partners subsequently notified all relevant local law enforcement agencies in their area of responsibility. As a direct result of this interstate information sharing, the suspect was located and arrested by the Georgia State Patrol.

This page intentionally left blank.

SECTION 2:

INFORMATION DISCOVERY AND ACCESS THROUGH COMMON STANDARDS

This section addresses the progress of ongoing efforts and new initiatives in the areas of information discovery and access. As defined in the 2012 National Strategy for Information Sharing and Safeguarding (National Strategy), discovery and access are two distinct concepts, in which discovery is the user's ability to *identify* the existence of information, and access is the user's ability to *retrieve* it.

The efforts of ISE mission partners and PM-ISE on fundamental elements of discovery and access are examined, to include data-level tagging; data aggregation; development and incorporation of interoperable, industry-accepted technical standards for information sharing solutions; and standards-based acquisition. Those activities that are identified as priorities in the National Strategy are noted in the following pages.

The following list of findings highlights accomplishments and opportunities for improvement. Further detail is provided in the following pages.

ACCOMPLISHMENTS

- Department of Homeland Security (DHS) launched the Enhanced Overstay Vetting and Biographic Exit Project, which seeks to increase DHS's capability of identifying immigration violators and prioritizing them for enforcement;
- The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division expanded the capabilities of the Law Enforcement National Data Exchange (N-DEx) to accommodate more records and users, and to share investigative reports in near real time with criminal justice partners;

- The Department of Defense (DoD) is adopting National Information Exchange Model (NIEM) as the best option for standards-based data exchanges;
- The PM-ISE initiated and resourced an integrated project with DHS and the Open Geospatial Consortium (OGC) to use NIEM in enabling geospatial data to be discoverable, retrievable, and usable across the ISE by any standards-conformant map viewer;
- The Object Management Group (OMG) officially approved the NIEM-Unified Modeling Language (NIEM-UML) profile as an OMG specification, opening the door for organizations to use NIEM-UML to simplify modeling in their architecture frameworks;
- The IJIS Institute "Springboard Team" conducted its first standards conformance test to determine whether a commercial data exchange met required interoperability standards; and
- The PM-ISE is supporting a pilot project on an open-source implementation of the NIEM-UML Profile which will accelerate innovation and further streamline the development of NIEM-based functional standards.

OPPORTUNITIES

- In the previous reporting period, 65% of agencies reported little or no progress in working towards metadata tagging solutions. Since June 2012, ISE agency initiatives designed to address this include the use of DoD Architecture Framework (DoDAF) artifacts to enable cross-domain sharing by both the DoD Joint Information Environment and the Intelligence Community Information Technology Enterprise (IC ITE), and the work of DHS and DOT to develop data-tagging implementation plans for discovery and access control on their networks.
- Last year's report found that centralized data correlation and data storage introduces privacy and security challenges that limit mission effectiveness; that finding is still valid. To address this, the National Strategy is prioritizing the development of a data aggregation reference architecture; the adoption of metadata standards to facilitate discovery, access, and monitoring across networks and security domains; and the definition and implementation of common standards to support automated discovery and access decisions. ISE activities that address these objectives are detailed in this section of the Report and in Section 3.
- Agency responses to the 2013 ISE Performance Assessment Questionnaire (PAQ) show that about 50% of ISE agencies consider ISE functional and technical standards when issuing grants or RFPs for ISE-related systems. While implementation guidance actions were issued for updating grant and acquisition language to support the use of common standards, 43% of agencies have not provided best-practice recommendations to support this initiative. PM-ISE is working with General Services Administration (GSA) to leverage National Strategy implementation actions to accelerate the use of information sharing standards in acquisition language, and to foster reuse of these standards across the ISE mission partners. Health and Human Services (HHS), as co-chair of the Council on Financial Assistance Reform, will work

with the Office of Management and Budget (OMB) to develop standard guidance for the grants and financial assistance community.

STANDARDS GOVERNANCE

ISA IPC STANDARDS WORKING GROUP, AND THE STANDARDS COORDINATING COUNCIL

As noted in previous reports, the ISA IPC Information Integration Sub-Committee (IISC) Standards Working Group (SWG) facilitates standards development and reuse by using a whole-of-government approach that fosters interoperable information exchanges between the Federal Government, state, local, tribal, and territorial (SLTT) government agencies, private-sector partners, and foreign partners and allies.[xlii] By adopting common technical standards and forming consensus on common frameworks, ISE partners can 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)[36] supports the ISA IPC Standards Working Group (SWG) in these efforts by representing the private sector's perspective in addressing the challenges of coordinating and influencing information sharing standards and initiatives.

SCC partners, OMG, and the IJIS Institute hosted the second annual Workshop on Information Sharing & Safeguarding Standards (WIS^3) in March 2013. WIS^3 brought together government, standards development organizations, and industry partners to exchange ideas about the present and future of information sharing. The challenges and solutions addressed include:

Common Information Exchange Models, and the role that these models play in enabling information interoperability, including how adoption of standards like NIEM can help overcome the challenges of standards certification and common frameworks;

Frameworks and Shared Services, and how service-oriented architecture (SOA), reference architecture patterning, and cloud computing enable information sharing;

Designing Privacy Protection into Policy to ensure that privacy policies accompany data during exchanges and aggregation, and to make privacy protections machine readable and standardized; and

Cybersecurity Information Sharing efforts to develop an information sharing framework for cybersecurity events.

[36] The SCC comprises 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). 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.

STANDARDS IMPLEMENTATION

The National Strategy states that departments and agencies have an obligation to make information available to any agency, department, or partner with a relevant national security mission, and to manage that information in a manner that is lawful while ensuring the protection of privacy, civil rights, and civil liberties. To do this across the ISE, agencies must define and adopt common standards to support automated policy-based discovery and access decisions.[37]

The ISA IPC SWG coordinates and oversees the government-wide adoption of these common standards for the ISE. Most importantly, the work done within ISE agencies and communities to identify, develop, and implement common standards ensures that mission-dependent information sharing capabilities are interoperable from the outset. Examples of agency standards governance bodies include:

The FBI's Advisory Policy Board (APB) and Technology Development and Deployment Board (TDDB) serve as authoritative bodies for standards development and ISE Technical Standards adoption, respectively;

The DoD CIO Executive Board oversees the DoD Standards Program, which develops and adopts standards for the Department;

The National Geospatial-Intelligence Agency's (NGA) Geospatial Intelligence Standards Working Group (GWG) is a National System for Geospatial-Intelligence (NSG) community forum for geospatial standards;

The Bureau of Justice Assistance's Global Standards Council; and

The NIEM Executive Steering Council, on which DHS, Department of Justice (DOJ), and the HHS are represented.

These agency standards-governance bodies, and others like them, inform and are informed by the government-wide standards implementation initiatives overseen by the ISA IPC. Currently, 93% of agencies that responded to the 2013 ISE PAQ report incorporating ISE Technical Standards into their enterprise architectures and IT capabilities.[xliii]

NATIONAL INFORMATION EXCHANGE MODEL (NIEM)

NIEM provides a common vocabulary and supports enterprise-wide information exchange standards and processes that enable agencies throughout the nation to effectively share critical information in emergency situations, as well as to support day-to-day operations. Today, all 50 states and 20 federal agencies are committed to using NIEM in some capacity, and at some level of maturity. The value of NIEM is demonstrated every day across the country as it facilitates

[37] National Strategy Priority Objective 8.

information exchanges to improve public safety, as well as health, human, and social services, and to strengthen homeland security.

Work on the newest version of NIEM—NIEM 3.0—began in August 2012. Driven by requirements to support information exchange between an ever expanding number of domains, including Biometrics; Chemical, Biological, Radioactive, and Nuclear (CBRN); Children, Youth, and Family Services (CYFS); Justice; Maritime; and Immigration and Screening, development activities are being reviewed by these communities with a planned release date scheduled for the fall of 2013.

NIEM UNIFIED MODELING LANGUAGE (NIEM-UML)

The NIEM Unified Modeling Language (NIEM-UML) is a developing industry standard designed to help organizations implement information exchanges across systems, agencies, and levels of government by giving them a visual understanding of what it means to be NIEM-conformant. UML allows organizations to use a blueprint-like model to adopt and incorporate NIEM-based information exchanges—making NIEM implementation less technically demanding.[xliv]

In September 2012, the OMG, whose members include hundreds of organizations, including virtually every large organization in the technology industry, officially approved the NIEM-UML profile as an OMG specification.[xlv] This opens the door for organizations like the DoD to use NIEM-UML to simplify modeling in their architecture frameworks. Audiences with varying degrees of familiarity with NIEM technical concepts can also create variations of existing NIEM exchange packages that interoperate with other NIEM models.

In addition, the PM-ISE is supporting a pilot project on the development of an open-source implementation of the NIEM-UML Profile, which will impact the development of NIEM-based functional standards, leading to interoperability between ISE agencies and mission partners.[xlvi] The two principal deliverables will be an open- source codebase that will enable tool developers to implement the NIEM-UML profile, and a tool that will enable users to automatically produce NIEM-conformant specifications using UML. These tools offer users a pre-harmonized vocabulary that is supported by the community and will ensure that all users derive the same meaning from data elements, a critical factor in achieving interoperability.

DOD ADOPTS THE NATIONAL INFORMATION EXCHANGE MODEL (NIEM)

In March 2013, the DoD CIO announced that in compliance with White House guidance on the adoption of reference information exchanges, DoD will adopt NIEM for standards-based data exchanges, and will work with the NIEM Program Management Office to create a Military Operations (MilOps) Domain as part of NIEM.[xlvii]

The Office of the DoD CIO will lead the development of a DoD Data Framework, which will provide guidance on governance, and technical direction for NIEM adoption. The DoD Data Framework will build upon the existing DoD data strategy, and will provide principles, rules, and additional guidance for managing data in a way that enables information sharing.

The DoD transition to NIEM will incorporate the ongoing efforts of DoD Universal Core (UCore) and Command, and Control (C2) Core. The DoD CIO will no longer support the development of further enhancements to UCore and C2 Core as unique DoD data exchange models, but the applicable data components in UCore and C2 Core will form the initial content in the NIEM Core and the NIEM MilOps domains, respectively.

NIEM BIOMETRICS DOMAIN

The NIEM Biometrics domain was formally established in July 2012 to support biometric-related services and mission-based activities, such as homeland security, national defense, border management, immigration benefits, and global law enforcement, through the joint development and alignment of Biometric Standards. Built upon the early foundations of the DOJ Law Enforcement Information Sharing Program (LEISP), and operating under the stewardship of the DHS Office of Biometric Identity Management (OBIM), the Biometrics domain will support information sharing; establish data-exchange standards; and promote interoperability between federal agencies, SLTT government agencies, private-sector partners, and foreign partners and allies, utilizing biometric data and information. With the establishment of the Biometrics domain, members of the biometric community of interest will have the tools and a formally governed, common forum to ensure that biometric data is discoverable and retrievable by ISE mission partners.[xlviii]

DHS NIEM CYBER INCIDENT-SHARING PROTOTYPE

DHS has sponsored a NIEM cyber-incident information sharing prototype to understand what data, tools, and techniques are necessary to enable cyber-incident information sharing across the Federal Government, SLTT government agencies, private-sector partners, and foreign partners and allies. The first phase of the prototype, conducted from May to August 2012, exchanged cyber-incident data based on a NIEM message header, the MITRE Corporation's Structured Threat Information eXpression (STIX)™ schema, and used a central repository hosted at Johns Hopkins University Applied Physics Lab. This phase of the prototype demonstrated how a centralized, trusted broker can facilitate a cyber-incident information exchange between multiple sites.

The second phase, conducted from September 2012 to March 2013, focused on controlling data access by using Personal Identity Verification (PIV) attributes and a Backend Attribute Exchange (BAE) across the enterprise for authentication.[xlix] Data owners used a NIEM-based common data-

tagging tool to tag data fields and to document the classification of the cyber incident. Data consumers, using a browser application, could search for and, based on their PIV credentials, access shared cyber incidents. The second phase demonstrated how data owners can control access to cyber incident information that is in distributed databases across the ISE.

USING NIEM TO SHARE INFORMATION BETWEEN THE DEPARTMENT OF DEFENSE AND THE DEPARTMENT OF VETERANS AFFAIRS

In the fall of 2012, the PM-ISE and the DoD initiated a pilot project using NIEM-UML-based tools to develop a NIEM Information Exchange Package Documentation (IEPD) for the DoD and the Department of Veterans Affairs (VA) to share electronic records of candidates undergoing the recruitment process for military service. The pilot involves secure collaboration between the U.S. Military Entrance Processing Command, the Office of the Deputy Chief Management Officer, and the Office of the Under Secretary of Defense for Personnel and Readiness. The pilot is nearing completion, and the lessons learned will be used as the foundation for future NIEM-based data exchange between DoD and the VA.

STANDARDIZING COUNTRY CODES ACROSS FEDERAL DATABASES

NGA, in its role as the geospatial intelligence functional manager,[38] is leading the Country Codes Working Group, a Federal Government forum that is coordinating the transition from the use of the two-character country codes defined in the Federal Information Processing Standard (FIPS) 10-4 to the three-character Geopolitical Entities, Names, and Codes (GENC) standard found in International Standards Organization (ISO) 3166. The transition to the new standard will impact all federal systems and standards that contain or include country identifiers. Most, if not all, ISE systems will be impacted by the transition. This new standard is crucial for enabling simplified discovery and retrieval of geographically-coded information by analysts and investigators across multiple databases.[i]

OPEN GEOSPATIAL STANDARDS

In order to be usable across all ISE communities, geospatial data must be standards-based, interoperable, and usable by any geospatial map viewer. The DHS Geospatial Concept of Operations identifies OGC and the use of NIEM as best practices for geospatial information sharing, and the National Level Exercise (NLE) 2012[39] validated the importance of standards-based interoperability for geospatial data—the general conclusion being that "mapable" data should be

[38] EO 13470, July 2008

[39] National Level Exercise (NLE) 2012 is part of a series of congressionally-mandated preparedness exercises designed to educate and prepare participants for potential catastrophic events.

discoverable, retrievable, and usable by any authorized user, using any standards-conformant map viewer.

In an effort to make data "mapable," the PM-ISE initiated and resourced an integrated project with the DHS NIEM Program Management Office (NIEM PMO), the DHS Office of Science and Technology, and the OGC, to enhance the NIEM architecture for the geospatial domain by developing, testing, and documenting embedded Geospatial Markup Language (GML) architecture reference guidance.

The OGC Interoperability Program initiative[40] objectives, referred to as Geo4NIEM, include developing NIEM-compliant geospatial standards and naming conventions; testing and demonstrating these standards and conventions with ISE community partners; and developing recommendations for the inclusion of a Geospatial Domain within NIEM. This initiative is designed to foster broader community adoption of NIEM across the geospatial community.

STANDARDS-BASED ACQUISITION FOR INFORMATION SHARING

The success of the ISE requires the consistent use of interoperable standards in the products and services that ISE organizations acquire. Effective information sharing requires employing the decentralized, distributed, and coordinated approach outlined in IRTPA. New technology is driving changes in infrastructure operations, including cloud, mobile, and SOA solutions.

Agencies are focusing on controlling costs, avoiding duplication, and sharing services. 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.

As a result, the PM-ISE is working with the ISA IPC's SWG and SCC to reevaluate 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.[li]

There is general movement across the ISE to employ standards requirements for contracts, indicating movement toward an information sharing culture. More than 60 standards development organizations were identified, 9 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 are still mandated.

[40] http://www.opengeospatial.org/standards/requests/98

Other 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 will be incorporated into the ISE Common Information Sharing Standards Manual updates.

In addition, last year's report included the PM-ISE and GSA sponsored initiative, through the American Council for Technology – Industry Advisory Council (ACT-IAC), to provide an industry perspective on standards-based acquisition. That initiative resulted in an ACT-IAC White Paper, "Responsible Information Sharing: Engaging Industry to Improve Standards-Based Acquisition & Interoperability," which identified the following findings on the use of ISE Interoperability standards:

- Focus on streamlining governance for interoperability standards. A repeatable standards-governance process is necessary to define interoperability requirements and coordinate standards development activities across mission areas and governmental jurisdictions.
- Develop a standards roadmap. In order to encourage adoption of interoperability standards, the government needs to clearly describe its target vision for how interoperability will be achieved and the standards that will enable it.
- Leverage standards conformance testing and pilots to minimize risk. Reusing standards that have been developed collectively, tested for standards conformance, or piloted within a certain mission area or IT platform will minimize risk.
- Incorporate standards requirements into all strategic management processes. Beginning with strategic planning, government's interoperability standards requirements need to be clearly defined and the potential return on investment from using standards needs to be captured.
- Enhance training and outreach. Enhancing training and improving outreach with industry and other stakeholder groups will garner greater dividends and help ensure results.

This joint effort with GSA was further refined with the release of the National Strategy, which details the need to "leverage collective demand through acquisition," as one of 16 priority objectives. Working with GSA, PM-ISE intends to use the analysis of agency-specific use of technical standards, the ACT-IAC White Paper, and the results from pilot programs to accelerate the use of information sharing standards in acquisition and grant language, and to foster reuse of standards. The recommendations from these efforts will be captured in a final report to be presented to policy makers.

PM-ISE is also participating in the Integrated Justice Information Systems (IJIS) Institute's Task Force on Procurement Innovation—an effort between government, industry, and academia that

will look at the challenges facing state and local police procurements. The purpose of the Task Force is to define the scope and priority of procurement issues relevant to improving the entire procurement process. It will take a national perspective, to include federal, state, local, tribal, and territorial programs, in order to define the context of "national" guidelines.

This Task Force will:

- Prepare a comprehensive catalogue of prevailing practices in each of the sectors so that members of the task force may intelligently review what is good and what is bad about existing approaches to procurement.
- Identify areas within current practices that members of the Task Force believe are contributing to less-than-optimal performance results.
- Specifically examine the role that nationally accepted technology standards may play in improving procurement practices.
- Specify additional steps needed to develop acceptance for procurement.
- Recommend a framework within which further development of a "best practices" guide can be developed and promoted to the entities involved in both the public and private sector.

The result of this Task Force may be the creation of an IJIS Institute Advisory Committee on Procurement Initiatives. In this event, the Task Force will work with the IJIS Institute to develop the charter, and recommendations on how the committee should be structured.

DATA AGGREGATION

The vision for Data Aggregation is to promote a whole-of-government data stewardship approach among mission owners (data producers) to allow the collective national security enterprise to discover cross-agency connections in real-time and to drive mission results, while ensuring that proper safeguards are enforced. The mission to disrupt terrorist acts before they occur is enabled by finding, sharing, and collaborating on interpreting 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 necessary to perform their missions through shared ISE enterprise services, while protecting the privacy, civil rights, and civil liberties of persons for whom no nexus to terrorism exists.

Key to enabling access and dissemination of aggregated data within the ISE is 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, civil rights, and civil liberties associated with the sharing of aggregated data are mitigated. The National Strategy identifies data aggregation, or enterprise-wide data correlation, as a goal, and several ISE agencies are implementing solutions.

DATA EXCHANGE TOOL KIT

DHS, the National Counterterrorism Center (NCTC), and two other members of the intelligence community (IC) began a data-exchange pilot program, sponsored by PM-ISE and supported by the ISA IPC Data Aggregation Working Group (DAWG), to improve interagency, person-centric information exchanges, and to highlight best practices and lessons learned. Year One of the pilot was completed in September 2012. The participants were successful in improving the consistency, timeliness, and quality of the exchanges of data produced by DHS and consumed by two members of the IC.[lii]

The team established a performance baseline for each exchange and created a NIEM-Extensible Markup Language (XML) sample data set for testing each exchange. The processes and templates developed in the pilot, along with lessons learned, were documented in the Data Exchange Toolkit, which provides comprehensive templates, guidelines, and documentation for data exchange, and highlights best practices and lessons learned. The Toolkit is available online at http://www.ise.gov/building-blocks.

In October 2012, the DAWG and DHS kicked off Year Two of the pilot, which is aimed at validating, refining, and re-using repeatable processes and tools to improve High-Valued Data Set (HVDS) exchanges across the ISE. The second-year goals, scheduled to be completed in September 2013, are to improve [two interagency, person-centric information exchanges], using NIEM for exchange services; to perform an information-exchange assessment using the Data Exchange Toolkit developed during Year One, in order to identify exchange improvement areas involving high value data; and to provide enhancement capabilities for processes developed in the previous pilot year to extend the impact and address a two-way information exchange.[liii] The use of NIEM, along with a strong performance management approach, will allow DHS and the DAWG to demonstrate improvements in information sharing using clear performance metrics.

DATA AGGREGATION CAPABILITY UPDATES AND SUCCESS STORIES

LAW ENFORCEMENT NATIONAL DATA EXCHANGE (N-DEX)

The FBI Criminal Justice Information Services (CJIS) Division's National Data Exchange (N-DEx) is the first and only national investigative information sharing system. N-DEx provides federal, state, local, and tribal criminal justice agencies with a secure mechanism for searching, linking, analyzing, sharing, and collaborating with partners in interpreting more than 180 million records spanning the criminal justice lifecycle. Over the past six months, N-DEx has enjoyed growth in both sharing and usage, experiencing a 20% increase in searchable ingested records; a 4% increase in contributing agencies; a 57% increase in total available system users;

and an 8% increase in average weekly searches. During 2012, the number of registered N-DEx users more than tripled.

N-DEx development is strategically aligned with the evolving needs of the criminal justice community, and in 2012 expanded system capabilities to accommodate records and users from probation, pre-trial services, parole, corrections, district attorneys, courts and magistrate offices, custodial facilities, regional dispatch centers, and prosecutors' offices. Several state Departments of Corrections are now sharing data with N-DEx, including Indiana, Kansas, Nebraska, and Mississippi. Also in 2012, the FBI began sharing its investigative reports in near real-time with its criminal justice partners via N-DEx.[liv]

DATA INTEGRATION AND VISUALIZATION SYSTEM (DIVS)

The FBI continued to implement a single, secure, web-based search and analysis capability called the Data Integration and Visualization System (DIVS), which imports electronic data from Sensitive But Unclassified/Controlled Unclassified Information (SBU/CUI) networks belonging to other government agencies. DIVS also provides an interface with internally produced data from FBI SBU/CUI networks. DIVS allows FBI agents and intelligence analysts to "connect the dots" to determine the identities and intentions of terrorists and other threats to the nation through the use of FBI and other agency data.[lv]

> In National City, CA detectives were investigating a missing person case that had been open for two years. After receiving access to N-DEx, a National City Police Department investigator searched the missing person's name in the system. N-DEx returned results indicating the person had been arrested and was incarcerated in a neighboring county. After confirming the information with the correctional institution, the name was removed from the police department's database as a missing person. N-DEx was instrumental in locating the missing person, closing the case, and freeing up resources for active cases.

The FBI met major milestones for its agents and analysts supporting ISE-related missions to use shared data from other government agencies by completing the migration of DIVS to the FBI Consolidated Data Centers; ingesting all critical Investigative Data Warehouse (IDW) data sets into DIVS, retaining validated IDW user functionalities; exceeding the target number of data sets into DIVS, bringing up the total number from 51 to 74; increasing the DIVS record capacity from three to four billion records through the addition of new server hardware and software purchases; and increasing usage to 1,901 users per day.

Among the upgrades are a single interface to common data collections, and the merger of single-search Foreign Intelligence Surveillance Act data. Another key feature for IDW users is the switch to the DIVS single sign-on process. DIVS access is seamless through an employee's desktop login—there is no separate log-in screen. As a result of the DIVS-IDW merger, analysts have easier access and greater visibility into geospatial and analytic tools.

Other tools that allow searching of imported data and reports have been reused and placed under the DIVS user interface. These include Specialized Search Tools for Financial Crimes Enforcement Network Suspicious Activity Reports (SAR); Consular Consolidated Database (CCD); Student Exchange and Visitor Information System (SEVIS); I-94 Arrival/Departure Records; and Suspicious Activity Report Batch Analysis Review (SARBAR).

Going forward, all data access will be tied to an attribute-based access control (ABAC) solution, which DIVS will be prepared to enforce. Perhaps the most critical, far-reaching outcome from the merger is the organizational focus DIVS brings to enterprise data management, enabling the FBI to build a better data-sharing environment for internal and external government stakeholders.

IDATA: BRINGING FBI SYSTEMS TOGETHER

The FBI Intelligence Data Association and Tagging Application (iDATA) is a data management and tagging tool designed to standardize, manage, relate, and deliver key FBI data sets by providing an authoritative central repository that utilizes common standard data elements such as Crime Problem Indicator (CPI), Case Classification, and Country codes, as well as FBI and U.S. IC collection requirements used within the intelligence lifecycle.

iDATA provides data managers with an intuitive web application, web services, and user interface that allows them to manage content flow between intelligence systems. The web services also provide enterprise-wide user search results of tagged collected intelligence with uniform data values. iDATA Release 1.3.1 has been deployed to the enterprise with a current pilot group review of web service search capabilities. Interface testing is expected to be completed by the end of the 4th quarter of FY 2013.

DHS-ENHANCED OVERSTAY VETTING AND BIOGRAPHIC EXIT PROJECT

In April 2013, information systems owned by several DHS components went live with modernization efforts that were developed under the Enhanced Overstay Vetting and Biographic Exit Project. This project seeks to increase DHS's capability to identify immigration violators and prioritize them for enforcement, with a focus on those who represent the greatest national security or public safety risk. The connections from the National Protection and Programs Directorate (NPPD), the Office of Biometric Identity Management's (OBIM) Arrival Departure Information System (ADIS); the Customs and Border Protection (CBP) Targeting and Analysis Systems Program Office's (TASPO) Automated Targeting System (ATS), and ICE's Counterterrorism and Criminal Exploitation Unit's (CTCEU) LeadTrac were upgraded from batch files processed via email to secure and fully automated interfaces.

The upgraded interfaces increased the accuracy and efficiency of lead generation and automated lead vetting. Part of this was achieved by updating the interface between ADIS and the Student & Exchange Visitor Information System (SEVIS), which is owned by ICE's Student & Exchange Visitor Program (SEVP). This update allowed a drastic increase in the efficiency of generating overstay leads based on SEVIS data, in addition to increasing the amount and relevancy of data displayed in ADIS's user interface. Concurrently, TASPO developed a new user interface for CTCEU analysts to use when manually vetting overstay leads. This interface aggregates data from several source systems in one location, saving analysts' time by reducing the number of manual queries they have to initiate.[lvi] CBP, ICE, and OBIM are currently developing the next phase of upgrades to this system to further increase the data quality, efficiency, and the quality of analytical tools for the national security overstay mission.

DHS COMMERCIAL TARGETING ANALYSIS CENTER (CTAC) DATA MASH-UP

CTAC is a multiagency fusion center that leverages the expertise of CBP and partner agency personnel for the purpose of targeting commercial shipments of high-risk commodities that pose a threat to the health and safety of the American public. The Center employs a six-step risk mitigation strategy during which it identifies risk; establishes a scope of targeting; systematically targets the risk; initiates cargo examination (in coordination with field resources); reports findings; and evaluates the results/effectiveness of the targeting.

The CTAC Data Mash-Up is a database that was created to assist DHS's CBP targeting efforts on behalf of partner agencies by better measuring targeting effectiveness. This required effective downstream results-reporting from multiple Federal Government systems. Mash-Up extracts information from various CBP and Consumer Product Safety Commission (CPSC) systems, in order to present targeting results in a cohesive stream of actions and events. This allows for effective analysis and tracking of results, which translates into better targeting decisions and reduced impact on trade flows into the United States. The information sharing capacity authorized under the CTAC Memorandum of Understanding (MOU) provides for the sharing of information between partner government agencies in order to make this program a success.

Evidence of CTAC's success can be seen in its efforts to prevent illegal imports of vehicles that violate National Highway Traffic Safety Administration (NHTSA) safety standards and EPA regulations. CBP has coordinated with the Environmental Protection Agency (EPA) and NHTSA—two agencies with regulatory authority over vehicles—to ensure that unsafe vehicles from overseas markets do not reach U.S. roadways. These three agencies have combined resources at CTAC to share data, analyze import trends, and conduct joint risked-based targeting, resulting in the seizure of dozens of illegal vehicles since October 2012.

DATA AGGREGATION CHALLENGES AND NEXT STEPS

The current state of data aggregation will soon undergo transformation as a result of three major trends: ongoing budgetary constraints; increased data complexity; and safeguarding requirements. The National Strategy is influencing this transformation by providing a framework for implementing a data aggregation reference architecture; identifying gaps and dependencies; and aligning with other ISE services such as discovery, access, and data tagging.

The data aggregation community is feeling the impact of budgetary constraints. The development of new projects is competing with mission priorities, leading to fewer technical resources available for transformation projects. As directed by the National Strategy, the DAWG will work to address these challenges over the next several years. The DAWG has begun building the framework for an architecture that enables communities of data owners to share information that has already been correlated for a specific mission need, and the services needed to interoperate with a larger community of data consumers, and has released a vision paper that describes the framework, services, and data required for interoperability.

In the summer of 2013, the DAWG will sponsor a government Data Aggregation Summit of system and data architects. The goal is to codify the vision for data aggregation and the value of a strategy that emphasizes sharing correlated data between departments and agencies rather than raw data. Following the summit, the DAWG will engage industry in soliciting input on architectural solutions that might help industry better understand government requirements.

Building on the success of the data aggregation pilot in 2012, a second pilot will be completed in September 2013 between the Department of State, DHS, and NCTC, to automate some manual processes in the Electronic System for Travel Authorization (ESTA) vetting process, using common standards and exchange methods. This pilot will influence the final reference architecture framework and will implement real-life improvements in the current process.

INTERLUDE: TESTING STANDARDS-BASED COMPLIANCE AND CONFORMANCE – IJIS SPRINGBOARD

Sponsored by PM-ISE and the DOJ's Bureau of Justice Assistance (BJA), and managed by the Integrated Justice Information Systems (IJIS) Institute, IJIS Springboard is a standards-based interoperability program designed to advance justice, public safety, and homeland security information sharing. The program provides an environment in which industry and government can cooperatively evaluate standards and certify that industry products are standards-compliant through a conformance management process.[lvii]

Based on lessons learned from the Open Geospatial Consortium's (OGC) Interoperability Program, Springboard strives to create a governance structure and process whereby industry can use government-approved standards in a consensus-based "open" standards implementation process, and can leverage existing technologies to accelerate information sharing.

SPRINGBOARD CERTIFIES FIRST PRODUCT

In December 2012, the IJIS Institute Springboard team conducted its first standards conformance test to determine whether a new Prescription Drug Monitoring Program (PDMP) Information Exchange (PMIX) met the required interoperability standards, using a web-based program that collects, analyzes, and reports information on the prescription, dispensation, and use of prescription drugs. Many states currently report problems with "pill mills"—doctors who prescribe large quantities of painkillers to people who do not need them medically—and the sharing of information about prescription drugs is one way to reduce prescription drug abuse.

Going forward, the IJIS Institute is prepared to test other standards through the Springboard program, in order to ensure conformance to the national standards for companies that create information sharing products for use in the areas of public safety and criminal justice. These standards not only improve information sharing across states, but they can save organizations and taxpayers money by ensuring that organizations (pharmacies, police departments, prisons) that use information products that conform to standards do not create a new solution every time they want to share data.

SECTION 3:

OPTIMIZING MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY

This section addresses ISE initiatives that are focused on sharing services and achieving interoperability across networks and security fabrics to enable efficiency, reduce duplication, and improve mission success. These activities are in many ways dependent upon and closely aligned with the adoption and implementation of common standards discussed in Section 2 of this Report and, as the standards activities rely upon the work of the ISA IPC Standards Working Group (SWG), the interoperability activities detailed in this section depend upon the ISA IPC's Information Integration Subcommittee (IISC) to provide oversight and governance through the Assured Sensitive but Unclassified (SBU) Network Interoperability Working Group and the Identity Federations Coordination (IFC) Working Group. Chaired by the Federal Bureau of Investigation (FBI) and the General Services Administration (GSA), respectively, these groups are carrying out the implementation activities for much of the interoperability objectives of the National Strategy for Information Sharing and Safeguarding (National Strategy).

The following list of findings highlights accomplishments and opportunities for improvement. Further detail is provided in the pages that follow.

ACCOMPLISHMENTS

- The ISA IPC Data Aggregation Working Group (DAWG) is developing a reference architecture framework to provide technical guidance to assist departments and agencies as they make decisions about developing interagency data-sharing requirements;
- The GSA Federal Identity Credential and Access Management (FICAM) Program Office is leading the implementation of the FICAM Roadmap across all security domains;

- The PM-ISE is coordinating an interagency effort with Department of Homeland Security (DHS), the Department of Interior (DOI), the National Geospatial Intelligence Agency (NGA), and the Department of Commerce (DOC) to develop a Geospatial Interoperability Reference Architecture (GIRA) in order to foster the reuse of geospatial services, reduce their IT investment costs, and promote information sharing;
- The ISA IPC Federated Identity Working Group (FIWG) developed *A Guide for Federal Relying Parties* on how to accept third-party credentials;
- The ISA IPC IISC led efforts with the Federal Cloud Credential Exchange (FCCX) project to provide a shared service for validation of third-party credentials that can be used by all departments and agencies;
- The PM-ISE supported an event deconfliction initiative between the Regional Information Sharing System (RISS) Program and the High Intensity Drug Trafficking Areas (HIDTA) Program to increase the safety of law enforcement officers;
- The SBU Working Group established a team of experts to develop an Identity and Access Management (IdAM) Reference Architecture for the ISE Enterprise Architecture Framework;
- The Regional Information Sharing Systems (RISS) Network worked with PM-ISE and SBU partners to develop a National Information Exchange Model (NIEM) Information Exchange Package Documentation (IEPD), which will facilitate the sharing of information among justice-related systems; and
- The PM-ISE is sponsoring an initiative to identify nationwide deconfliction standards and solutions, to interface deconfliction systems, and to develop a nationwide deconfliction strategy.

OPPORTUNITIES

- Last year, 33% of ISE agencies reported that they did not accept IT security certification bodies of evidence from other federal agencies, nor did they make accreditation decisions without retesting. This year's data shows incremental progress in federated identity management, with only 10% of ISE agencies (from the 2012 population) reporting that they do not practice IT security reciprocity with other federal agencies, and all responding agencies reporting progress in implementing federated identity management solutions aligning to the FICAM roadmap. The Backend Attribute Exchange (BAE) pilot and the Federal Cloud Credential Exchange (FCCX) project discussed in this section are focused on addressing federated identity management.
- Resource constraints continue to impact interoperability efforts for SBU/CUI networks, with only 40% of ISE agencies this year reporting that they have implemented interconnection plans for SBU/CUI networks supporting ISE related missions.[41] This is being addressed, in part,

[41] IdAM solutions will continue to be a focus area until this gap is closed.

by the establishment of the ISA IPC Information Integration Sub-Committee (IISC) Identity Federation Coordination (IFC) working group, which seeks to improve governance of identity-related efforts across the Federal Government and across all security domains.

ISE INTEROPERABILITY FRAMEWORK (I^2F)

Defining and adopting baseline capabilities to enable data, service, and network interoperability is a priority objective of the National Strategy. The PM-ISE developed I^2F to be a key component in implementing this objective in that it will identify key decision points for ISE interoperability; provide a comprehensive, high-level description of each interoperability domain; establish the framework[42] for implementing ISE information sharing capabilities and projects; and provide an alignment of interoperability reference architectures across the ISE.[lviii]

The I^2F will accomplish these objectives primarily through alignment to enterprise architecture frameworks used by ISE constituents; by introducing common templates to guide development of common interoperability artifacts; and by promoting tools and methodologies that promote interoperability considerations on reference architecture development and implementation.

In addition, the I^2F is designed to help ISE agencies better respond to complex policy challenges and to improve the delivery of services and information to citizens by driving long-term information sharing requirements—leveraging reuse capabilities for improvement, and information systems planning, investing, and integration to support the effective conduct of U.S. counterterrorism activities. I^2F version 1.0 provides a pathway to align the strategic goals and objectives of federal departments and agencies, state, local, tribal, and territorial (SLTT) government agencies, private-sector partners, and foreign partners and allies to facilitate interoperability and information sharing. It builds upon and leverages existing policies, business practices, and technologies in a manner that fully protects the legal rights of all U.S. persons.

ALIGNMENT TO EXISTING ARCHITECTURE FRAMEWORKS

The I^2F references current architecture frameworks used throughout the Federal Government to frame the applicable interoperability principles and domains. The interoperability domains are aligned with the following frameworks:

- Federal Enterprise Architecture Framework (FEAF)
- DoD Architecture Framework (DoDAF)

[42] The OMB has suggested using the term "interoperability framework" for the ISE rather than "enterprise architecture," to highlight the fact that the ISE is a cross-agency construct to be used as guidance for agencies developing the information sharing aspects of their enterprise architectures. The term "enterprise architecture" is used in the OMB context to refer to the architectures prepared by CIOs to manage the IT resources of a specific department or agency.

- Global Reference Architecture
- Intelligence Community Architecture Principles

These frameworks provide methodologies and artifacts that enhance interoperability among diverse systems and data types to facilitate the transfer and exchange of necessary information. They align capabilities, competencies, and services in a way that is best defined for their specific communities. The I^2F references these frameworks so that ISE participants can understand how the I^2F interoperability requirements can be put into the context of existing enterprise architecture (EA) efforts. The I^2F provides a higher-level mechanism to align reference architectures, which provide more specific requirements aligned to a specific service or capability. The final version of the I^2F, scheduled for delivery in November 2013, will include detailed architecture alignment and interoperability artifacts.

A WHOLE-OF-GOVERNMENT APPROACH TO DATA STEWARDSHIP AND DATA CORRELATION

In February 2012, the ISA IPC DAWG released the report *ISE Data Aggregation Capabilities Applicable to Terrorism.* This report recommended accelerating the convergence of existing data aggregation architectures and encouraging the development of a data aggregation reference architecture with an end-state vision for government-wide data aggregation activities.

In order to realize the end-state vision, in 2013 the DAWG began to develop a reference architecture framework designed to provide technical guidance to departments and agencies as they make decisions about developing interagency data-sharing requirements.

The reference architecture is intended to align services, capabilities, and standards as well as White House programmatic guidance and PM-ISE implementation guidance; the initial version is planned for release by December 2013. This whole-of-government approach will keep data as close to the data owners as possible, while using standards to enable common services for discovery and access management, and data correlation. Benefits include: increased data protection; more rapid information sharing; improved data quality for mission operators; and improved safeguarding to reduce the risk of bulk data leaks due to insider threats.

GEOSPATIAL ARCHITECTURE INTEROPERABILITY

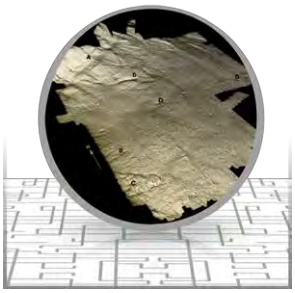
To foster the reuse of geospatial services, reduce their IT investment costs, and promote information sharing, the office of the PM-ISE is coordinating an effort with the DHS, DOI, NGA, and the DOC to develop a Geospatial Interoperability Reference Architecture (GIRA). Currently in draft, it is expected that GIRA will be published during the first quarter of 2014.

GIRA is intended to provide guidance and direction to managers and systems architects from federal agencies, SLTT agencies, private-sector partners, and foreign partners, in order to ensure the interoperability of geospatial services, fostering information sharing and ensuring fiscal responsibility. It provides a framework for the development of new geospatial system and solution investments; transition target architecture for the alignment of existing geospatial capabilities; methods for driving the integration of shared services with other investments; and performance measures for validating and reporting results.[43]

GIRA sets the direction and provides specific requirements, standards, recommended best practices, and reference artifacts toward a targeted interoperable geospatial capability. GIRA is expected to provide a common, reference architecture to effectively manage, support, and achieve interoperability through geospatial system integration, acquisition, and/or development; and to provide a documented architecture that can be used to support geospatial program technical oversight and technical assessments for geospatial investments.[lix]

GEOSPATIAL INFORMATION AS A NATIONAL RESOURCE

The Geospatial Intelligence Working Group (GWG) serves as a DoD, IC, federal, and civil community-based forum. Its purpose is to advocate for IT standards and standardization activities related to geospatial intelligence (GEOINT). In this capacity, the GWG supports the NGA in carrying out GEOINT responsibilities. The GWG places a heavy emphasis on collaboration between standards and enterprise architecture to promote re-use, interoperability, and open, "non-specific vendor" architectures.



Collaboration among GWG members also promotes the development of new standards by promoting understanding the future needs of the development community. For example, in support of an NGA agency-wide Identity and Access Management (IdAM) system, a design pattern was developed specific to implementing IdAM in an Open Geospatial Consortium (OGC) paradigm. This work led to collaboration between NGA prototype efforts and international standards development organization test beds, with the purpose of collectively reducing technical risks and advancing the use of common standards.

[43] The Office of Management and Budget (OMB) Circular A-16, "Coordination of Geographic Information and Related Spatial Data Activities," provides for improvements in the coordination and use of spatial data, and describes effective and economical use and management of spatial data assets in the digital environment for the benefit of the Federal Government and the Nation.

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT: COORDINATING IDENTITY EFFORTS ACROSS THE FEDERAL GOVERNMENT

FEDERATED IDENTITY MANAGEMENT

The GSA FICAM Program Office is leading the implementation of the National Strategy priority objective of extending and implementing the FICAM Roadmap across all security domains. In accordance with this planning, OMB is working with several qualified agencies to establish an Identity and Access Management Shared Services Line of Business, and the ISA IPC established the Identity Federation Coordination Working Group to work towards the interoperability of the various FICAM-related initiatives, and to improve governance of identity-related efforts across the Federal Government and across all security domains.[lx] The Identity Federation Coordination Working Group will coordinate with SLTT partners to facilitate participation of non-federal partners in Identity, Credential, and Access Management (ICAM) activities, and to ensure that solutions are interoperable across the ISE.

The Federated Identity Working Group (FIWG), another ISA IPC working group under the Information Integration Sub-Committee (IISC), worked on developing a guide for *Federal Relying Parties,* which provides supplemental instructions on how to implement a citizen-facing government website. The FIWG enabled federated identity trust across government agencies, focusing on cross-organizational identity federation, and supporting the development of content for other "how to" guides for agency use. The FIWG will develop additional guides to assist departments and agencies who are federating identities across government, and to ensure interoperability.[lxi]

The IISC coordinated efforts with the Federal Cloud Credential Exchange (FCCX) project, which will provide a shared service for validation of third-party credentials that can be used by all departments and agencies. As part of the National Strategy for Trusted Identities in Cyberspace, FCCX would enable the acceptance of third-party credentials to facilitate access to online government services. It would also include access to non-federal credential providers with a pre-established relationship as approved FICAM credential providers under the FICAM Trust Framework Solutions Program.

FICAM efforts are aimed at using industry-based credentials that citizens already have. In order to ensure that these credentials are trustworthy, the government requires well-defined processes to ensure that these processes meet federal requirements. These processes, codified as Trust Frameworks, include requirements for the establishment of credentials and their issuance; privacy requirements; and auditing qualifications and processes.

FICAM MATURITY MODEL

The FICAM Maturity Model was developed and released concurrently with the latest version of the FICAM Roadmap and Implementation Guide. The Maturity Model presents a series of questions with reference to the FICAM Roadmap and Implementation Guidance, which then determines the current level of maturity. The results provide respondents with a clear understanding of what needs to be done in order to improve an organization's maturity.[44]

FIRST RESPONDER ACCESS CARD TECHNOLOGY

Emergency response officials must be able to collaborate in order to ensure public safety. For this to happen, many identity management challenges must be overcome. While federal agencies are rapidly deploying secure common identification standards, SLTT emergency response officials are also working to establish a Personal Identity Verification-Interoperable (PIV-I)/First Responder Authentication Credential (FRAC) standard that will be interoperable between local, state, and federal government partners.

In response, the DHS Directorate for Science and Technology (S&T) has been working on a smart-phone app that will allow SLTT officials to verify and track first responders arriving at a scene, as well as exchange attributes to make sure they have the necessary training. The application is being developed for SLTT officials so they can easily and inexpensively verify first responders as they arrive at a scene.[lxii]

The DHS S&T Identity Management Testbed, hosted at Johns Hopkins Applied Physics Lab, has developed an app that can read PIV and PIV-I credentials as well as DoD Common Access Cards by using a commercial off-the-shelf Bluetooth smart-card reader. Because of the expense of these readers, DHS is also looking to take advantage of handsets that have built-in field communication to provide a more cost-effective access control tool. The app has been tested by Federal Emergency Management Agency (FEMA), and by other officials in Chester County, PA and in West Virginia.

[44] The 2013 ISE Performance Assessment Questionnaire results show that 82% of agencies responded that they plan to adopt FICAM.

ASSURED SENSITIVE-BUT-UNCLASSIFIED (SBU) – CONTROLLED-UNCLASSIFIED INFORMATION (CUI) INTEROPERABILITY

The Assured Sensitive But Unclassified/Controlled Unclassified Information Network Interoperability Working Group (SBU/CUI WG) works under direction of the National Security Staff and ISA IPC, and is responsible for advancing interagency interoperability at the national level.

During the reporting period covered by this Report, the Working Group continued its efforts to establish interoperability across existing networks; to identify areas of improved collaboration that are needed to remedy functional gaps; and to formulate action plans.

In addition to establishing an IdAM Implementation Roadmap with specific partner milestones through the end of FY 2013, the Working Group also developed its first five-year SBU Strategic Plan—*SBU Way Forward*—to supplement the shorter-term milestones and objectives. The Working Group also agreed to a "sunset" for the SBU Working Group once Simplified Sign-On (SSO) has been achieved across the SBU/CUI federation.

Since June 2011, the Sensitive But Unclassified Working Group has been focused on SSO, search and discovery, and standardized security controls. In 2012, the SBU/CUI Working Group realigned SSO,[45] search and discovery, and security focus teams to concentrate on IdAM. The SBU/CUI Working Group includes these four major law-enforcement, public-safety, and intelligence systems:

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

Additionally, this year the working group welcomed observer-contributor participation from NGA, DOI, and the Federal Aviation Administration (FAA).

This project included a detailed matrix of network visualizations in both federal and non-federal space, including graphical illustrations; e.g., ontology of connecting partnership nodes, an initial data model, and a final report that includes a detailed scope of the federated partnership.

Interoperability progress within the SBU environment was highlighted by PM-ISE and the SBU Working Group at several organization conferences, including the International Association of Law Enforcement Intelligence Analysts (IALEIA); the National Law Enforcement Intelligence Units

[45] Also referred to as Single Sign-On.

(LEIU); DoD Identity Protection and Management (IPM); the Counterintelligence Coordination Committee (CICC); and an in-house Executive Summit of interagency Chief Information Officers.

Despite continued challenges in partner resources and internal program priorities, the SBU partnership continues to make progress, drive policy changes, and establish technical advancements for interoperability within the SBU domain across federal, state, and local communities.[lxiii]

INTEROPERABILITY – INCREMENTAL PROGRESS

Partners continued to expand the SBU federation with new service-identity providers through existing partner portals. Resource constraints continue to impact SBU Working Group partners and their ability to synchronize efforts with federated partners in order to achieve all milestones, but progress continues.

With PM-ISE support, RISS facilitated the transition of the Institute for Intergovernmental Research (IIR) into the National Information Exchange Federation (NIEF), and coordinated with the Oregon State Information Network (OSIN) and the South Dakota Connect Project to use RISSNet as their identity provider.

Separately, PM-ISE supported an interoperability initiative between RISS Program and the HIDTA Program to enable event de-confliction and program standardization to increase the safety of law enforcement officers.[lxiv]

The SBU Working Group continued shared senior executive level leadership responsibility by rotating the SBU Working Group chair every six months to solidify partnerships and enhance collaboration on the employment of the HSIN.

Partner connectivity to HSIN will be initiated late in FY 2013, to coincide with the completion of its migration to its new, HSIN-Release 3 platform. During the last year measureable progress and achievements by SBU partners continues to accelerate toward the goal of full interoperability.

Increased leadership also enabled the Working Group to establish an ad hoc expert team to develop an Identity and Access Management (IdAM) Reference Architecture for the ISE Enterprise Architecture Framework.

HSIN FACILITATED PROMPT RESPONSE TO BOSTON MARATHON BOMBINGS

HSIN provided continuous, secure, web-conferencing capability to more than 400 individual, multi-jurisdictional intelligence officials nationwide, on-demand. This capability has been important in ensuring awareness and coordination between DHS I&A, fusion center, and state and local law enforcement officials during the ongoing investigation.

HSIN has also provided a secure, trusted platform for the sharing of documents and general updates between DHS National Protection and Programs Directorate (NPPD) and trusted members of the private sector through the NICC.

Further, the HSIN Help Desk supported an unprecedented number of requests for the use of HSIN resulting from the Boston bombing. The day after the bombing, the HSIN Help Desk fielded 1,200 individual calls. In the week that followed, they responded to more than 5,000 requests. (Typically, the Help Desk gets 250 inquiries per day or 1,750 inquiries a week.) Before the Boston attack, the highest number of calls the Help Desk had received in one day was 500, during the Deep Water Horizon Oil Spill.

FEDERATED ATTRIBUTE SHARING ON THE SECRET FABRIC

The purpose of the Federated Attribute Sharing on the Secret Fabric (FASS) study was to determine how the IC agencies operating on the Secret fabric could best establish a full IdAM presence and support the needs of authentication, authorization, and attribute retrieval.[46] These capabilities are needed as the IC moves beyond hosting files and browsing to operating re-hosted versions of mission apps and meeting the demands of EO 13587.

The FASS study showed that some IC agencies are moving ahead to establish applications and an IdAM component presence on Secret Internet Protocol Router Network (SIPRNET), and some do not need to do so. Where each agency stands in its progress is driven by demand from its own and from other Secret-level users on the fabric. Those agencies hosting significant applications (for example, NSA and NGA) are heading towards re-hosting their IdAM components; other agencies, who are not hosting resources, are interested in how identities can be provisioned.

The second major finding of FASS was that attribute federation within the IC components, with the DoD, and with other federal partners should be straightforward and fairly easily accomplished. For example, the IC's *Security Assertion Markup Language Attribute Sharing Profile* protocol is successfully implemented on Joint Worldwide Intelligence Communications System (JWICS); the DoD *Enterprise Identity and Attribute Service* interface is heavily used in the DoD today; and finally, there is some test use of the *Backend Attribute Exchange* (BAE) protocol.

[46] Implementation Strategy, Federated Attribute Sharing on the Secret Fabric (FASS), Draft Version 2.0, 9 November 2012

The third finding of this study was that there will be significant work needed in order to handle the IC's non-Common Access Card (CAC) holders. These users will need to be provisioned in order to be able to have their attributes discovered.

DEVELOPING INTEROPERABILITY, SIMPLIFIED SIGN-ON (SSO) AND SEARCH CAPABILITIES

RISS is the only non-federal entity, and RISSNet is one of only four networks participating in an interagency project—known as the Assured Sensitive but Unclassified (SBU) Interoperability Initiative—that are designed to save users time, maximize limited resources, and help law enforcement officers quickly identify and use actionable information.

RISS is a foundational partner in establishing federated identity management and access control within the SBU community. In 2012, working with PM-ISE and the SBU partners, RISS led the development of an Information Exchange Package Documentation (IEPD), which will facilitate the sharing of information through a security-trimmed federated search among justice-related systems.

RISS is also working with fellow SBU partners, such as Intelink, LEO, and HSIN, to develop SSO and search capabilities. More than 10,000 users from trusted partner systems are using federated identity to access RISSNet resources. Through RISSNet and RISS's partnerships, an unprecedented level of information has been shared, resulting in the arrest and prosecution of thousands of criminals and the seizure of millions of dollars in narcotics, property, and currency.

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

The IdAM framework continues alignment with the Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guide and connects with other IdAM initiatives, like the Backend Attribute Exchange (BAE) initiative with GSA.

The Federal Government continues to develop a strong BAE capability. In 2012, PM-ISE initiated work on operationalizing a BAE by partnering with the GSA's Office of Government-Wide Policy on an initial test scenario in which an ISE mission partner will use BAE to access information from an external portal, such as the RISS.

OTHER SHARED SERVICES

THE DHS COMMON OPERATING PICTURE (COP)

Homeland Security Presidential Directive 5 (HSPD-5) designates the Secretary of the Department of Homeland Security as the "Principal Federal Official for Domestic Incident Management." To meet its statutory requirements, the DHS Office of Operations Coordination and Planning, in collaboration with the DHS Office of the Chief Information Officer, developed, operates, and maintains the Department's Common Operating Picture (COP).

The DHS COP uses a services-oriented architecture that allows it to leverage existing DHS investments and enterprise-class capabilities and provides shared services, including both public and private cloud services, with base map and imagery services, as well as more than 500 data layers with street-level views, geo-coding and mobile Internet access.[lxv]

Since February 2012, the DHS COP has monitored more than 1,300 activities and published over 750 incident reports. The COP has more than 3,500 users, including 1,700 DHS, and more than 600 other federal users across more than 100 organizations; 136 state users across 62 fusion centers; and more than 900 state and local law enforcement users. The number of users continues to increase steadily.

The Common Operating Picture Domain Executive Steering Committee (COP ESC), established by DHS in early 2012, continues to advance information sharing practices and COP capabilities across DHS. The COP ESC provides governance and oversight of all aspects of the COP Domain, which includes investments, systems, data, policies, and the procedures needed to ensure that homeland security partners have an enduring capability to effectively, efficiently, and rapidly access situational awareness information.

CRITICAL EVENT DECONFLICTION

Investigative efforts create the potential for conflict between agencies or officers who are unknowingly working in close proximity to each other, or who may be coordinating an event focused on the same suspect at the same time. In these instances, agencies or officers may unintentionally interfere with each other's cases, potentially impacting the integrity of ongoing investigations, or resulting in endangering officers. Interconnecting existing event deconfliction systems and developing nationwide standards for deconfliction is necessary to ensure the safety of law enforcement officers.

To meet the need for standards development and systems interoperability, PM-ISE is sponsoring an initiative to identify nationwide deconfliction standards and solutions; connect deconfliction systems; and develop a nationwide deconfliction strategy.

Between January and April 2013, the initiative developed and tested an interface between the RISS Officer Safety Deconfliction System (RISSafe) and HIDTA's Case Explorer deconfliction system, which is now fully operational. Since January 2013, 62,657 operations have been entered, identifying 25,054 conflicts. In addition, the FBI is utilizing its Guardian Program (iGuardian, eGuardian, and Guardian) to allow for event deconfliction both at the Unclassified and Secret classification levels.

The Washington/Baltimore (W/B) High-Intensity Drug Trafficking Area (HIDTA) is a key player in efforts to make the three deconfliction systems used by HIDTA—RISSafe, Secure Automated Fast Event Tracking Network (SAFETNet), and Case Explorer—interoperable. Using technology developed through Mercyhurst University and the University of Maryland and housed at the W/B HIDTA, Case Explorer and RISSafe have been interfaced to allow for event deconfliction to take place across both systems for users in the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network®. The interface has been in operation since March 2013 and has proven successful. Efforts are underway to expand this interface across the entire RISS Project, beginning with the RISS Western States Information Network (WSIN).

Elsewhere, the El Paso Intelligence Center (EPIC) is developing an interface between SAFETNet and Case Explorer which will close the loop across all three event deconfliction systems used by the HIDTAs.

DHS INFORMATION SHARING SEGMENT ARCHITECTURE V 3.0

In March 2013, DHS completed an update to their Information Sharing Segment Architecture (ISSA), which will serve as a guide for implementing the target architecture of the DHS Information Sharing Environment (DHS ISE). This update, known as ISSA Version 3.0, introduces a standard set of information sharing and technical capabilities in order to provide the entire DHS mission and enterprise functions with the policies, strategies, leadership, architecture, and governance needed to consistently share information. ISSA Version 3.0 focuses on improving its network of trust; enhancing its ability to securely and efficiently share information with stakeholders, especially the Intelligence Community (IC); and promoting better information sharing across DHS.

The ISSA provides a blueprint for the DHS ISE that is designed to ensure that access to information does not hinder, but rather strengthens, the homeland security mission. Through the implementation of the ISSA Version 3.0, DHS will be able to achieve interoperability through common standards; identify redundancies and potential technological conflicts; locate opportunities for streamlining and/or collaborating with partners; identify information sharing gaps; align technology to mission goals and objectives; and gain a more thorough understanding of the complete functionality being provided by a specific technology for information sharing.

FBI LAW ENFORCEMENT ENTERPRISE PORTAL (LEEP)

Scheduled for deployment in 2013, the FBI's LEEP will provide the law enforcement, intelligence, and criminal justice communities with SSO access to Law Enforcement Online (LEO); the Law Enforcement National Data Exchange (N-DEx); the Joint Automated Booking System (JABS); INTELINK; INTELINK Chat; RISSNet (Identity and Service Provider); the National Gang Intelligence Center (NGIC); the Internet Crime Complaint Center (IC3); and the DOJ my File Exchange (myFX).

LEEP will allow users to access these services via their home agency networks by simply clicking on an icon that is pre-populated at initial log-on. Participating agencies include the Chicago Police Department, the Texas Department of Public Safety, the Los Angeles Sheriff's Department, the Michigan State Police, the Atlanta Police Department, the Regional Information Sharing Systems Network (RISSNet), and INTERPOL's U.S. National Central Bureau.

When users access LEO via LEEP, they will have access to LEO Special Interest Groups (SIGs)—collaborative environments for law enforcement agencies with common information needs; LEO Virtual Office (VO)—for storing agency training, policy, and procedure information; LEO Virtual Command Center (VCC)—a simple, effective, and secure information sharing and crisis management tool for law enforcement; and LEO-partnered sites and databases, including the Violent Criminal Apprehension Program (ViCAP); the Operational Response and Investigative Network (ORION); the eGuardian; Hostage Barricade Database System (HOBAS); the Innocence Lost Database (ILD); the National Center for Missing Exploited Children (NCMEC); and the National Alert System (NAS).

THE DOI INCIDENT MANAGEMENT ANALYSIS AND REPORTING SYSTEM (IMARS)

The Department of the Interior (DOI) Incident Management Analysis and Reporting System (IMARS) is a records-management system designed to provide seamless sharing of law enforcement reporting information between all DOI law enforcement programs, and to provide a consistent, reliable way to share information with partner agencies. Deployed to more than 6,000 users in FY 2012, IMARS allows DOI to manage law enforcement activities on the 500 million acres of land that it owns and manages in order to ensure the safety and protection for millions of visitors each year.

These responsibilities require the collection, analysis, management, and reporting of information by DOI law enforcement officers, including tribal law enforcement. IMARS access allows officers, agents, and dispatchers to access departmental and national databases from their immediate locations, significantly enhancing officer safety in the field. DOI is currently testing and evaluating an interface between IMARS and the FBI's eGuardian system.

DEA'S DE-CONFLICTION AND INFORMATION COORDINATION ENDEAVOR (DICE) TOOL

First deployed in November 2009, the De-confliction and Information Coordination Endeavor (DICE) software tool continues to enable HIDTA, federal, state, and local law enforcement with enhanced investigative efficiencies through the ability to de-conflict information, such as phone numbers, e-mail addresses, license plates, and financial account information over a secure Internet browser.

INTERLUDE: BACKEND ATTRIBUTE EXCHANGE OPERATIONAL PILOT

Over two years in the making, this year the Backend Attribute Exchange (BAE) Operational Pilot, a PM-ISE funded project designed to address a critical gap in intergovernmental access control, met a significant capability milestone for automated access control across multiple federal and state information systems. The capability allows for automated access decisions that enable users to successfully access the information needed to complete their mission while automatically ensuring that the information safeguards are enforced.[lxvi]

During this pilot demonstration, users in Texas logged into the Texas network and accessed a protected federal database via the National Identity Exchange Federation (NIEF).[47] The net result of timely access to information promotes the protection of law enforcement officers and the disruption of criminal or terrorist activity.

RISSNet relied on an attribute maintained and provided by a separate federal agency—in this case DOJ's Bureau of Justice Assistance (BJA)—to authorize the user's access to its protected gang database. The transaction was carried out automatically, behind the scenes, invisible to the end user.

BAE PILOT RESULTS

The outcome marks a significant improvement in a historically cumbersome, bureaucratic, and time-consuming process of verification for access to critical information. The pilot establishes the BAE as an effective, functional building block for the backbone of the Federal Government's information sharing and safeguarding strategy.

KEY PARTNERS

The GSA's Office of Government-wide Policy (GSA OGP); NIEF; the DOJ's BJA; the Institute for Intergovernmental Research (IIR); the RISS Program;[48] the Texas Department of Public Safety; and the Texas State Police all played key roles in making this pilot a success.

[47] NIEF is a collection of U.S. government agencies that have come together to share sensitive law enforcement information. It was created in 2008 as an outgrowth of the Global Federated Identity and Privilege Management (GFIPM) program, which seeks to develop secure, scalable, and cost-effective technologies for information sharing within the law enforcement and criminal justice communities, based on the paradigm of federated identity and privilege management.

[48] RISS serves federal, state, local, and tribal criminal justice agencies in their effort to identify, detect, deter, prevent, and solve criminal and terrorist-related investigations.

SECTION 4:

STRENGTHENING SAFEGUARDING OF INFORMATION

This section describes key achievements over the past year in safeguarding the 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 need to both protect and share national security and counterterrorism-related information that is stored on and disseminated electronically from Federal Government information systems has become of increasingly critical importance. Sharing and safeguarding information 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.

> "…strike the proper balance between sharing information with those who need it to keep our country safe and safeguarding it from those who would do us harm."[49]
>
> PRESIDENT BARACK OBAMA

Recent information breaches and disclosures highlight vulnerabilities in the protection of sensitive and classified information. Continued implementation of structural reform and standardized policies, however, will strengthen oversight as well as align security best practices.

[49] National Strategy for Information Sharing and Safeguarding, December 2012

The release of Executive Order 13587—*Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* — in October 2011, and the December 2012 White House release of *The National Strategy for Information Sharing and Safeguarding* (National Strategy) have provided additional policy guidance for driving improvements in the sharing and safeguarding of classified information.

While departments and agencies made some progress in improving the security of classified networks during the last reporting period, recent events involving insider threats reinforce the need to continue the work begun under EO 13587 in order to make substantive improvements to safeguarding the security of our classified networks.

The Steering Committee has mapped out clear, consensus-based goals and a plan for measuring progress on classified sharing and safeguarding.

In 2013, the Steering Committee will continue to oversee Department and Agency implementation of initial priorities, and will develop and implement plans for addressing emerging vulnerabilities on classified systems. These actions will continue to improve the security of our classified information and systems, and will enhance the support of our critical national security missions, while continuing to promote responsible sharing of classified information.

The following list of findings highlights accomplishments and opportunities for improvement. Further detail is provided in the following pages of this section.

ACCOMPLISHMENTS

- The Administration disseminated in November 2012 a Presidential Memorandum on the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs;
- DHS expanded its Enhanced Cybersecurity Services (ECS) program, in accordance with EO 13636, *Improving Critical Infrastructure Cybersecurity,* to better assist critical infrastructure owners and operators in improving protection of their systems from unauthorized access, exploitation, or data exfiltration;
- HHS established a Cyber Threat Analysis Unit (CTAU) to develop indicators of compromise, and to detect intrusions or exfiltrations of HHS systems or data at their earliest stages;
- The Defense Industrial Base (DIB) Enhanced Cybersecurity Services (DECS) activity was approved as an optional element of the DoD's DIB Cybersecurity and Information Assurance (CS/IA) Program, providing a means for the Federal Government to share classified cybersecurity information with Cleared Defense Contractors (CDC);

- DoD is rolling out a program that will allow users of mobile devices working anywhere—from remote battlefields to the Pentagon—to rapidly share classified information and protected data across all components;
- The IACP co-hosted a Cyber Threat Roundtable with DHS that brought together more than 20 state and local representatives, and various associations from across the country;
- The Comprehensive National Cybersecurity Initiative Five (CNCI-5) led the Federal Cybersecurity Centers[50] in documenting their requirements for government-wide, cybersecurity information sharing.

OPPORTUNITIES

- Continuing efforts by the Steering Committee to advance the priority areas will improve security by strengthening the identification of individuals who are accessing classified systems; limiting access on the basis of the individual's "need-to-know" through technical controls; reducing the opportunity for information to be removed from the secure environment; improving efforts against insider threats; and improving audit capabilities. Considerable work remains in three priority areas: Reduced Anonymity, Access Control, and Enterprise Audit.
- As noted last year, cybersecurity can be improved through effectively sharing cyber-vulnerability and intrusion information; and the ISE's information sharing processes can enable cybersecurity information sharing. The work of CNCI-5 and the focus of FEMA's National Level Exercise (NLE) 2012, detailed in this section, highlight the ways in which the sharing of cybersecurity information can make networks more secure.

THREAT ENVIRONMENT AND VULNERABILITIES

As in the unclassified environment, the threats to classified systems and information are real, growing, and multidimensional. The classified environment also presents an increasingly complex threat and risk environment resulting from increasing interconnection of systems as well as shared services and their human users.

Our understanding of the threats and associated vulnerabilities for classified systems and information is also improving. The increasing interconnection of classified systems and the flow of information across systems will increase the potential impact of compromises to the security of this information.

[50] The Federal Cybersecurity Centers are: the NSA/CSS Threat Operations Center (NTOC); the DHS National Cybersecurity Communications and Integration Center (NCCIC); the U.S.-Cyber Emergency Response Team (US-CERT); the National Cybersecurity Investigative Joint Task Force (NCI-JTF); the Intelligence Community Incident Response Center (IC-IRC); and the USCYBERCOM Joint Operations Center (JOC).

ESTABLISHING PRIORITIES

The Steering Committee identified five priority areas for departments and agencies to focus their efforts in improving the safeguarding of classified information within their classified networks, with the understanding that these areas will take several years to fully implement.

These priorities include:

- Removable Media
- Insider Threat Programs
- Reduced Anonymity
- Access Control
- Enterprise Audit

In 2012, the Steering Committee developed clear, consensus-based goal descriptions for each priority, which included identifying initial and final milestones [(initial operating capability [IOC] and final operating capability [FOC], respectively)]. IOC represents a minimum threshold of immediate improvements needed to safeguard classified networks, while FOC represents the end-state capability required for sustained, comprehensive protection of classified networks.

The Steering Committee has requested all departments and agencies that handle classified information to apply milestone definitions to their respective operating environments and to forecast when they will be able to verify attainment of IOC and FOC for each priority.

Each department and agency is starting from a different capability and resource level. Each has projected different timeframes for completion, based on its starting point and resources. Because of this mixed picture, and the need for collective attainment of IOC and FOC goals to manage shared risk, the Steering Committee is actively working with the departments and agencies to accelerate IOC and FOC attainment.[lxvii]

AREAS OF PROGRESS

To evaluate individual and collective progress on the priorities, the Steering Committee developed a set of information sharing and safeguarding indicators. The 39 departments and agencies that handle classified information on computer networks each submitted quarterly progress reports on these indicators. Two safeguarding indicator areas—removable media and implementing insider threat capabilities—made progress over the past year based on the quarterly analysis of agency reporting.

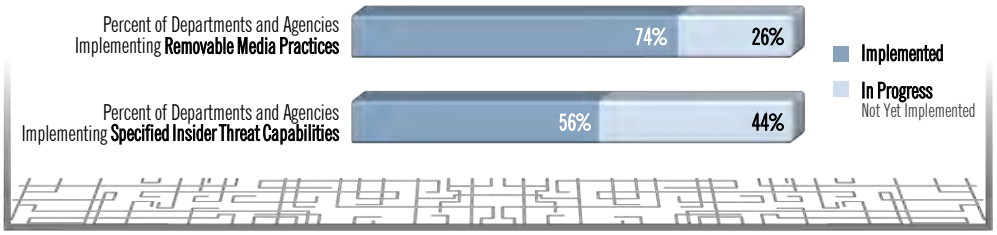


Figure 2. Departments and Agencies made some progress in 2012 towards reaching the full operating capability for Removable Media Management and initial operating capability for Implementing Insider Threat Capabilities.

On November 21, 2012, a Presidential Memorandum on the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, developed by the interagency Insider Threat Task Force (ITTF), was disseminated to the heads of all departments and agencies. The Minimum Standards provide departments and agencies with the elements necessary to establish effective insider threat programs. Elements include the capability of gathering, integrating, and centrally analyzing and responding to key threat-related information; monitoring employee use of classified networks; providing the workforce with insider threat awareness training; and protecting the civil liberties and privacy of all personnel.

The ITTF has conducted insider threat forums to introduce and explain the policy and standards to agency leaders.

REMAINING GAPS AND EMERGING VULNERABILITIES

Although departments and agencies made some progress in 2012 on the first two priorities—Removable Media, and Implementing Insider Threat Capabilities—considerable work remains on these two priorities, as well as on the other three priorities, and on emerging vulnerabilities to classified systems and information. Gaps in reaching IOC and FOC represent continuing vulnerabilities for classified systems and information.

Our continuing efforts in these priority areas will improve security by strengthening the identification of individuals accessing classified systems; limiting access on a basis of the individual's "need-to-know" through technical controls; reducing the opportunity for information to be removed from the secure environment; improving efforts to prevent insider threats; and improving audit capabilities. Additional discussion on gaps and vulnerabilities is included in the classified supplement to this report.

THE WAY FORWARD FOR STRENGTHENING SAFEGUARDING IN 2013

Numerous cross-cutting federal committees are collaborating to establish best practices through the Federal Identity and Access Management and the Joint Continuous Monitoring Group, which will address the other three priorities: Reducing Anonymity, Accessing Control, and Enterprise Auditing.

In 2013, the Steering Committee will continue to oversee the progress of departments and agencies on the first five priorities, identified in 2012. Additionally, the Steering Committee will oversee the commencement of independent assessments, conducted by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force.

OTHER KEY SAFEGUARDING-RELATED ACCOMPLISHMENTS

A number of other notable safeguarding accomplishments merit recognition. The section below highlights progress in several areas.

DEFENSE

PKI HARD TOKENS – DOD COMMON SERVICE PROVIDER

During this reporting period, the Steering Committee determined that all agencies operating on Federal Government classified or Secret networks must implement a hardware-based Public-key Infrastructure (PKI) solution to protect their information and networks; remove anonymity; and improve the overall security of federal Secret networks.

DoD, which was already in the process of implementing a PKI Secret Internet Protocol Router Network (SIPRNET) token capability, decided to leverage its existing infrastructure to stand up a common service provider (CSP) capability for all federal agencies, with the exception of those agencies who have their own systems. The Defense Information Systems Agency (DISA) is the operator of DoD PKI, and will be the CSP for the federal agencies.[lxviii]

Further discussion on how PKI solutions are protecting the Top Secret networks is found in the classified supplement to this Report.

JOINT INFORMATION ENVIRONMENT[51]

The Defense Department continues to work toward transformation into a joint information environment, with defense industry and interagency partners, in support of the President's cybersecurity policy to establish a framework for a voluntary process to share information on cyber attacks and potential security risks to the nation's critical infrastructure.

In May 2012 an information sharing program between DoD and eligible Defense Industrial Base (DIB) companies was formally established with the publication of a federal rule, 32 CFR Part 236, DoD-DIB Voluntary Cybersecurity/Information Assurance (CS/IA) Activities.

This voluntary program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

Under the DIB CS/IA program, DoD provides classified and unclassified cyber-threat information and information assurance best practices to DIB participants. In turn, DIB participants report cyber incidents that may involve DoD information for analysis, the development of coordinated mitigation strategies, and, when needed, cyber intrusion damage assessments of compromised DoD information. The DoD Cyber Crime Center is the DIB CS/IA operational focal point for cyber threat information sharing, DIB incident reporting, and response.

The Defense Department's information priorities include defining the joint information environment architecture for military networks; addressing redundant security infrastructure; and providing command and control to the U.S. military and its mission partners to enable enhanced communications and to promote mission accomplishment.

DEFENSE CYBER CRIME CENTER (DC3)

DC3 is a national cyber center and serves as the operational focal point for the Defense Industrial Base Cybersecurity and Information Assurance (DIB CS/IA) Program.

The DC3 DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE) is the hub for cyber analysis and information sharing between Defense Industrial Base (DIB) Partners and U.S. Government (USG) Stakeholders.

Established in 2007 in response to the critical need to improve information sharing, DC3/DCISE is the DoD focal point for the voluntary DIB CS/IA Program which was formed

[51] The Joint Information Environment (JIE) facilitates the convergence of DoD's multiple networks into one common and shared global network, and provides enterprise services such as email, Internet/Web access, common software applications and cloud computing. In addition to enhanced network security, JIE objectives include increased operational efficiencies and cost savings through reduced infrastructure and manpower.

to assist DIB companies in safeguarding DoD unclassified information residing on or transiting DIB unclassified networks.

DC3/DCISE produces actionable threat products—the unclassified Threat Information Product(s) (TIPS) provide indicators that companies can use at their discretion to help defend their corporate networks.

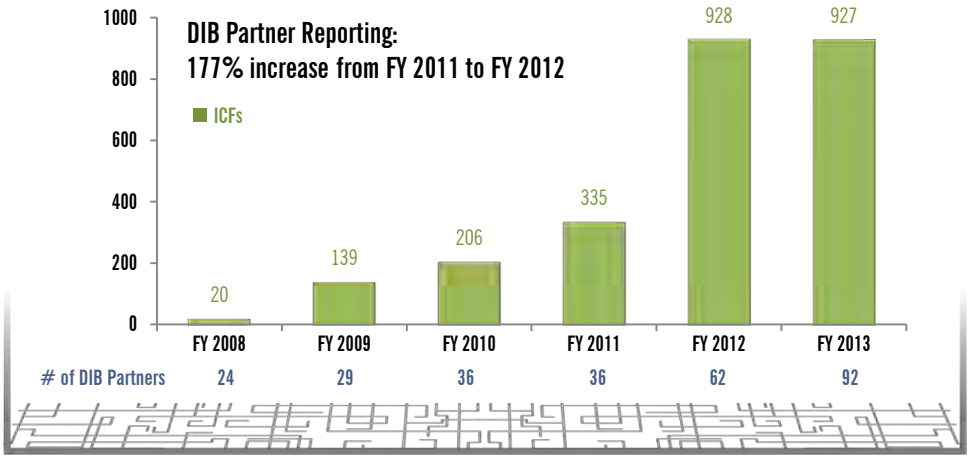


Figure 3. The Incident Collection Form (ICF) is used by DIB partners to submit incident data to DC3 via a secure web site.

When partner companies report events, according to a mutually agreed tiered schema, DC3/DCISE performs analysis and diagnostics and remediation consults, backed up by forensics and malware analysis from DC3 Defense Computer Forensics Laboratory (DCFL).

Beyond simply providing threat products, the partnership is promoting a change in business culture with respect to how partner companies make decisions to protect their key intellectual property.

As the U.S. continues to face enormous challenges in protecting aiding industry in protecting its intellectual property, the processes developed by the DC3/DCISE and the trust relationships established with the DIB partners also help afford the USG a unique and valuable aperture on threats to the Defense Industrial Base.

SECURING INFORMATION ON MOBILE DEVICES

DoD is rolling out a program that will allow users to employ a range of mobile devices—working anywhere in the world, from remote battlefields to the Pentagon—to rapidly share classified information and protected data.

The goal of the implementation plan is to ensure that mobile devices throughout the Department—as well as their apps, email, other functions, and

the wireless networks supporting them—can operate securely even in hostile and remote environments, and can adapt to changing technology and a growing number of users.

Officials have established a phased implementation plan involving vendor competition for development of a system that could serve as a model for large companies that also need to protect the transmission of both open and confidential data.

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

Safeguarding activities covered under EO 13587 present additional opportunities for building P/CR/CL protections at the programmatic level. The Steering Committee is coordinating with National Security Staff to enhance insider threat and continuous monitoring programs. To support the implementation of these programs, agency legal counsel and P/CR/CL officers have developed guidance for federal agencies to incorporate into their respective agency policy documents and other tools supporting comprehensive P/CR/CL safeguarding programs.

INTERLUDE: HOMELAND SECURITY AND CRITICAL INFRASTRUCTURE

ENHANCED CYBERSECURITY SERVICES (ECS)

DHS is the lead agency for coordinating the activities of the Federal Government for the protection of the nation's critical cyber and communications networks and infrastructure. As such, DHS directly supports federal civilian departments and agencies in developing capabilities that will improve their cybersecurity posture in accordance with the Federal Information Security Management Act (FISMA); and works regularly with critical infrastructure owners and operators to strengthen their facilities, respond to threats, and coordinate mitigation efforts against attempted disruptions. To accomplish this, the DHS Enhanced Cybersecurity Services (ECS) program was expanded in February 2013 by EO 13636, Improving Critical Infrastructure Cybersecurity.

ECS is a voluntary information sharing program that assists critical infrastructure owners and operators to improve protection of their systems from unauthorized access, exploitation, or data exfiltration. ECS consists of the operational processes and security oversight required to share sensitive and classified cyber threat information with qualified Commercial Service Providers that will enable them to better protect their customers—critical infrastructure entities. ECS augments, but does not replace, these entities' existing cybersecurity capabilities. The ECS information sharing process protects critical infrastructure entities against cyber threats that could otherwise harm their systems.[lxix]

In May 2012, the Defense Industrial Base (DIB) Enhanced Cybersecurity Services (DECS) activity was approved as an optional element of the DoD's preexisting DIB Cybersecurity and Information Assurance (CS/IA) Program. DECS provides a means for the Federal Government to share classified cybersecurity information with cleared defense contractors to enable enhanced cybersecurity protections for defense information that resides on or passes through DIB networks and systems.

COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE FIVE (CNCI-5)

The Comprehensive National Cybersecurity Initiative Five (CNCI-5) led the federal cybersecurity centers[52] to document their requirements for government-wide, cybersecurity information sharing, while accommodating legal, privacy, and policy considerations. CNCI-5's work focuses on developing requirements for the information sharing architecture (ISA). Currently, the federal cybersecurity centers are developing an implementation plan to accelerate development of the ISA in FY 2014.

[52] The Federal Cybersecurity Centers are: the NSA/CSS Threat Operations Center (NTOC); the DHS National Cybersecurity Communications and Integration Center (NCCIC); the U.S.-Cyber Emergency Response Team (US-CERT); the National Cybersecurity Investigative Joint Task Force (NCI-JTF); the Intelligence Community Incident Response Center (IC-IRC); and the USCYBERCOM Joint Operations Center (JOC).

The concepts are being tested by an Enhanced Shared Situational Awareness (ESSA) Pilot to share spear-phishing threat activity between the United States Computer Emergency Readiness Team (US-CERT) and the NSA Threat Operations Center (NTOC). The pilot validated ESSA technology requirements, as well as highlighting the need for additional inter-departmental work on cybersecurity information sharing policies. Accordingly, CNCI-5 chartered a working group to create a government-wide policy framework.

DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) CYBER THREAT ANALYSIS UNIT

HHS is a world leader in the development of health-related research, technical data, and sensitive information impacting global health security. As intelligence trends and cyber intrusions have demonstrated in recent years, sensitive information and intellectual property are targeted not only by foreign intelligence services and foreign actors, but others as well, e.g. academic and research institutions; and private-sector companies. Losses of sensitive economic information and intellectual property to hostile actors or foreign adversaries pose significant national security risks and economic costs.

The HHS Office of Security and Strategic Information (OSSI) has established a Cyber Threat Analysis Unit (CTAU), which is building forensic capabilities to address these threats and support the operational mission of the HHS operating divisions that are most targeted for their highly sought-after intellectual property and sensitive technical data and research; divisions like the Centers for Disease Control and Prevention, the Food and Drug Administration, the Centers for Medicare & Medicaid Services, and the National Institutes of Health.

CTAU conducts in-depth analysis of IC and law enforcement cyber intelligence, and information on attempted intrusions into HHS networks, and uses trend analysis and forensics to examine threats, conduct predictive analysis, categorize vulnerabilities, and develop indicators of compromise to detect intrusions or exfiltrations at their earliest stages. Within HHS, OSSI is disseminating cyber threat information across the operating divisions to ensure that vulnerabilities are addressed and techniques are readily identified to safeguard networks from intrusions or cyber attacks.

STATE AND LOCAL GOVERNMENTS

Fusion Center Cybersecurity Evaluation Environment

The office of the PM-ISE assisted the National Fusion Center Association (NFCA) and the International Association of Chiefs of Police (IACP) by facilitating a Cybersecurity Evaluation Environment Pilot Kick-off event in conjunction with the Northern California Regional Intelligence Center (NCRIC).

The event built upon previous discussions (primarily during an August 2012 meeting hosted by the NCRIC, and the December 2012 DHS-IACP Cybersecurity Roundtable), and was held to generate multi-organizational support and urgency for piloting a Fusion Center cyber information sharing capability in 2013.

The event focused on:

1) Soliciting cyber information sharing requirements from industry partners;

2) Articulating the government's perspective on and potential processes for information sharing with the private sector; and

3) Explaining federal, state, and local government requirements for cyber information sharing within the government.

Participants reached consensus concerning high-level requirements, themes, and elements of a common vision for the future of cybersecurity information sharing.

Next steps include piloting Federal Cyber Center information sharing with fusion centers by leveraging current information sharing activities and business processes to enhance:

1) Protection of state, local, and CIKR networks;

2) Cyber crime investigations; and

3) Resiliency and response with integrated information sharing.

INTERNATIONAL INFORMATION SAFEGUARDING ACTIVITIES

Cybersecurity Information

Canada and the United States jointly engaged with the private sector on cybersecurity issues, enhanced real-time information sharing between cyber operation centers, continued cooperation on promoting public awareness of cybersecurity issues, and developed a joint Cybersecurity Action Plan to support and inform both nations' cybersecurity efforts. Canada and the United States continued to strengthen cooperation on international cybersecurity and Internet governance issues, including engagement with the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group, the Organization of American States, the Meridian Process and Conference, the G8, the U.N. Group of Government Experts, and the preparatory process for the World Conference on International Telecommunications.

Critical Infrastructure Information

Canada and the United States are connected by their critical infrastructure, from bridges and roads to energy infrastructure and cyberspace. The Beyond the Border Action Plan includes measures to enhance the resiliency of our shared critical and cyber infrastructure, and to enable our two countries to rapidly respond to and recover from disasters and emergencies on either side of the border.

Canada and the United States continued implementation of the Canada-U.S. Action Plan for Critical Infrastructure, including conducting a Regional Resilience Assessment Program project for the Maine-New Brunswick region. There are plans to conduct joint risk analysis, develop collaborative cross-border analytical products, and share methodologies as well as best practices to enhance critical infrastructure security and resiliency.

SECTION 5:

PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES[lxx]

This section addresses ISE initiatives that are focused on ensuring the protection of privacy, civil rights, and civil liberties (P/CR/CL) through the consistent government-wide application of protections.

The following list of findings highlights accomplishments and opportunities for improvement. Further detail is provided in the pages that follow.

ACCOMPLISHMENTS

- The Information Sharing and Access Interagency Policy Committee (ISA IPC) P/CL Subcommittee is developing guidelines for information sharing and safeguarding agreements that will both ensure that mission needs are met and that P/CR/CL are protected;
- DOC, HHS, Treasury, and DOE finalized their privacy policies;
- DoD is near completion of its updated Privacy Directive;
- DHS established a formal process for conducting compliance reviews for the implementation of privacy protections within and across the Department's information sharing programs;
- Treasury conducted a pilot of the compliance review self-assessment checklist drafted by the P/CL Subcommittee's Compliance Review Working Group to determine if the effectiveness of this tool as a review and audit mechanism for agency compliance is within ISE privacy policies;
- DOI is developing a computer-based course entitled "Privacy for the Information Sharing Environment" that will provide guidance on compliance requirements for P/CR/CL protections;

- DHS hosted a National Fusion Center P/CL Officer Workshop, in coordination with the NSI PMO, and the DOJ Bureau of Justice Assistance; and
- The PM-ISE hosted its fourth roundtable outreach event with the advocacy community in order to build stronger P/CR/CL protections in operational programs, training, and guidance materials.

OPPORTUNITIES

- While there have been initiatives to measure and ensure privacy compliance, there currently is not an effective ISE-wide performance measurement for internal agency compliance, oversight, and accountability mechanisms to ensure consistent application of P/CR/CL protections. The development of these measures is a priority for the ISA IPC P/CL Subcommittee.

STRATEGIC OBJECTIVES AND PRIORITIES ESTABLISHED FOR THE ISE

Several priority objectives identified in the National Strategy have P/CR/CL implications, and their implementation will provide for a more uniform application of P/CR/CL protections across the ISE by helping mission partners reach a common understanding of such safeguards.

Over the last year, the Privacy and Civil Liberties (P/CL) Subcommittee and its Privacy and IT Working Group (PITWG) have been developing guidelines for information sharing and safeguarding agreements that will both ensure that mission needs are met, and ensure the protection of personally identifiable information and P/CR/CL. A common process for framing these agreements adds value by promoting a mutual understanding of appropriate protections among information sharing partners, and by sharpening the partners' focus on legal and policy requirements, data uses, and identification of mission purposes for the acquisition of information. This is particularly important when partners have vastly different authorities and mission requirements.

With input from the Data Aggregation Working Group, PITWG has taken these principles into consideration in its on draft policy guidance to address key P/CR/CL requirements for information sharing and safeguarding agreements and identifying ways to streamline the development process. The policy guidance is projected to be disseminated to ISE stakeholders in 2013 and subsequently supplemented by a checklist, which may include sample language.

P/CR/CL GOVERNANCE

The ISA IPC works with the office of the PM-ISE and serves as a key governance body for carrying out the strategic vision and priority objectives set forth in the National Strategy. It brings federal partners together to develop strategic, cross-cutting approaches to addressing information

sharing and safeguarding requirements. The ISA IPC P/CL Subcommittee is comprised of senior privacy and civil liberties representatives from ISE federal mission partners as identified in EO 13358, or as designated by the Director of National Intelligence. The Subcommittee is steered by an Executive Committee of senior P/CL officers from the ODNI, DHS, and DOJ, and is chaired by the ODNI Civil Liberties Protection Officer.

Since its re-constitution in September 2010, the P/CL Subcommittee has advised the ISA IPC on the best means for strengthening the protection of P/CR/CL within information sharing and safeguarding activities by federal agencies, SLTT government agencies, and private-sector partners. Over the past year, P/CL Subcommittee members have focused on supporting initiatives and developing tools to help mission partners consistently apply P/CR/CL requirements, including technical assistance to support the development of ISE privacy policies, the development of draft guidance to streamline the process for developing information sharing agreements, and the development and piloting of a compliance review self-assessment template.

Established by the Implementing Recommendations of the 9/11 Commission Act of 2007, the Privacy and Civil Liberties Oversight Board (PCLOB) became operational as an independent oversight agency within the executive branch during the 2012-2013 reporting period. The Board has a full-time chairman and four part-time board members. All are nominated by the President and confirmed by the Senate.

The PCLOB has both a consultative and an oversight role regarding P/CR/CL in the Federal Government's development and use of the ISE. The PCLOB has two primary purposes: 1) to analyze and review actions the executive branch takes to protect the U.S. from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and 2) to ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.

DEVELOPMENT AND IMPLEMENTATION OF ISE PRIVACY POLICIES

A significant area of focus and P/CL Subcommittee attention has been in the development and adoption of written P/CR/CL policies, as required by the *ISE Privacy Guidelines*. In last year's Annual Report, PM-ISE reported that federal partners continued to make slow but steady progress toward the completion of these P/CR/CL policies, with 79% of federal ISE departments and agencies having completed-policies in place.[53] As of July 2013, the completion rate is 93%, due to DOC, HHS, Treasury, and DOE having finalized their policies. DoD is currently revising its directive, DoDD 5400.11, to commit to following the *ISE Privacy Guidelines* in lieu of issuing a stand-alone ISE privacy policy.

[53] Agencies with completed policies in place include: the CIA, the ODNI, NCTC, DHS, DOI, DOJ, FBI, DOS, and DOT.

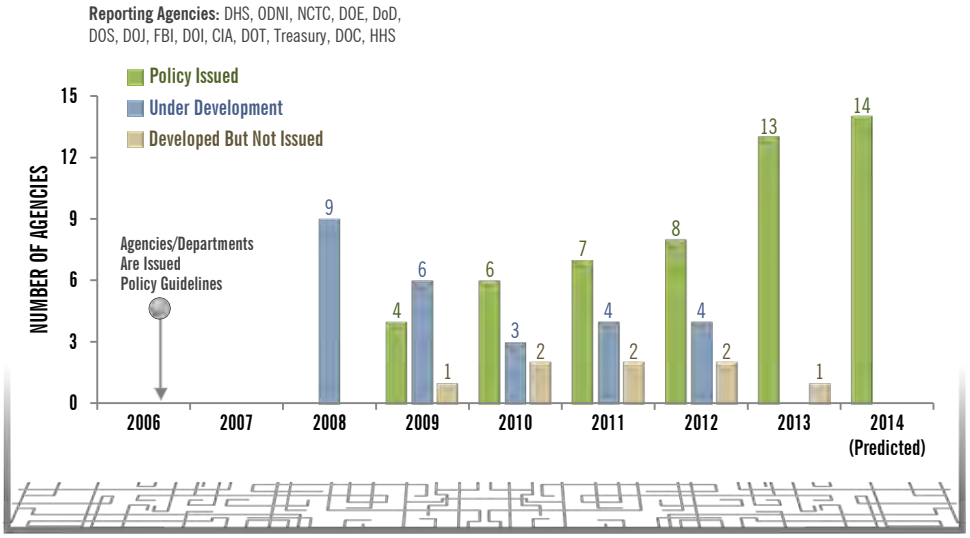


Figure 4. Federal ISE Privacy Policy Status.

State, local, tribal and territorial partners continue to demonstrate their commitment to protecting P/CR/CL by prioritizing the development and implementation of privacy policies that are at least as comprehensive as the ISE Privacy Guidelines. In addition, all 78 fusion centers have an approved privacy policy that is at least as comprehensive as the ISE Privacy Guidelines.

COMPLIANCE ACTIVITIES

During the past year, ISE agencies reported using one or more of the following mechanisms for ensuring compliance with statutory and regulatory authorities, *ISE Privacy Guidelines* requirements, agency legal guidance, protocols, and policies:

- Reviewing information sharing and safeguarding agreements and other mechanisms to ensure that the activities comply with legal and agency policy requirements;
- Conducting programmatic reviews of law enforcement programs;
- Auditing intelligence systems;
- Reviewing intelligence reporting that is to be shared within the ISE, before that information is disseminated to ISE partners; and
- Periodic Office of Inspector General reviews of privacy and security practices.

In addition, DHS established a formal process to conduct compliance reviews for the implementation of privacy protections within and across the Department's information sharing programs. Over the last year, the DHS Privacy Office conducted and completed a review of DHS's participation in the Nationwide Suspicious Activity Reporting Initiative (NSI) and is currently updating its internal processes to comply with recommendations resulting from this review.

Also of note, the Department of the Treasury conducted a pilot of the compliance review self-assessment checklist that had been drafted by the P/CL Subcommittee's Compliance Review Working Group in 2012. The objective of the pilot was to determine the effectiveness of this tool as a review and audit mechanism for agency compliance with their respective ISE privacy policies. Pursuant to the *ISE Privacy Guidelines*, federal agencies are required to have an adequate review and audit mechanism in place to verify compliance with the Guidelines. The results and recommendations from the pilot will be evaluated by the P/CL Subcommittee and used to enhance the efficacy of the checklist.

CRITICAL ROLE OF THE P/CL OFFICIAL

As emphasized in previous annual reports, P/CL officials from federal ISE agencies must be actively involved with information sharing and safeguarding activities for their respective agencies. P/CL officials are charged with directly overseeing the implementation of, and compliance with, the *ISE Privacy Guidelines* and P/CR/CL policies and procedures within their agencies.

ISE mission partners are actively working to ensure that legal and policy P/CR/CL requirements are appropriately and consistently integrated into programmatic activities. Full integration of P/CR/CL protections not only facilitate compliance with legal and policy requirements, but also ensure that mission needs are met.

The responses to this year's performance assessment questionnaire indicate an increase in the involvement in ISE activities by P/CL officials, although the level of participation in ISE activities appears to be uneven across the agencies. Future progress can best be achieved by having P/CL officers work closely with operational stakeholders in the planning, development, and oversight of information sharing and safeguarding efforts, and by establishing a common understanding between and among mission partners on the need for and scope of these protections.

In light of the National Strategy emphasis on streamlining the development process for information sharing agreements, P/CL officials are a critical resource for ISE agencies. P/CL officials must be involved early in the development process to ensure that mission-appropriate P/CR/CL protections are built into the agreements, and must be able to appropriately participate in reviews of compliance with the terms and conditions of information sharing agreements, including compliance with ISE requirements. For these reasons, ISE mission partners should assess whether their P/CL officials have the appropriate authority and resources needed to provide appropriate oversight over P/CR/CL issues that arise out of their agencies' participation in the ISE.

TRAINING AND OUTREACH

Training and outreach are essential parts of P/CR/CL protections. Commitment to P/CR/CL safeguards builds trust with partners and the community, reinforces information sharing activities, and necessarily involves training personnel who are authorized to share protected information in the ISE. The National Strategy includes as a priority the need to provide training for information sharing, safeguarding, and handling to promote consistent, trusted processes. This training must address P/CR/CL legal and policy requirements, and must include role-based training where appropriate.

At the federal level, mission partners have emphasized the importance of training ISE personnel on P/CR/CL protections, although the responses to the annual ISE Performance Assessment Questionnaire reveal that the types of training and the substantive depth of the modules differ from agency to agency. The types of training that were identified in the responses include privacy awareness and annual refresher training; ISE Core Awareness training available at ise.gov; training on the agency's ISE privacy policy, including data handling, disclosure, redress, etc.; additional or specialized training developed by an agency or component privacy officer; specialized training on EO 12333, *U.S. Intelligence Activities*, and the application of dataset-specific requirements, including P/CR/CL protections; training that focuses specifically on civil liberties protections; and training on the sharing of protected information in the NSI.

During this reporting cycle, the Department of the Interior (DOI) stands out for its efforts in developing a computer-based course entitled "*Privacy for the Information Sharing Environment*" that will provide guidance to all DOI law enforcement officials, as well as employees and contractors with ISE responsibilities, on compliance requirements for P/CR/CL protections. The module is expected to be completed in FY 2013.

At the state and local level, training through various workshops and other presentations has helped to prevent the potential loss of institutional and subject matter knowledge resulting from the turnover in staff, liaison officers, and other fusion center personnel.

In November 2012 the DHS Office for Civil Rights and Civil Liberties and the DHS Office of Intelligence and Analysis hosted a National Fusion Center Privacy, Civil Rights, and Civil Liberties (P/CR/CL) Officer Workshop, in coordination with the NSI PMO and the DOJ Bureau of Justice Assistance. Out of 78 fusion center P/CR/CL Officers, 68, or roughly 87%, were present to hear about the latest P/CL protection best practices and lessons learned. They were given a "toolkit" with more than 15 P/CL training modules and exercises for conducting further training at their centers.

Fusion centers develop, implement, and enforce P/CR/CL safeguards to protect constitutional and other legal rights, and to ensure that they are addressing their legal and policy obligations while engaged in the fusion center process. Their commitment to these safeguards also builds trust with partners and the community, which in turn fosters increased information sharing, which is vital to executing the fusion process.

The NSI has also continued to implement a comprehensive and multi-tiered approach to analyst/investigator training. This training, as with all NSI role-based training modules, emphasizes the importance of P/CR/CL protections in the process of identifying and documenting suspicious activity. The curriculum stresses, among other things, that reporting of suspicious activity must be based on one or more of the sixteen observed preoperational behaviors, and not be based solely on personal attributes such as race or ethnicity, or the individual's exercise of his or her civil liberties, which are protected by the Constitution.

Outreach between ISE mission partners and with the advocacy community promotes transparency of ISE initiatives, and fosters an opportunity to assess public concerns and perceptions. Many federal and SLTT mission partners have established strong relationships with the advocacy community as part of their office or agency outreach program. Over the past eight years, PM-ISE's engagement with the advocacy community on ISE matters has resulted in stronger P/CR/CL protections in operational programs, training, and guidance materials. In May 2013, PM-ISE hosted its fourth roundtable outreach event with the advocacy community, in collaboration with federal, state, and local mission partners.

PRIVACY, CIVIL RIGHTS AND CIVIL LIBERTIES – NEXT STEPS

The ISA IPC Privacy and Civil Liberties (P/CL) Subcommittee has developed a series of next steps:

- Develop and implement effective and comprehensive compliance, oversight, and accountability mechanisms for ensuring consistent application of mission-appropriate P/CR/CL protections by ISE mission partners.
- Define and implement a common process and template for the development of information sharing agreements, to streamline the process and promote best practices.
- Promote a common understanding of P/CR/CL protections across information exchanges of datasets, and other mission information through information sharing agreements.
- Develop and implement ISE P/CR/CL training that can be leveraged by ISE mission partners.
- Ensure a process for periodic outreach to the privacy, civil rights, and civil liberties advocacy community, to promote awareness and dialogue concerning developments across the ISE.

This page intentionally left blank.

SECTION 6:

MANAGING AND FOSTERING A CULTURE OF RESPONSIBLE INFORMATION SHARING

This section addresses progress on oversight and management functions that support information sharing and safeguarding, including the alignment and harmonization of governance bodies, performance management, training, and information sharing and safeguarding incentives within the ISE.

The following list of findings highlights accomplishments and opportunities for improvement. Further detail is provided in the pages that follow.

ACCOMPLISHMENTS

- The Federal Chief Information Officer (CIO) Council, the Steering Committee, and the Information Sharing and Access Interagency Policy Committee (ISA IPC) are overseeing the implementation of the National Strategy priority objectives through their respective working groups;
- DHS and FEMA delivered introductory and intermediate risk analysis training courses for fusion center analysts;
- DHS sponsored a bi-monthly series of specialized analytic seminars designed to enhance the capabilities of fusion center analysts to effectively monitor and evaluate potential threats in analysts' areas of responsibility;
- DHS, in partnership with the U.S. Secret Service (USSS), sponsored a cyber-analysis training pilot program focused on the current threat environment, best practices, and resources available to fusion center analysts;

- The FBI held the first annual National Cyber Executive Institute, a three-day seminar for training leading industry executives on cyber-threat awareness and information sharing;
- DHS partnered with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Program Management Office (PMO) to support the delivery of a series of SAR analysis courses designed to help analysts better understand the processes for reviewing, vetting, and analyzing SAR;
- The National Maritime Intelligence-Integration Office (NMIO), in partnership with the NSI PMO and in coordination with the U.S. Coast Guard (USCG), is delivering a new SAR awareness training module to increase awareness among the maritime sector's workers, security personnel, and executives;
- The National Information Exchange Model (NIEM) Biometrics Domain (NBD) kicked off a new training initiative, the first in a series of sessions which focus on tailoring NIEM resources to best reach the biometrics community; and
- The office of the PM-ISE launched the Data Exchange Toolkit via the Building Blocks of the ISE website. The toolkit guides users through the basic steps needed to evaluate and improve existing data exchanges.

OPPORTUNITIES

- Responses to the 2013 ISE Performance Assessment Questionnaire (PAQ) show mixed results with respect to agency adoption and implementation of incentive tools for information sharing and safeguarding. Ninety percent of responding agencies—a 10% increase from last year—reported that "information sharing and collaboration" is an evaluated performance objective for employees with direct ISE responsibilities. However, responding agencies reported a decrease in the number of candidates nominated for information sharing and collaboration awards compared to the previous year.[54]

IMPROVING GOVERNANCE

Oversight of the implementation of the National Strategy for Information Sharing and Safeguarding (National Strategy) is a government-wide effort being carried out by three committees—the Federal CIO Council, the Steering Committee, and the ISA IPC—each of which uses working groups for these efforts.[55]

[54] It is unclear what caused this decline. One possible explanation is that specific incentives for information sharing are less likely to be awarded as information sharing and collaboration are gradually becoming key components of job functions, especially those jobs that require interagency collaboration. This supposition is supported by the increase in employee information sharing performance objectives, and the fact that 71% of agencies, up from 62% last year, report that they offer mission-specific training that supports information sharing and collaboration. Although there is no supporting data, it is also possible that the current fiscal environment has made it necessary to cut back on monetary awards. Further analysis is being done to understand these results.

[55] See the Way Forward section of this Report for details.

Given the number and diversity of stakeholders and communities involved, the ability to convene agencies from across the government in mature committee structures is critical to getting partners to the table, and to agreeing upon efficient implementation plans.

To support these efforts, ISE agencies are increasingly assigning dedicated staff to oversee information sharing and safeguarding activities, and to participate in interagency processes to implement whole-of-government best practices. According to the 2013 ISE PAQ, 95% of ISE agencies report that, in compliance with Executive Order (EO) 13587, they have designated a senior official who is accountable for the sharing and safeguarding of classified information on computer networks.

THE ISE PERFORMANCE FRAMEWORK

In 2013, the office of the PM-ISE aligned the ISE performance management framework to the priority objectives in the National Strategy. Comprising a roadmap for ISE agencies, the framework provides maturity-driven, time-sequenced actions for agencies as they implement National Strategy priority objectives and execute other information sharing and safeguarding activities in response to annual ISE Implementation Guidance. The framework's performance measures allow the office of the PM-ISE to assess the maturity of the nations' ability to detect, analyze, and respond to terrorism, WMD, and homeland security threats.

To assist agencies in planning for and executing the framework's goal-based initiatives, the office of the PM-ISE created a set of mission-based test 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 may be impacted as information sharing and safeguarding capabilities mature—from current capabilities to those that are expected in five to seven years. The National Strategy prioritizes the reusable and cross-cutting capabilities of the ISE and validates the mission-based test scenarios in the ISE performance framework, which are described in detail in Appendix B. Mission-based test scenarios assist the ISE by demonstrating information sharing priorities and capabilities in a mission context, and allow the ISE to assess progress on desired capabilities by providing a line-of-sight view from a National Strategy objective to an ISE cross-cutting capability to an agency's program implementation.

For each scenario, PM-ISE has created performance measures that reflect expectations for information sharing and safeguarding capabilities at each level of maturity in the areas of community, process, and technology.[56] This gives agencies the tools they need 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

[56] Community is defined as engagement with state, local, federal, tribal, and international partners. Process is defined as common methodologies and practices that enable joint operational accomplishments. And technology is defined as technical solutions that automate shared agreements and make solutions interoperable between ISE partners.

needed to achieve our strategic goals for each ISE stakeholder mission. ISE agency performance data is an output of this process, as discussed throughout this Report, and is detailed in Appendix A.

	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 IS&S progress to mission performance. Shows that agencies are linking information sharing metrics to mission performance metrics.
PROCESS	Designed to measure compliance with SE 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.

NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING GOALS

Figure 5. ISE Performance Framework Capability Areas and Maturity Stages.

BUDGET-PERFORMANCE INTEGRATION

The White House issues programmatic guidance for responsible information sharing. The PM-ISE subsequently issues ISE Implementation Guidance that provides more specific direction for agency activities in order to achieve the priorities defined in the programmatic guidance. The implementation guidance provides the basis for an objective, system-wide set of performance goals for the following year, as required by IRTPA.[lxxi]

The programmatic guidance defines funding priorities for budget-year development. The implementation guidance, developed collaboratively with the agencies, defines near-term activities for agencies, and informs agencies' budget-year development.

ISE Implementation Guidance is an important tool for coordinating the ISE-specific activities of federal agencies. The office of the PM-ISE, through the ISA IPC governance process, tracks the progress of these activities and milestones, ensuring that the ISE continues to advance toward its goals and objectives, and informs performance goals for the following year. Actions are

capabilities-focused, aligned with mission objectives, and subject to the annual performance assessment process.

Throughout the year, the office of the PM-ISE works with agencies to complete the actions specified in the ISE Implementation Guidance. Table 2 provides a status of actions overdue, underway, and due to be completed during the period of July 1, 2012 to May 31, 2013. A detailed account of ISE investments can be found in Appendix C.

Table 2. Progress toward ISE Implementation Guidance.

IMPLEMENTATION GUIDANCE ACTION	DUE	OWNER	STATUS
Conduct independent assessments of department and agency compliance with established safeguarding policy and standards.	31-Mar-12	DoD/NSA	Not Complete
Deliver to the PM-ISE an inventory of existing federal, state, local and tribal public safety information systems that could be migrated to a cloud configuration.	30-Sep-12	DOJ	Not Complete
Establish processes to monitor and report fusion center compliance with respect to privacy, civil rights, and civil liberties requirements.	30-Sep-12	DHS	Complete
Implement process to monitor NSI compliance with privacy, civil rights, and civil liberties requirements.	30-Sep-12	DOJ	Complete
Finalize mechanisms to share information on adjudicated radiological shipments; standardizing information sharing on general radiological shipments and licenses; and sharing post-seizure analysis and information.	30-Sep-12	DHS, DOT, NRC	Not Complete
With local and tribal law enforcement entities at ports of entry, institutionalize cargo screening information sharing, including screening related to WMD, and disaster response and emergency management information sharing.	30-Sep-12	DHS, DOJ	Not Complete
Assemble individual agency-wide governance responsible for agency-wide coordination of information sharing activities for information exchange standards, federated trust standards, messaging framework standards, and information security framework standards.	30-Sep-12	DoD, DHS, DOJ, DOS	Complete
Identify the credential provider for the required level of assurance credentials for each system.	29-Mar-13	All	Not Complete
Deliver to the PM-ISE an agency-specific report outlining the work completed to date and planned activities for FY 2014 and FY 2015.	30-Mar-13	DoD, DHS, DOJ, DOS	Complete
Deliver to the PM-ISE an IC-specific report outlining the work completed to date and planned activities for FY 2014 and FY 2015.	30-Mar-13	ODNI	Complete
For the actions marked "not complete," PM-ISE will work through the ISA IPC governance process to bring these actions to closure.			

Over the next year, with the ISA IPC, the PM-ISE intends to integrate the governance, performance framework, budget and performance integration processes described above, as well as other processes into an ISE Management Plan. The concepts of the ISE Management Plan are discussed further in the Way Forward of this Report.

RESPONSIBLE INFORMATION SHARING TRAINING

Successful sharing of terrorism-related information across the 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—depends upon each individual in the ISE consistently and properly executing responsible information sharing duties. This consistent execution grows out of robust, agency-based programs that provide sustained training to analysts, operators, and investigators with direct ISE responsibilities.

In response to the 2013 ISE PAQ, 86% of agencies reported implementing mission-specific training that supports information sharing and collaboration. 93% 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.[57]

RISK ANALYSIS COURSES

DHS Office of Intelligence and Analysis (I&A) worked with the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and FEMA to deliver introductory and intermediate risk analysis training courses for fusion center analysts. The courses were developed to help intelligence analysts and critical infrastructure protection analysts gain an enhanced understanding of risk analysis through the application of the core components of risk (threat, vulnerability, and consequence), and by highlighting sample fusion center risk products. Participants gained the appropriate training, tools, and mentoring to develop a sample fusion center risk product and a stronger peer-to-peer network. DHS has delivered more than 16 of these trainings in 12 states to date.

SPECIALIZED ANALYTIC SEMINAR SERIES

Beginning in February 2013, DHS sponsored a bi-monthly series of specialized analytic seminars designed to enhance the capabilities of fusion center analysts by bringing together a diverse range of subject matter experts in seminars to discuss the knowledge, skills, and resources necessary to effectively monitor and evaluate potential threats in analysts' areas of responsibility. The series addressed the following topics in the context of fusion center operations: Human Trafficking; Financial Crimes; All Hazards; Gangs; Maritime; and Drugs.

[57] See Appendix A for more detail.

Forty-five fusion center analysts participated in the first seminar on human trafficking. The workshop provided an overview of human trafficking indicators, briefings on trafficking trends and tactics, as well as a panel discussion on resources available to support state and local analysts. The seminar also included several case studies presented by state and local officials on human trafficking products. Partner organizations included the DHS Blue Campaign, the FBI, the Federal Law Enforcement Training Center, ICE, and the Human Smuggling and Trafficking Center (HSTC).

CYBER ANALYSIS TRAINING

In November 2012, DHS I&A, in partnership with USSS, sponsored a cyber-analysis training pilot program. Approximately 20 fusion center cyber analysts from around the country attended. The program focused on the current threats, best practices, and resources available to fusion center analysts. Three additional courses will be delivered in 2013. In February 2013, the FBI held the first annual National Cyber Executive Institute, a three-day seminar to train industry executives on cyber threat awareness and information sharing.

SAR ANALYSIS COURSE

DHS I&A partnered with the NSI PMO to support the delivery of a series of SAR analysis courses designed to assist analysts to better understand processes for reviewing and vetting SAR, as well as processes for formally analyzing SAR to inform fusion center analytic efforts and products. The SAR Analysis courses provide instruction on various methods and approaches to analyzing SAR as part of overall analytic processes. Specifically, the course will instruct participants in the methods for evaluating SAR; for conducting structured inquiry focused on SAR trends, relationship, and patterns; and for incorporating SAR analysis into fusion center product development. Additionally, the FBI retooled the NSI's SAR analytic training course for the purpose of providing the course to federal partners, as part of the NSI Federal Plan.

NATIONAL FUSION CENTER ANALYTIC WORKSHOP

On January 15-17, 2013, DHS sponsored a National Analytic workshop designed to support the continued development of the National Network's Critical Operational Capability 2 (Analyze)—the ability to assess local implications of threat information through the use of a formal risk assessment process. The meeting covered topics ranging from privacy, civil rights, and civil liberties, to human trafficking, to cybersecurity, to regional strategic threat assessment development, to critical infrastructure protection and risk analysis. Nearly 200 people attended, representing fusion centers from throughout the country. The NSI SAR Analyst course was also provided as an optional training course during the last day of this workshop.

NSI TRAINING

The NSI training strategy is designed to increase the effectiveness of state, local, tribal, and territorial 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.

The 2013 ISE PAQ data indicates that more than 80% of federal ISE agencies provide SAR training to their personnel. To date, DOJ Bureau of Justice Assistance (BJA) has trained more than 110,000 federal law enforcement officers, and a total of 291,502 line officers from all 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and Guam. In addition, BJA trained a total of 2,196 law enforcement analysts within both fusion centers and the Federal Government, and is working with the New York City Fire Department to institutionalize the SAR training within their training academy. The NSI conducted more than 70 speaking engagements in 2012, reaching homeland security advisors, chiefs of police, state colonels, sheriffs, critical infrastructure key resources owners and operators, tribal law enforcement executives, private sector security executives, probation/parole/corrections executives, fire/emergency management services personnel, fusion center directors, and federal partners.

SAR – MARITIME TRAINING

The National Maritime Intelligence-Integration Office (NMIO), in partnership with the NSI PMO and in coordination with the USCG, is delivering a new SAR awareness training module to increase awareness among the maritime sector's workers, security personnel, and executives. The program will be identical in format to NSI PMO's other "Hometown Security Partners" training, and will be accessed through online training portals.

The training will educate those in the maritime industry who have a potential of being exposed to indicators and behaviors associated with criminal and or terrorist activity. Additionally, the NSI PMO, the NMIO, the DHS, the FBI, and the USCG have partnered and begun visiting 10 U.S. port facilities to increase NSI-Maritime Safety Information awareness, and to capture best practices regarding the SAR program in each port.

NIEM BIOMETRICS DOMAIN TRAINING

On February 26, 2013 the NIEM Biometrics Domain kicked off a new training initiative, the first in a series designed to share knowledge of NIEM and the NIEM Biometrics Domain, which operates under the stewardship of the DHS Office of Biometric Identity Management (OBIM). The session focused on tailoring NIEM resources to best reach the biometrics community, with the goal of

raising awareness and understanding of the standardized information sharing capabilities, best practices, and resources available to biometric stakeholders worldwide. The training included an overview of NIEM governance, domains, tools, models, Implementation Exchange Package Documentations, and the NIEM value proposition.

PERFORMANCE INCENTIVES

Effective and secure information sharing is ultimately the result of, and completely dependent upon, the daily actions of the countless individuals within 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 the National Strategy's vision of providing the right information, at the right time, to any authorized user. Including responsible information sharing objectives in performance appraisals, and creating agency awards for responsible information sharing, can be powerful tools to help achieve this vision.

Responses to 2013 ISE PAQ show mixed results with respect to agency adoption and implementation of these tools: 90% of responding agencies, a 10% increase from last year, reported that "information sharing and collaboration" is an evaluated performance objective for employees with direct ISE responsibilities.[58] Interestingly, responding agencies reported a decrease in the nomination of candidates for information sharing and collaboration awards from last year—a troubling trend when taken at face value. However, it is unclear what is causing the decline. It could be that as information sharing and collaboration become integrated as key components of job functions, especially those jobs that require interagency collaboration, specific incentives for information sharing are less likely to be awarded.

This supposition is supported by the increase in the incorporation of information sharing performance objectives by agencies, and the fact that 71% of agencies—up from 62% last year—report that they offer mission-specific training that supports information sharing and collaboration. It could also be the case that the current fiscal environment, including the Federal Government's required response to sequestration, has made it necessary to cut back on monetary awards. Further analysis is being done to interpret these results.

BUILDING BLOCKS OF THE ISE

Leveraging ISE partners' lessons learned and best practices to enable collaboration and re-use is critical to the success of the ISE. In order to make available the requisite tools to achieve this, the office of the PM-ISE launched "Building Blocks" in August 2012.

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

Building Blocks is an online, public-facing training tool available on www.ise.gov that provides an in-depth view of how the office of the PM-ISE, with its partners, creates a responsible Information Sharing Environment. The tool outlines the 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. The tool is designed to help ISE mission partners find and share best practices, guidelines, and lessons learned with other partner agencies as well as with the public.

Figure 6. The Building Blocks of the ISE.

Building Blocks highlights ISE partner success stories by outlining how they were able to implement information sharing guidelines within their own agency. Learning how to establish a governing body, build a strategy, and then develop performance measures against that strategy are just a few of the topics detailed on the tool.

Users are also guided through the process of developing an implementation plan, building in interoperability, and applying standards. The toolkit explains the importance of fostering engagement with stakeholders and the practical concepts behind privacy and security implications.

In March 2013, the office of the PM-ISE launched the Data Exchange Toolkit using a pilot conducted by DHS and NCTC. This toolkit is available on the Building Blocks site, and guides users through the basic steps needed to evaluate and improve existing data exchanges. Users first define scope and identify candidates for the exchange. Next, users access and identify solutions; then plan and implement those solutions. Finally, the toolkit explains how to evaluate improvements achieved.

THE WAY FORWARD

The security of the Nation hinges on the ability to affect "… collaboration across the Federal Government—and with our state, local, tribal, private-sector, and international partners ..."[59]

In December 2012 the President issued the National Strategy for Information Sharing and Safeguarding (National Strategy), which provides a roadmap for a broader collective effort of responsible sharing and safeguarding of national security information, while reaffirming existing ISE policies and strategies. The National Strategy has established principles, goals, and a set of priority objectives that create a vision and a way forward for the ISE.

On behalf of the President, PM-ISE plans for and monitors the implementation of the ISE[60] under the broad framework and vision of both the 2012 National Strategy and the 2007 National Strategy for Information Sharing and Executive Orders 13388, *Furthering Strengthening the Sharing of Terrorism Information to Protect Americans* and 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Networks*. With the release of EO 13636, *Improving Critical Infrastructure Cybersecurity*, and PPD-21, *Critical Infrastructure Security and Resilience*, PM-ISE is engaged with the National Security Staff and agencies to develop plans to extend ISE management frameworks and activities to also support effective federal progress with cybersecurity information sharing.

As described throughout this Report, significant progress has been made over the year implementing ISE capabilities, by advancing responsible information sharing, improving decisionmaking, and promoting partnerships. This section builds on last year's Way Forward and is informed by both qualitative and quantitative assessments of that progress, performance, and challenges over the past year.

[59] National Security Strategy, 2010, pg. 51
[60] IRTPA Sec 1016(f)(2)(A)(i).

Under the ISA IPC, co-led by PM-ISE and the National Security Staff, a government-wide effort is underway to prioritize, plan, and coordinate continued, agency-based implementation of the ISE via a focus on the priority objectives of the National Strategy. Working in coordination with NSS, PM-ISE has set clear, unified and integrated priorities that span across the policy framework described above. PM-ISE priorities are described later in this section.

Overall, PM-ISE has embraced the new tasks and the larger scope of the ISE while addressing the U.S. Government Accountability Office's (GAO) concerns, as outlined in GAO's Terrorism-Related Information Sharing High Risk List.[61]

MANAGING IMPLEMENTATION OF RESPONSIBLE INFORMATION SHARING

INSTITUTIONALIZING A MANAGEMENT FRAMEWORK

The National Strategy, supported with White House Programmatic Guidance, has updated the vision for the ISE. Both are rooted in the requirements of Intelligence Reform and Terrorism Prevention Act (IRTPA). Together they form the core drivers of PM-ISE's annual capability-focused Implementation Guidance. The PM-ISE Implementation Guidance is developed in partnership with the agency-based stewards of the National Strategy's 16 priority objectives, and provides the basis for a system-wide set of milestones and timelines for the following year, as required by IRTPA.[62] Overall, the annual planning cycle helps move agencies closer to the target vision of national security through responsible information sharing.

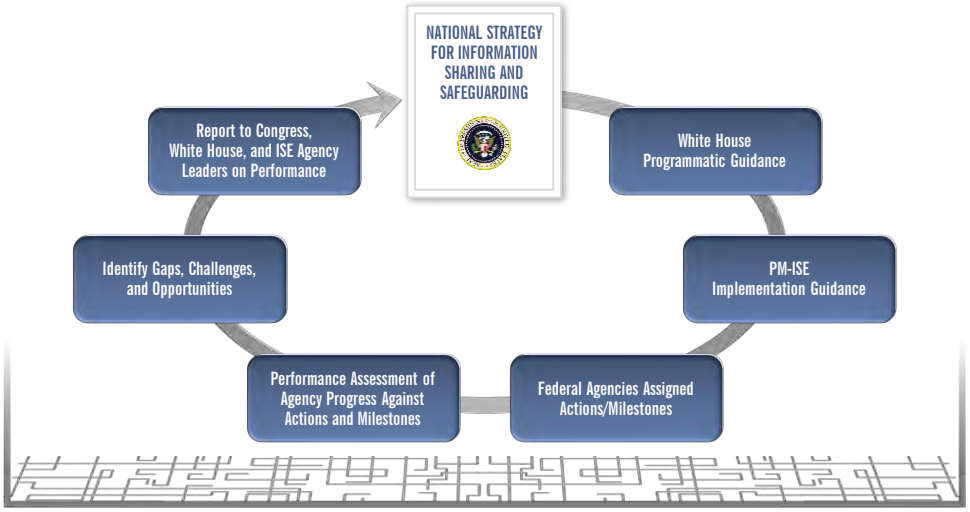


Figure 7. ISE Annual Planning Cycle.

[61] GAO-13-283 High Risk Series Update, February 2013.
[62] IRTPA Sec 1016 (h) (2) (B)

ACCOUNTABILITY AND COMMITMENT BY FEDERAL DEPARTMENTS AND AGENCIES

The PM-ISE Implementation Guidance outlines the actions assigned to specific federal agencies, articulates the desired milestones and timelines, and identifies the sequenced requirements needed to improve responsible information sharing and safeguarding for targeted capabilities, programs, systems, and initiatives. Annual performance assessments measured against this guidance provide accountability for progress over time, enabling leadership to make informed programmatic and budget decisions in subsequent years. The status of completed and incomplete Implementation Guidance actions can be found in Table 2 in Section 6 of this report.

Agencies lead the delivery, operation, and use of the ISE, and are accountable to the White House for the goals and actions identified in programmatic and ISE Implementation Guidance. Agencies are committed to responsible information sharing under the National Strategy through their participation in the ISA IPC, the White House-chaired Senior Information Sharing and Safeguarding Steering Committee, and the Federal Chief Information Officers Council.

ISE INTEROPERABILITY FRAMEWORK (I^2F)

Planning under the National Strategy highlighted a government-wide need to better describe and specify common requirements for interoperability and to promulgate guidance on applying sound information management principles and practices. The ISE Interoperability Framework (I^2F), described in Section 3 of this Report, provides an interoperability-focused enterprise architecture capability for the ISE. The I^2F describes a coordinated approach to interoperability built on common ISE intellectual property: a unifying architecture framework anchored under OMB's Common Approach, common profiles, standards and standards-based acquisition, and reference architectures. Agencies will use I^2F to enable integration of core ISE standards and architecture frameworks into their information technology decisions and implementations, by providing a direct reusable way of leveraging cross-cutting standards and architecture, and interoperable capabilities. The I^2F is foundational to defining and adopting baseline capabilities and common requirements that enable data, service, and network interoperability, and to implementing the Federal IT Shared Services Strategy to facilitate adoption of shared services.

ISE MANAGEMENT PLAN

PM-ISE is also developing an ISE Management Plan, consistent with existing policy and guidance from the White House, designed to guide how PM-ISE and ISE stakeholders collaborate, using common business processes and tools, to create a unity of effort across the government in advancing the implementation of the ISE.

The Management Plan describes a process-oriented approach to effectively manage the implementation of strategic priorities for responsible information sharing. It serves as a resource for ISE stakeholders, providing mechanisms they can use to participate in the ISE, and includes a

repository of relevant guidance, directives, and illustrative use cases. The ISE Management Plan will benefit stakeholders by demonstrably providing guidance on how ISE stakeholders:

- Identify, prioritize and resolving common problems;
- Assess and manage performance gaps;
- Harmonize policy;
- Convene communities of interest; and
- Leverage and extend good ideas, best practices, and tools.

The PM-ISE intends to document these management processes and the I^2F to increase awareness, facilitate stakeholder integration, and institutionalize management capabilities across the ISE.

IMPLEMENTATION ROADMAP

As previously done in the 2012 Annual Report, PM-ISE has updated an implementation roadmap to plan and coordinate a sustainable agency-based approach to accomplishing the goals and realizing the vision of the National Strategy, using the ISE Annual Planning Cycle, and the management processes described above and in Section 6 of this report. Over the past year, the ISE has undertaken a significant effort to clearly define and prioritize the challenges to realizing the vision of the National Strategy. This strategic gap analysis resulted in an interagency consensus on 16 priority objectives, outlined in the National Strategy, charting a path forward for the ISE.

CHANGE MANAGEMENT – BASED ON ONGOING AND ANNUAL ASSESSMENTS

The chart of the implementation roadmap that follows indicates which priorities and capabilities are now completed, and which are still outstanding. Those that are currently underway, overdue, or newly defined are also identified. The PM-ISE and agencies via the ISA IPC have used the ISE Annual Planning Cycle to update the Implementation Roadmap, anchored in the prior year's work, with a forward-looking view of advancing National Strategy priority objectives.

Extensive government-wide planning anchored in the ISA IPC has allowed for updating incomplete actions and detailing newly defined actions, sequenced across a multi-year horizon. Agencies are charged with implementation, and assessed with performance measures; all of which establishes a means for measuring progress toward National Strategy goals.

Those capabilities that are determined "complete" have been done so based on agency reports in the ISE performance questionnaire, tests of the mission-based scenarios, as well as the completion of milestones and delivery of outcomes assigned in the annual ISE Implementation Guidance. Agency implementation of the roadmap is subject to the availability of appropriations,

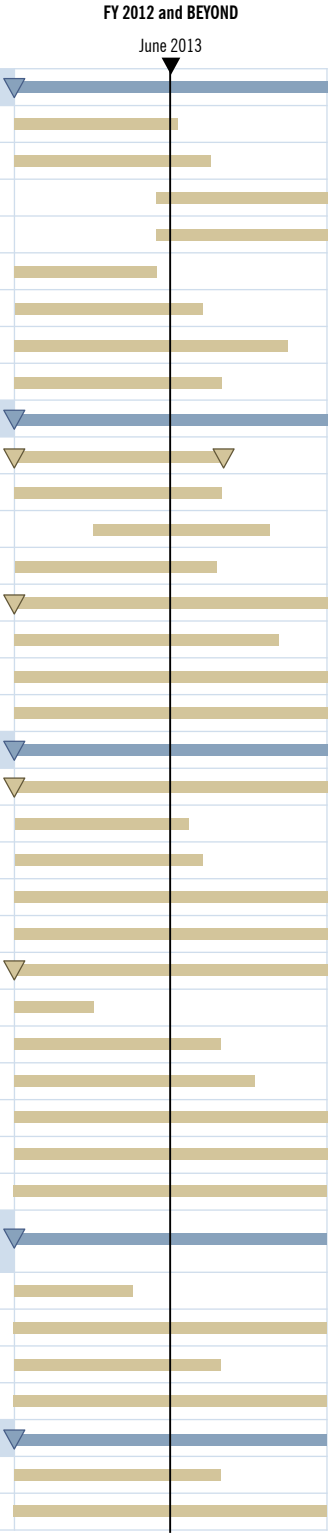
based on agency budgets, and regularly reviewed and adjusted through a change management process led by the ISA IPC.

Agency adoption and integration of the process and tools described in the ISE Management Plan and the I^2F will increase the maturity of ISE implementation planning, change management and investment management and the overall effectiveness of information sharing and safeguarding.

The implementation roadmap, framed by the goals of the National Strategy, and updated to include FY 2014 Implementation Guidance, is shown below:

IMPLEMENTATION ROADMAP

	GOALS, PRIORITIES, AND CAPABILITIES	START	FINISH
1	**DRIVE COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY**		
1-1	Fusion Center Performance Framework and Resource Allocation[1] – **Completed**	FY09	FY13
1-2	Expand NSI Participation[1, 2] – **Overdue**	FY09	FY13
1-3	Alerts, Warnings and Notifications[1] – **New**	FY13	Ongoing
1-4	Requests for Information (RFIs)[2] – **New**	FY13	Ongoing
1-5	Common Information Sharing Analytics[1, 2]	FY11	FY13
1-6	Critical Infrastructure and Key Resources Information Sharing[1, 2]	FY11	FY13
1-7	Governance and Performance Measurement [1,2]	FY11	FY14
1-8	Common Procedure and Templates for Information Sharing Agreements[2]	FY12	FY13
2	**IMPROVE INFORMATION DISCOVERY AND ACCESS THROUGH COMMON STANDARDS**		
2-1	ISE Technical and Functional Standards[1, 2]	FY12	FY13
2-2	Embed Geospatial Markup Language within NIEM[1]	FY10	FY13
2-3	Interoperability Framework[1, 2] – **New**	FY12	FY14
2-4	Data Aggregation Architecture[1, 2]	FY12	FY13
2-5	Access Control, Identity Management[1]	FY12	Ongoing
2-6	Public Key Infrastructure (PKI) IOC[1]	FY10	FY14
2-7	FICAM Implementation[1]	FY12	Ongoing
2-8	Plan and Integrate Controlled Unclassified Information Requirements[2]	FY10	Ongoing
3	**OPTIMIZE MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY**		
3-1	SBU Interoperability[1, 2]	FY12	Ongoing
3-2	Assured Credentials[1] – **Overdue**	FY11	FY13
3-3	Authoritative Attribute Sourcing[1]	FY12	FY13
3-4	Federated SEARCH[1]	FY09	Ongoing
3-5	Standards-based Acquisition[1, 2]	FY12	Ongoing
3-6	Domestic Information Sharing Architecture[1, 2]	FY12	Ongoing
3-7	SLTPS Access to Classified National Security Information[2] – **Completed**	FY10	FY12
3-8	Federal Switch for Indian Countries[1]	FY11	FY13
3-9	Case and Event De-confliction System Interoperability[1]	FY12	FY14
3-10	Public Safety Cloud[1] – **New**	FY12	Ongoing
3-11	Radiological Shipments, Licenses, and Cargo-Screening Information Sharing[1]	FY10	Ongoing
3-12	Global Nuclear Detection Architecture[1]	FY11	Ongoing
4	**STRENGTHEN INFORMATION SAFEGUARDING THROUGH STRUCTURAL REFORM, POLICY AND TECHNICAL SOLUTIONS**		
4-1	Agency Governance, Oversight and Performance Management – **Completed**	FY10	FY12
4-2	Agency-level Insider Threat Program Implementation[1]	FY09	Ongoing
4-3	SECRET PKI Implementation[1]	FY11	FY14
4-4	Audit Data Sharing, Security Reciprocity and Risk Assessment[1, 2]	FY10	Ongoing
5	**PROTECT PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES THROUGH CONSISTENCY AND COMPLIANCE**		
5-1	Issue Fusion Center, SAR and Federal Privacy Guidelines[1]	FY09	FY13
5-2	Enhance P/CR/CL Protections Across the ISE[1]	FY07	Ongoing



[1] FY 2013 and 2014 Implementation Guidance
[2] Supports implementation of an NSISS Priority Objective

Figure 8. Implementation Roadmap.

TARGETING CAPABILITIES NOT YET ACHIEVED

Those capabilities that have not yet been achieved are identified via the test scenarios, the annual performance questionnaire and gap analysis, and interagency planning efforts. We expect to see PM-ISE and our partner agencies deliver material progress on the following capabilities called for in the National Strategy during the next reporting period:

GOAL 1: DRIVE COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY

- Achieve a responsible information sharing culture that leverages best practices throughout government, both federal-wide and agency-based, including state, local, and tribal government as well as critical infrastructure and key resources, and private-sector stakeholders where appropriate (Figure 8: 1.6 and 1.7)
- Expanding re-use of existing information sharing tools and technologies, such as standardizing agency-level services to align across the ISE; creating common exchange processes across all levels of government to enable timely receipt and dissemination of information and appropriate responses (RFI and AWN); expanding NSI participation (Figure 8: 1.2, 1.3, and 1.4)
- Common procedures and templates for interagency information sharing agreements; reducing the time needed to build sharing agreements; more attention devoted to sharing information with the appropriate users in a timely and trusted manner (Figure 8: line 1.8)

GOAL 2: IMPROVE INFORMATION DISCOVERY AND ACCESS THROUGH COMMON STANDARDS

- Embedding geospatial tags into our ISE information sharing standards (Figure 8: 2.2)
- Improved communication of ISE requirements to allow industry adoption of interoperability frameworks (Figure 8: 2.3)
- Discovery and correlation of information across disparate holdings to allow data originators to see that responsible information sharing policies are enforced, and that authoritative, up-to-date information to identify relationships between people, places, things and characteristics that are not otherwise obvious are referenced (Figure 8: 2.4)

GOAL 3: OPTIMIZE MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY

- Assured credentialing across SBU security networks (Figure 8: 3.2)
- Authoritative attribute sourcing (Figure 8: 3.3)

- Transformation of a domestic information sharing architecture, integrating the community through participation in common task forces and functions to enable common functions, such as event deconfliction to promote officer safety (Figure 8: 3.6 and 3.9)

GOAL 4: STRENGTHEN INFORMATION SAFEGUARDING THROUGH STRUCTURAL REFORM, POLICY, AND TECHNICAL SOLUTIONS

- Insider-threat program implementation across all agencies that have access to classified information (Figure 8: 4.2)
- Shared audit and cyberthreat information on interconnected networks (Figure 8: 4.4)

GOAL 5: PROTECT PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES THROUGH CONSISTENCY AND COMPLIANCE

- Develop and implement effective compliance, oversight, and accountability mechanisms to ensure consistent application of mission-appropriate P/CR/CL protections. (Figure 8: 5.1 and 5.2)

PM-ISE VISION, MISSIONS, AND PRIORITIES

PM-ISE, in accordance with IRTPA, has documented a set of missions and priorities designed to further the ISE.

Necessarily an agile organization due to its multiple roles and responsibilities, PM-ISE is able to adjust to new requirements for responsible information sharing between federal, state, local, tribal, and private-sector partners. Though many ISE priorities are addressed through the separate governance structures, PM-ISE's role and authority as an executive agent allow for an integrated perspective and a unique view of complementary activities, dependencies, enabling cross-cuts, alignment, and overlapping missions.

With its integrated view of National priorities, PM-ISE has affirmed the following vision and missions to define its body of work for the next year, to include facilitating or supporting, coordinating and executing the ISE initiatives agreed to in the Implementation Roadmap.[63]

[63] Many items in the ISE Implementation Roadmap are led and executed by ISE agencies. In those cases, PM-ISE only serves in a monitoring role and therefore direct alignment will not be shown in the PM-ISE vision and mission.

VISION: NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

MISSIONS:

ADVANCE RESPONSIBLE INFORMATION SHARING TO FURTHER COUNTERTERRORISM AND HOMELAND SECURITY MISSIONS

- Innovate and standardize information sharing capabilities nationwide to support more effective and efficient decisionmaking (Figure 8: 3, 3.1, and 3.10)
- Transform the domestic information sharing architecture to better identify and respond to threats (Figure 8: 1.2, 3.6, and 3.10)
- Support technical implementation of cybersecurity information sharing efforts by extending the use of ISE tools (Figure 8: 2.3, 2.4, 3, and 4.4)

IMPROVE NATIONWIDE DECISIONMAKING BY TRANSFORMING INFORMATION OWNERSHIP TO STEWARDSHIP ACROSS ISE STAKEHOLDERS

- Achieve greater interoperability through consensus-based standards and increasing the use of standards in grants and acquisitions (Figure 8: 2.1, 2.3, and 3.5)
- Interconnect existing networks and systems with strong identity, access, and discovery capabilities (Figure 8: 2.5 and 2.7)
- Standardize, reuse, and automate information sharing policies and agreements with strong protection of privacy, civil rights, and civil liberties (Figure 8: 1.8 and 5)

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

- Align and institutionalize governance to foster better decisionmaking, accountability, and implementation (Figure 8: 1.1, 1.7, and 4.1)
- Build responsible information sharing culture and capabilities through engagement, coordination, training, the sharing of best practices, and performance management (Figure 8: 1.6, 1.7, and 3.8)

CONCLUSION

We have faced exceptional challenges over the past year, including new and evolving threats, increasing amounts of data to manage, and a constrained fiscal environment. PM-ISE and our partners have continued to make progress in advancing our vision of national security through responsible information sharing. Collectively we have laid a path and are building on existing efforts to strengthen national capabilities.

As the National Strategy outlines in its Way Forward:

> Together, we can reach beyond legacy information sharing protocols and embed in our missions and cultures the assurance decisions are better informed when supported by all relevant information. This also requires, however, a balanced commitment to appropriately safeguard information, its sources, and collection methods, while also respecting legal and policy restrictions on use. Success depends upon the collective ability to achieve equilibrium between sharing and safeguarding, build on past successes, and continue the maturation of the Information Sharing Environment.

In the coming year, we will continue to use all of our tools and capabilities to support implementation of the National Strategy and to build a stronger information sharing environment. Together with our mission partners, we will enhance national security through responsible information sharing.

ENDNOTES

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

[xlviii] IRTPA §1016(b)(2)(C)(F)
[xlix] IRTPA §1016(b)(2)(E)(I), (h)(2)(H)
[l] IRTPA §1016(b)(2)(C)(F)(J)(L)
[li] IRTPA §1016(b)(2)(A)(C)(F)(K), (h)(2)(D)
[lii] IRTPA §1016(b)(2)(C)(F)
[liii] IRTPA §1016(b)(2)(C), (h)(2)(H)
[liv] IRTPA §1016(b)(2)(A)(D)(F)
[lv] IRTPA §1016(b)(2)(C), (h)(2)(H)
[lvi] IRTPA §1016(b)(2)(A)(C), (h)(2)(H)
[lvii] IRTPA §1016(h)(2)(D)
[lviii] IRTPA §1016(b)(2)(A)(B)(D)(F)(J)(K)(M)
[lix] IRTPA §1016(b)(2)(C)(F)(J), (h)(2)(D)
[lx] IRTPA §1016(b)(2)(E)(I)
[lxi] IRTPA §1016(b)(2)(E)(F)(I)
[lxii] IRTPA §1016(b)(2)((I)(O)
[lxiii] IRTPA §1016(b)(2)(A)(B)(F)
[lxiv] IRTPA §1016(b)(2)(A)(D)(F)(J)
[lxv] IRTPA §1016(b)(2)(A)(B)(C)(D)(E)(F)(J)(K)(L)(M)
[lxvi] IRTPA §1016(A)(D)(F)(K)(N)
[lxvii] IRTPA §1016(b)(2)(I)(O), (h)(2)(J)
[lxviii] IRTPA §1016(b)(2)(E)(I)
[lxix] IRTPA §1016(h)(2)(J)
[lxx] IRTPA §1016(h)(2)(I)
[lxxi] IRTPA §1016(h)(2)(B)

APPENDICES

This page intentionally left blank.

APPENDIX A – ISE PERFORMANCE DATA

This Report provides an executive-level summary of ISE activities over the previous year to illustrate the major focus areas and investments by ISE agencies, and provides a basis of performance analysis by the office of the 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 ISE Annual Performance Assessment; and
- Identification of gaps and opportunities for improvement to better inform future investments.

HIGH-LEVEL ANALYSIS OF THE ANNUAL ISE PERFORMANCE ASSESSMENT REPORT

The ISE Performance Framework, detailed in Section 6 of this Report, defines three stages of maturity to communicate expected capabilities for the following year.

Maturity Stage 1 – capabilities currently expected for ISE agencies;

Maturity Stage 2 – capabilities that are expected to be developed two to three years from baseline; and

Maturity Stage 3 – capabilities that are expected five to seven years from baseline.

2013 is the first, full performance assessment year after the 2012 baseline year. Analysis in this Report focuses on Maturity Stage 1 initiatives and capabilities, some of which are incorporated into National Strategy for Information Sharing and Safeguarding (National Strategy) implementation plans.[64] Overall, the 2013 ISE Performance Assessment found no statistically significant[65] increase in performance for Maturity Stage 1 initiatives and capabilities when compared to the 2012 baseline analysis.

[64] The National Strategy employed an extensive gap analysis which resulted in the creation of 16 Priority Objectives required to implement the vision for the Strategy. These gaps will not be covered comprehensively in this analysis, but are discussed elsewhere in this Report.

[65] Statistical significance – at least 0.05.

Early implementation planning for many of the 2013 performance focus areas was incorporated into the 16 priority objectives in the National Strategy, released in December 2012.[66] The implementation roadmap, discussed previously in the Way Forward section, provides actions, milestones, and accountability leads that are aligned with the priority objectives in the National Strategy.

GAPS, CHALLENGES, AND OPPORTUNITIES

In the process of compiling this Report, and based on collaboration with ISE agencies, PM-ISE identified several additional gaps, challenges, and opportunities for improvement of the ISE.

Significant findings on key issues from 2012 are compared in tables below with the findings from this year's assessment on like issues. The tables are aligned to the five goals in the National Strategy and identify areas that (1) were not meeting Maturity Stage 1 expectations as previously reported in 2012 compared with 2013 findings and mitigation activities,[67] (2) are Maturity Stage 2 and 3 areas of assessment that are at risk, and (3) represent additional gaps, challenges, and opportunities for improvement for ISE.

Most departments and agencies are meeting Maturity Stage 1 expectations; however, there are underperforming areas which are identified in this report. 2014 will be the first execution year for Maturity Stage 2 initiatives, and ISE agencies are well positioned to meet the expected goals. Data from the 2013 ISE performance assessment suggest that some select Stage 2 and 3 issues require closer management oversight to meet forecasted expectations.

Near-term actions to address these issues are reflected in the high-level implementation roadmap found in the Way Forward section of this Report. The roadmap includes implementation guidance from the PM-ISE to the agencies, based upon White House priorities for information sharing and safeguarding. PM-ISE and the ISA IPC will monitor ISE agency efforts to implement White House guidance through the governance and performance management processes outlined in Section 6 of this Report.

[66] 75% of the questions in the 2013 Performance Assessment Questionnaire (PAQ) were constant from the 2012 questionnaire. The remaining 25% of questions were expanded to focus on newly identified gaps from the 2012 assessment and new mission areas identified through strategic planning by federal governance bodies. Publishing the 2012 National Strategy in December of 2012 allowed for the 2013 ISE Performance Assessment to be explicitly aligned to National Strategy goals and sub-goals, giving the ISE a clear strategic footing for monitoring progress.

[67] Further details can be found in the body of the report.

NATIONAL STRATEGY GOAL 1 – COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY	
2012 FINDINGS – MATURITY STAGE 2 AND 3	**2013 FINDINGS – MATURITY STAGE 2 AND 3**
PUBLIC-PRIVATE SECTOR INFORMATION SHARING GAP	
• According to the National Infrastructure Advisory Council (NIAC), federal-private sector information sharing was still immature, leaving a large gap in public-private sector information sharing. • In particular, intelligence sharing between Federal Government and private sector operators of critical infrastructure was lagging behind the "marked improvements" the NIAC observed in the sharing of federal intelligence with state, local, tribal, and territorial (SLTT) governments over the last several years.	• Many challenges noted in last year's report with respect to sharing information between the federal government and private sector owner/operators of critical infrastructure persist, but there has been a concerted effort on the part of the Federal Government to address the NIAC report findings over the past twelve months. Details of these activities are included in Section 1 of this Report, under the heading, "Private Sector Information Sharing."
OPPORTUNITIES TO IMPROVE SUSPICIOUS ACTIVITY REPORTING ANALYSIS	
No corresponding 2012 finding.	• PM-ISE released a report, "Improving Suspicious Activity Reporting (SAR) Analysis." PM-ISE is working with DHS and FBI to address the findings and recommended mitigation strategies in the report. • Fusion centers reported that the inability to download ISE-SAR data from the NSI Federated Search Tool and/or eGuardian limits fusion center analysts' ability to integrate information into their analytic processes. • In addition, many fusion centers report they do not have a consistent process for incorporating ISE-SAR into their analytic workflow; and, that the ISE-SAR Functional Standard needs to be updated to bring the document up-to-date with current analysis on behaviors and indicators of violent extremism and mobilization to violence. • As of January 2013, 56 federal agencies, representing 226 individual organizations are in various stages of NSI participation, and four additional agencies have been identified that may be able to participate. Of the 56 agencies, 21 are NSI-compliant.
RFI/AWN COMMON PROCESSES	
No corresponding 2012 finding.	• Federal Operation Centers' have not adopted a common RFI exchange process and lack both a common AWN information exchange process and information exchange protocols.

NATIONAL STRATEGY GOAL 1 – COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY	
2012 FINDINGS – MATURITY STAGE 2 AND 3	**2013 FINDINGS – MATURITY STAGE 2 AND 3**
TRIBAL INFORMATION SHARING GAPS	
• There were opportunities to increase tribal information sharing through the National Network of Fusion Centers. • PM-ISE and its federal partners were focused on addressing and improving some of the foundational policy, governance, relationship, and capacity issues related to tribal information sharing. • SLT partners were expanding tribal participation through Fusion Liaison Officer (FLO) programs.	• As noted last year, gaps continue in tribal information sharing. Challenges include lack of resources, reluctance of some states to allow tribal law enforcement access to federal and state databases, tribal reluctance to engage outside law enforcement entities, and insufficient training on fusion center capabilities. • PM-ISE, in coordination with DOI, BIA, DOJ, OTJ, NCTC, FBI, DHS, and IACP convened the Tribal Information Sharing Working Group (TISW) to examine information sharing in Indian County. As of April 2013, the TISW identified eight major findings that hinder tribal information sharing and is developing recommendations for mitigation.
ISE AGENCY INCENTIVES FOR INFORMATION SHARING AND SAFEGUARDING ACTIVITIES	
No corresponding 2012 finding.	• Responses to the 2013 ISE Performance Assessment Questionnaire show mixed results with respect to agency adoption and implementation of incentive tools for information sharing and safeguarding. • 90% of responding agencies—a 10% increase from last year—reported that "information sharing and collaboration" is an evaluated performance objective for employees with direct ISE responsibilities. • Responding agencies reported a decrease in the nomination of candidates for information sharing and collaboration awards from last year.[68]

[68] It is unclear what caused the decline—one possible explanation is that specific incentives for information sharing are less likely to be awarded as information sharing and collaboration are gradually becoming key components of job functions, especially those jobs that require interagency collaboration. This supposition is supported by the increase in employee information sharing performance objectives and the fact that 71% of agencies, up from 62% last year, report that they offer mission-specific training that supports information sharing and collaboration. Although there is no supporting data, it is also possible that the current fiscal environment has made it necessary to cut back on monetary awards. Further analysis is being done to understand these results.

NATIONAL STRATEGY GOAL 1 – COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY	
2012 FINDINGS – MATURITY STAGE 2 AND 3	2013 FINDINGS – MATURITY STAGE 2 AND 3
THE NEED TO TRANSFORM INFORMATION SHARING BUSINESS MODELS	
• 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. • 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.	• The 2012 finding that cost savings could be realized is still valid. • Global Justice Sharing Initiative put out a call to action in November 2012 to develop single-sign-on capabilities; leverage cloud solutions; develop shared services; ensure interoperability between law enforcement systems; and, collaborate with Federal partners to coordinate federal funding, policy support, and adoption of common standards and technologies. • To further interoperability between law enforcement deconfliction systems, PM-ISE is sponsoring a nationwide deconfliction strategy should be initiated to include identifying deconfliction standards and interface deconfliction systems.

NATIONAL STRATEGY GOAL 2 – INFORMATION DISCOVERY AND ACCESS THROUGH COMMON STANDARDS	
2012 FINDINGS – MATURITY STAGE 2 AND 3	**2013 FINDINGS – MATURITY STAGE 2 AND 3**
ENTITY DATA TAGGING	
• 65% of ISE agencies reported little or no progress in working towards metadata tagging solutions—this reduces agencies' ability to automate access decisions based upon user and data attributes, and hinders the ability to discover and retrieve data, perform analysis, and maintain provenance and lineage on terrorism-related data.	• Agencies reported progress on working towards metadata tagging solutions. ◦ DoD CIO is implementing the DoD Joint Information Environment and the Office of the Director of National Intelligence is implementing IC Information Technology Enterprise (IC ITE)—both are using DoD Architecture Framework (DoDAF) artifacts which enable cross domain sharing. ◦ DHS and Department of Transportation are developing data tagging implementation plans for discovery and access control on their networks.
DATA AGGREGATION	
• Centralized data correlation and data storage introduces privacy and security challenges that limit mission effectiveness. • The development of 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.	• The challenges to enterprise data correlation noted in last year's findings persist. • Development of data aggregation architecture is a priority objective of the National Strategy, as are priority objectives to adopt metadata standards to facilitate discovery, access, and monitoring across networks and security domains, and define and implement common standards to support automated discovery and access decisions.

NATIONAL STRATEGY GOAL 3 – OPTIMIZING MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY	
2012 FINDINGS – MATURITY STAGE 2 AND 3	**2013 FINDINGS – MATURITY STAGE 2 AND 3**
ASSURED NETWORK INTEROPERABILITY	
• Approximately one-half of ISE agencies implemented interconnection plans for SBU/CUI networks supporting ISE-related missions. • A constrained fiscal environment, fragmented architectures, and policy challenges hindered agency efforts in this area. • To help address these gaps, the SBU/CUI Interoperability Working Group was focusing on identity and access management (IdAM) solutions to provide a simplified sign-on capability between mission partners' SBU and CUI networks.	• Resource constraints continue to impact interoperability efforts for SBU/CUI networks, with only 40% of ISE agencies this year reporting having implemented interconnection plans for SBU/CUI networks supporting ISE related missions.[69] • In 2012 Integration Sub-Committee established the Identity Federation Coordination working group to improve governance of identity-related efforts across the federal government and across all security domains.
ISE MISSION SYSTEM ACQUISITION PROCESSES	
• Only about 50% of ISE agencies considered ISE functional and technical standards when issuing grants or requests for proposals (RFP) for ISE-related system acquisitions. • PM-ISE, in partnership with GSA, began several efforts to address the standards-based acquisition issue and to develop a baseline set of standards for information exchange. • PM-ISE intended 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.	• Only about 50% of ISE agencies consider ISE functional and technical standards when issuing grants or RFPs for ISE-related systems. • While guidance actions were issued for updating grant and acquisition language to support the use of common standards, 43% of agencies have not provided best-practice recommendations to support this initiative. • PM-ISE is working with GSA to leverage National Strategy implementation actions to accelerate the use of information sharing standards in acquisition language, and to foster reuse of these standards across the ISE mission partners. HHS, as a co-chair of the Council on Financial Assistance Reform, is actively working on incorporating standards guidance in grant language guidance.

[69] IdAM solutions will continue to be a focus area until this gap is closed.

NATIONAL STRATEGY GOAL 3 – OPTIMIZING MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY	
2012 FINDINGS – MATURITY STAGE 2 AND 3	**2013 FINDINGS – MATURITY STAGE 2 AND 3**
FEDERATED IDENTITY MANAGEMENT	
• 33% of ISE agencies did 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 was 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.	• Federated identity management progress continues incrementally. ◦ The percentage of agencies (from the 2012 population) that did not practice IT security reciprocity with other federal agencies decreased to 10% from 33% ◦ All responding agencies reported progress in implementing federated identity management solutions aligning to the FICAM roadmap • The BAE pilot continues to progress, with PM-ISE and GSA developing 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). • In addition, ISA IPC Information Integration Subcommittee (IISC) led the Federal Cloud Credential Exchange project to provide a shared service for validation of third party credentials, and the IISC's Federated Identity Management Working Group developed a guide for federal agencies on how to accept third party credentials.
LEGISLATIVE SUPPORT FOR SHARED SERVICES	
• No corresponding 2012 finding.	• Many of the current budget models for IT do not allow for flexibility, pooling, and extending the availability of funding. Support for removing limits on transferring funding across appropriations and agencies will better allow for provisioning common administrative IT services.
ESTABLISHING AN ENTERPRISE ARCHITECTURE MANAGEMENT CAPABILITY	
• No corresponding 2012 finding.	• PM-ISE began developing an ISE Interoperability Framework (I^2F) which will align enterprise architecture frameworks used by ISE partners and promote tools and methodologies that advance interoperability.[70]

[70] I2F addresses GAO's High Risk List action item – GAO recommended establishing an enterprise architecture management capability to guide projects designed to further implement the ISE.

NATIONAL STRATEGY GOAL 4 – STRENGTHENING SAFEGUARDING OF INFORMATION	
2012 FINDINGS – MATURITY STAGE 2 AND 3	**2013 FINDINGS – MATURITY STAGE 2 AND 3**
CLASSIFIED INFORMATION SHARING AND SAFEGUARDING GOVERNANCE GAPS	
• 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 was positioned for continued improvements in classified information sharing and safeguarding in the next year.	• Our continuing efforts in the these priority areas will improve security by strengthening the identification of individuals accessing classified systems, limiting access on a basis of the individual's "need-to-know" through technical controls, reducing the opportunity for information to be removed from the secure environment, improving efforts against insider threats, and improving audit capabilities.
OPPORTUNITY WITH CYBERSECURITY INFORMATION SHARING	
• Cybersecurity can be improved through effectively sharing cyber-vulnerability and intrusion information. • ISE's information sharing processes can enable cybersecurity information sharing.	• Comprehensive National Cybersecurity Initiative Five led the Federal Cybersecurity Centers[71] to document requirements for sharing cybersecurity information into an information sharing architecture (ISA). Implementation of the ISA was selected as one of the President's Cybersecurity Advisor's top priorities for FY 2014. • Federal Emergency Management Agency's National Exercise Division conducted National Level Exercise (NLE) 2012,[72] a series of exercise events that examined the ability of the United States to execute a coordinated response to a series of significant cyber incidents. One of the four overarching objectives that guided NLE 2012 was to examine the ability to share information across all levels of government and with the private sector as well as the general public, to create and maintain cyber incident situational awareness, and coordinate response and recovery efforts.

[71] Federal Cybersecurity Centers are: NSA/CSS Threat Operations Center (NTOC), DHS National Cybersecurity Communications and Integration Center (NCCIC), US-Cyber Emergency Response Team (US-CERT), National Cybersecurity Investigative Joint Task Force (NCI-JTF), Intelligence Community Incident Response Center (IC-IRC), USCYBERCOM Joint Operations Center (JOC).

[72] Federal Emergency Management Agency Quick Look Report National Level Exercise 2012, March 2013.

NATIONAL STRATEGY GOAL 5 – PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES	
2012 FINDINGS – MATURITY STAGE 2 AND 3	**2013 FINDINGS – MATURITY STAGE 2 AND 3**
CONSISTENT, GOVERNMENT-WIDE APPLICATION OF PRIVACY PROTECTIONS	
• Compliance with the requirements of the ISE Privacy Guidelines remained incomplete. • Six years after the issuance of the ISE Privacy Guidelines, a small number of ISE agencies were 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 was 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.	• ISE agencies continue to develop and implement privacy protection policies as required by the 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.[73] • Department of Defense (DoD) has revised its directive to conform DoD with ISE Privacy Guidelines in lieu of issuing a separate DoD privacy policy. • PM-ISE and the ISA IPC Privacy and Civil Liberties Subcommittee have monitored progress of and provided technical assistance to remaining ISE departments and agencies.
PRIVACY COMPLIANCE	
• Of the agencies with privacy policies, 79% made no progress in verifying that their ISE-enabling business processes are in compliance with their ISE privacy policy. • Approximately 33% of agencies with ISE privacy policies completed those policies within the past 12 months—agencies were still in the initial stages of implementing ISE privacy protections and policies. • Agencies with established policies reported 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) was 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.	• While there have been initiatives to measure and ensure privacy compliance, there currently is not an effective ISE-wide performance measurement for internal agency compliance, oversight, and accountability mechanisms to ensure consistent application of P/CR/CL protections.[74]

[73] Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the "information sharing environment" (ISE).

[74] The development of these measures is a priority for the ISA IPC Privacy and Civil Liberties Subcommittee.

NATIONAL STRATEGY GOAL 5 – PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES	
2012 FINDINGS – MATURITY STAGE 2 AND 3	2013 FINDINGS – MATURITY STAGE 2 AND 3
PRIVACY COMPLIANCE	
• Of the agencies with privacy policies, 79% had made no progress in verifying that their ISE-enabling business processes are in compliance with their ISE privacy policy. • Approximately 33% of agencies with ISE privacy policies completed those policies within the reporting period—agencies were still in the initial stages of implementing ISE privacy protections and policies. • However, agencies with established policies reported consistent progress in implementing ISE policies, including the proactive integration of protections into the development of new systems and initiatives, contributing to the maturity of agency protection capabilities.	• Agency reporting shows an increase in maturity for the implementation of ISE privacy protections and policies since last year—yet, while 87% of agencies reported having adequate review or audit mechanism in place to verify personnel compliance with the ISE Privacy Guidelines, only 79% of agencies reported have ISE privacy protection policies in place. • A standardized model for compliance in the form of a compliance self-assessment tool is being finalized by the P/CL Subcommittee to further assist federal ISE mission partners in identifying gaps and providing more detailed and measured performance reporting.

As discussed in the body of this Report, the ISE Performance Framework allows the office of the PM-ISE to 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. The framework for the assessment and the details of the data are described below.

Seventy-five percent of the 2013 ISE PAQ (detailed later in this appendix) was constant from the 2012 questionnaire. The remaining questions were expanded to focus on newly identified gaps from the 2012 assessment and new mission areas identified through strategic planning by federal governance bodies. Publishing the 2012 National Strategy in December of 2012, allowed for the 2013 ISE Performance Assessment to be explicitly aligned to its goals and sub-goals, giving the ISE a clear strategic footing for monitoring progress.

Responses to the 2013 ISE PAQ 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.

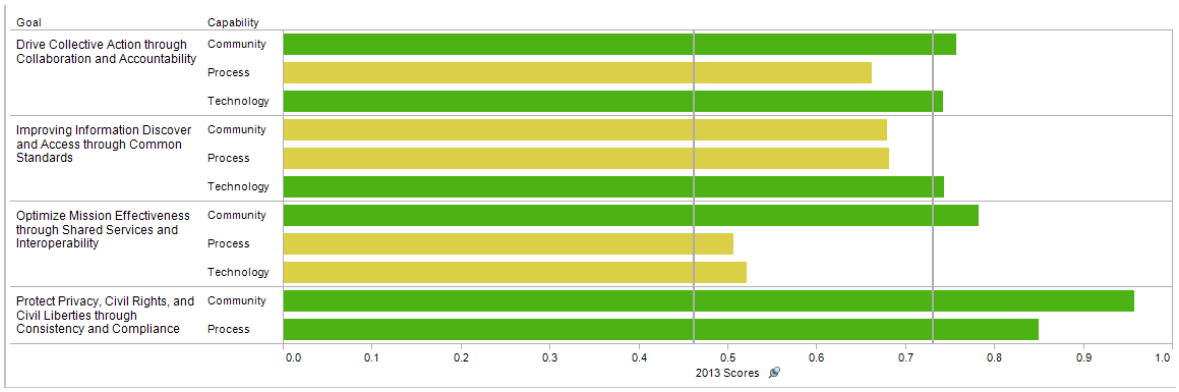


Figure 9. Overall 2013 ISE Performance by Goal and Capability Area

The goals and sub-goals are aligned to the Administration's strategic guidance, priorities, and to the required ISE attributes per IRTPA Section 1016(b)(2). Each ISE performance assessment question is aligned to a specific subtopic, maturity stage, and to the capability areas of community, process, and technology. These alignments allow PM-ISE to use agency responses to the ISE PAQ to determine ISE-wide progress against both the Administration's priorities and the attributes of the ISE, while maturing community involvement, and process and technology adoption and use. As 2012 was a baseline year for PM-ISE's performance methodology and a year for finalizing the National Strategy, responses to "Maturity Stage 1" questions remain 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 indicate that the PAQ did not address certain goals and sub-goals for a given maturity stage).

Table A-1. Overall 2013 ISE Performance by Goal, Sub-goal, and Maturity Stage.

		MATURITY		
GOAL	SUB-GOAL	Stage 1	Stage 2	Stage 3
Drive Collective Action through Collaboration and Accountability	Encourage Progress through Performance Management, Training, and Incentives			
	Improve Governance and Remove Barriers to Collaboration			
	Mature the Use of Common Operating Models			
	Streamline the Development of Information Sharing Agreements			
Improve Information Discover and Access Through Common Standards	Develop Clear Policies and Rules for Discovery and Access			
	Drive the use of Information Sharing Standards			
	Enhance Enterprise-wide Data Correlation			
	Improve Identity, Authentication, and Authorization Controls			
Optimize Mission Effectiveness through Shared Services and Interoperability	Improve Assured Data Services, and Network Interoperability			
	Leverage Collective Demand through Acquisition			
	Share Services that Benefit All Partners			
Protect Privacy, Civil Rights, and Civil Liberties through Consistency and Compliance	Build Protections into the Development of Information Sharing Operations			
	Ensure Accountability and Compliance Mechanisms			
	Increase Consistent Government-wide Application of Privacy Protections			

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.

Table A-2. ISE Performance Framework Capability Areas and Maturity Stages.

	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.

The following sixteen departments and agencies participated in the 2013 ISE PAQ:

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

TRENDS FROM THE 2012 ISE PERFORMANCE ASSESSMENT QUESTIONNAIRE

Due to the planning efforts around the new National Strategy, there has been little change from the 2012 to the 2013 assessment responses on the whole. With agencies that have participated in both the 2012 and 2013 assessments, there were generally consistent overall response scores (or a very slightly positive overall trend), with a notable exception in the privacy area, where significant improvement was made.

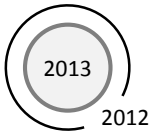
Agency responses are detailed below. For those questions carried over from the 2012 ISE PAQ, comparisons are provided detailing how the ISE departments and agencies changed year over year. In addition, agencies were requested to provide narrative examples of activity for all relevant questions and comments that further explain their response choice. 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.

The graphics below detail the trends from the 2012 to 2013 responses where the same agencies answered in both years to show a direct comparison. The legend accompanying the graphics in the upper corner of the page describes that the inner pie chart displays the 2013 response while the staggered outer ring displays 2012 data. The colors represent the same response from each year. For example, the Yes-No questions are either designated by the color green ('Yes') or red ('No') for both the inner pie chart and outer ring. An outer ring will not be displayed for those questions only asked in 2013.

The percentages depicted below are based on the total number of responding agencies for this question. For example, if only 15 out of the 16 agencies responded to a "Yes/No" question and 10 responded "Yes," the resulting percentage would be 67% (10 out of 15).

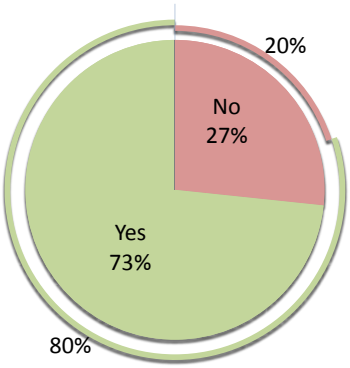
The 2013 ISE PAQ population differed slightly from 2012. Army Intelligence, Marine Corps Intelligence, and the Defense Intelligence Agency responded to the 2012 ISE PAQ but did not submit responses to the 2013 ISE PAQ. In 2012, the Federal Bureau of Investigation responded independently to the ISE PAQ, but its responses in 2013 were consolidated with the Department of Justice submission along with the Drug Enforcement Agency and the Bureau for Alcohol, Tobacco, and Firearms. In addition, the 2013 ISE PAQ allowed agency sub-components to answer and consolidate responses for agency scoring. The question by question analysis below shows all (sub-agency) responses, where applicable.

Due to the assessment population differences, PM-ISE only performed trending analysis on the common respondents *and* questions between 2012 and 2013. It is for this reason that data cannot as a whole be directly compared between the 2012 and 2013 ISE Annual Reports.



COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY

Question:
Does your agency utilize eGuardian (FBI)?



# of Responses: 15

Maturity Level (1-3): 1

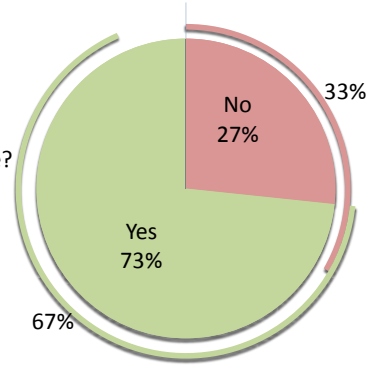
DOJ: Yes - The Protective Operation Group, Security Operations Section, Security Division, utilizes eGuardian in conducting protective intelligence threat assessments and risk assessments in support of protection strategies for threatened employees. It is also utilized for Domain assessments in support of travel of executives and information on persons who have demonstrated an inappropriate interest in the FBI or its personnel.

DOI: Yes - We use eGuardian as our SAR shared space.

DoD: Yes - Currently, there are 1396 DoD eGuardian accounts.

DOT: Yes - E-Guardian is primarily used by the Department of Transportation member assigned to the FBI's National Joint Terrorism Task Force.

Question:
Does your agency participate in the Nationwide Suspicious Activity Reporting Initiative?



# of Responses: 15

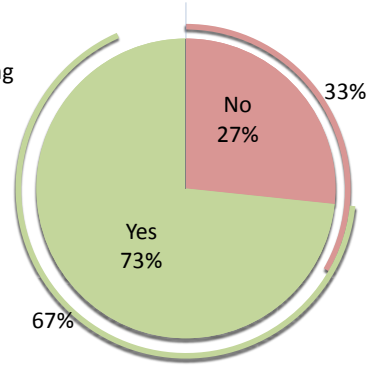
Maturity Level (1-3): 1

DOJ: Yes - Both the department and components participate in SAR. The Bureau of Justice Assistance (BJA), within the Office of Justice Programs (OJP) is the program manager for the NSI. BJA works extensively with state & local law enforcement, which includes providing training materials and coordinating the national rollout of the NSI.

DOS: No - Diplomatic Security (DS) is aware of the NSI and anticipates providing SARs in the future. DS has been upgrading SIMAS to make it compliant with the SBU Interoperability Fabric being implemented by the National SARs Initiative.

HHS: Yes - HHS is establishing a liaison effort with the FBI to input SAR information into eGuardian. HHS is beginning to implement a department wide notification process which will provide guidance to the physical security staff how to report events.

Question:
Does your agency provide SAR training (either directly or indirectly)?



# of Responses: 15

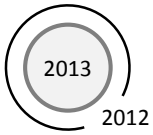
Maturity Level (1-3): 1

DHS: Yes - DHS does provide analytic training on the use of SAR for Component personnel and state and local analysts.

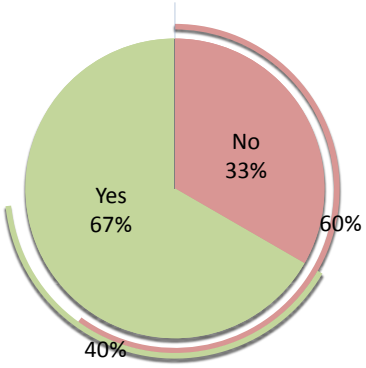
DOJ: Yes - BJA/OJP develops SAR training materials in conjunction with federal SLT authorities and fusion centers.

DOT: Yes - For Department of Transportation (DOT) employees in general, training was provided on how to submit a "Quick SAR" via DOT's Intranet. As for individual designated officials from each of the DOT modes of transportation, these officials were provided training on how to use Blue Mercury—that is, access the database, input information, and monitor the flow of information into Blue Mercury from their individual modes.

NGA: Yes - eGuardian training is provided directly to those individuals who have eGuardian user accounts. Also, annual Antiterrorism Level I training (both instructor-led and via CBT) for all employees includes SAR training.



Question:
Does your agency have a live SAR database?



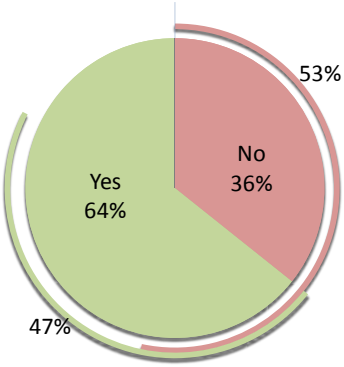
# of Responses: 15

Maturity Level (1-3): 1

DHS: Yes - Authorized DHS participants use the SAR Vetting Tool (SVT); a tool developed by NSI that enables DHS participants to evaluate whether a properly collected SAR meets the criteria to be considered an ISE-SAR and should be contributed to the DHS ISE-SAR Server.

HHS: Yes - We currently utilize the LEO accounts to enter information into eGuardian-Guardian. In the near future we will have direct access to eGuardian to facilitate the entering and sharing of information.

Question:
Does your agency have a process in place to validate SARS?



# of Responses: 14

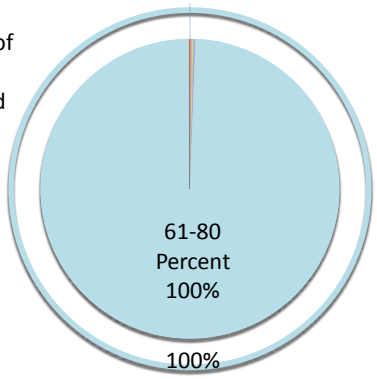
Maturity Level (1-3): 1

DHS: Yes - DHS uses the ISE-SAR vetting approach defined within the ISE Functional Standard.

DOT: Yes - Each SAR received in the Office of Intelligence, Security, and Emergency Response is vetted by one of the intelligence analysts to determine the validity of the SAR. Once vetted, and if there is a terrorism nexus, the SAR is sent forward to NSI.

NGA: Yes - SARs are validated by the responsible JTTF. NGA conducts preliminary investigations to determine potential threats, and develops necessary mitigation measures to counter and/or defeat terrorist operations.

Question:
What percentage of critical milestones has the NSI-related Security Incident Management and Analysis System (SIMAS) program met successfully?

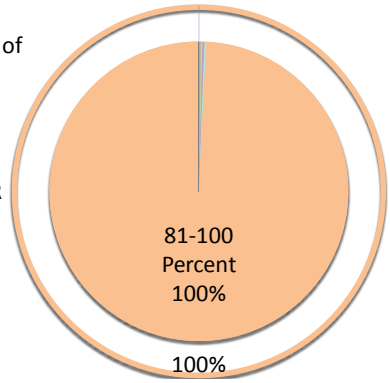


# of Responses: 1

Maturity Level (1-3): 1

DOS - The current SIMAS project (75% complete) will result in the replacement of the existing system. The new system will capture and store SAR related data in a NIEM compliant manner. The current project will establish the foundation from which a new future project may be executed that will result in the transmission of this data to external entities. The current milestones are not inclusive of the efforts that will be needed to implement a data sharing infrastructure, approvals and associated inter-agency agreements.

Question:
What percentage of State and Major Urban Fusion centers has your agency provided training to in CIKR issues?

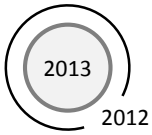


# of Responses: 2

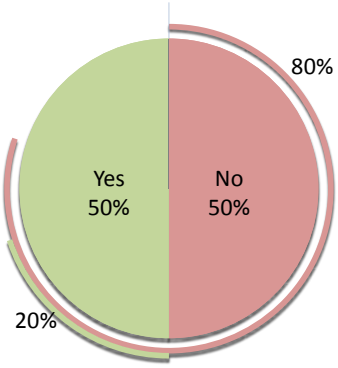
Maturity Level (1-3): 2

DOJ - The NSI PMO provided SAR awareness training for private sector security officers to all 78 fusion centers.

DHS - 86%. This covers the 52 "Major and Urban" fusion centers. Although there are 25 additional recognized fusion centers, there has been no staff trained from primary fusion centers in Hawaii, New Hampshire, New Mexico, Oregon, Puerto Rico, South Dakota, nor the U.S. Virgin Islands. Training has been provided through the delivery of the National Protection and Programs Directorate/Infrastructure Protection (NPPD/IP) Field Resource Toolkit, and the Introduction and Intermediate Risk Analysis Courses for Fusion Center Analysts



Question:
Does your agency use a government wide template in developing information sharing agreements?



# of Responses: 14

Maturity Level (1-3): 2

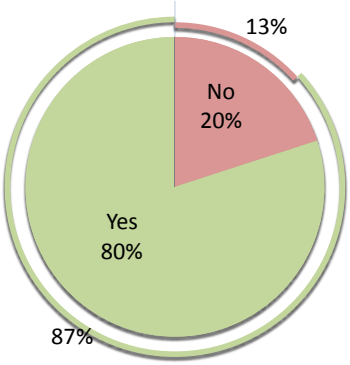
DHS: Yes - uses a standard MOA template for use with all Federal Departments/Agencies. The Information Sharing and Collaboration Branch facilitates these agreements.

DOJ: No - By corporate policy, the FBI uses a standard template for all FBI MOUs. The FBI, however, is unaware of the existence of a single government-wide MOU template or associated process to ensure consistency and coherence among and between interagency information sharing agreements.

DoD: No - The DoD does not use a government wide template in developing information sharing agreements. However, DoD is an active participant in National Strategy for Information Sharing and Safeguarding (NSISS) implementation plan activities, to include Priority Object 2 which include work to develop such a template based on common legal and policy compliance requirements.

TREAS: Yes - IRS only: The GLD Office maintains templates for business MOU/MOAs. Cybersecurity maintains the ISA templates which follow NIST SP 800-47 Appendices A&B.

Question:
Does your agency participate in the National Joint Terrorism Task Forces?



# of Responses: 15

Maturity Level (1-3): 2

DoD: Yes - Currently, the U.S. Army Criminal Investigative Command (CID) has two Agents at the National Joint Terrorism Task Force (NJTTF) and one Agent at the Dallas JTFF.

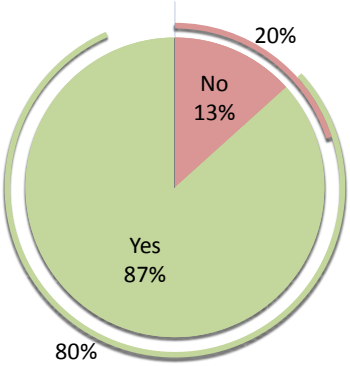
DOT: Yes - The Department of Transportation (DOT) has assigned a member of the Office of Intelligence, Security, and Emergency Response, Intelligence Division fulltime to support the NJTTF working a range of LE and IC related issues that impact DOT.

TREAS: No - IRS-CI has allocated one full-time Senior Analyst to the NJTTF.

DOI: Yes - We have a full-time and a part-time person assigned to the FBI NJTTF.

DOS: Yes - We participate in 28 locations.

Question:
Does your agency participate in the Joint Terrorism Task Forces (FBI)?

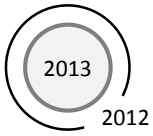


# of Responses: 15

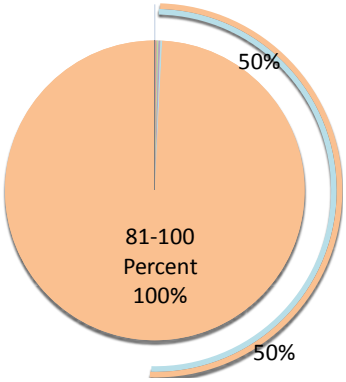
Maturity Level (1-3): 2

TREAS: Yes - OIA participates on a limited basis, as mission dictates. 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. The classification of their position is based on the availability of the CI agent and work in the area of assignment.

DOI: Yes - We have full-time, part-time and liaison officer positions.



Question:
What percentage of State and Major Urban Fusion centers has your agency provided training to in Analytics?

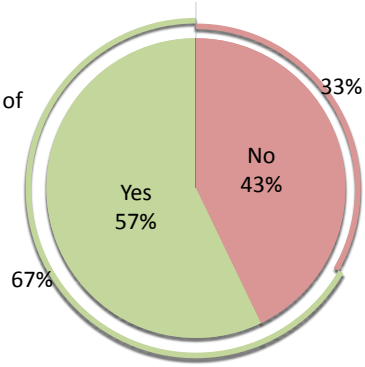


# of Responses: 1

Maturity Level (1-3): 2

DOJ: 81-100% - BJA: 95% of fusion centers (74 of 78) have received analytic training.

Question:
Does your agency participate in the National Network of Fusion Centers (state and major urban areas)?



# of Responses: 14

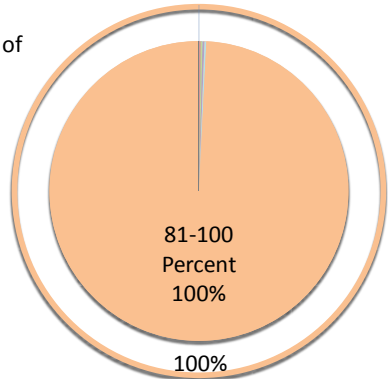
Maturity Level (1-3): 2

DOJ: Yes - The FBI's OPEU program manages the FBI's engagement with fusion centers in terms or providing personnel, subject matter expertise, FBI Net connectivity, funding for miscellaneous equipment, and a Fusion Center Directors Orientation Program that brings decision makers to FBIHQ to discuss best practices for intelligence and information sharing.

DOS: Yes - Diplomatic Security participates in the Northern Virginia Regional Intelligence Coordination Center. DS Agents assigned to JTTF squads may sit in a Fusion Center in situations where their FBI Squad is so detailed. IE - JTTF LA.

DOC: Yes - Commerce routinely reviews products produced by the Fusion Centers and when relevant information is noted, we incorporate it into internal intelligence overview documents.

Question:
What percentage of State and Major Urban Fusion centers has your agency provided training to in P/CR/CL Issues?



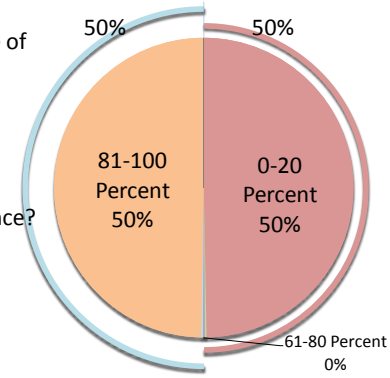
# of Responses: 2

Maturity Level (1-3): 2

DHS: 81-100% - To date, DHS has conducted a one and a quarter day, train-the-trainer course for fusion center privacy/civil liberties officers (delivered with support from the PM-ISE) for trained the privacy/civil liberties officers from 68 of the 77 currently recognized fusion centers.

DOJ: 81-100% - 95% of fusion centers (74 of 78) have received training that included P/CR/CL.

Question:
What percentage of State and Major Urban Fusion centers has your agency provided training to in Counterintelligence?

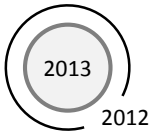


# of Responses: 2

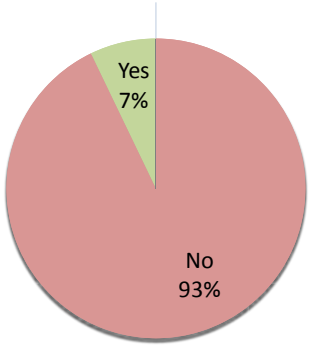
Maturity Level (1-3): 2

DOJ: 0-20% - The NSI PMO does not provide specific counterintelligence training. The NSI PMO provides SAR and SAR awareness training to help identify terrorism related behaviors. These trainings have been developed for law enforcement, fire/EMS, probation/parole/corrections officers, 9-1-1 call operators, emergency management personnel, and private sector security. NOTE: While DOJ does not provide specific CI training, the FBI is committed to placing more analysts at Fusion Centers with CI expertise, in accordance with the RAC policy, to improve counterintelligence capabilities at Fusion Centers.

DHS: 81-100% - DHS conducted 7 Counterintelligence Fundamentals Workshops to State and Major Urban Area Fusion Centers in FY 12 covering a total of 165 State, Local, Tribal and Federal LE personnel.



Question:
Has your agency delivered a plan to align resource decisions to the Resource Allocation Criteria (RAC) policy to DHS?



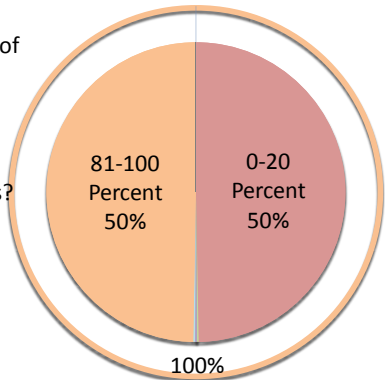
# of Responses: 14

Maturity Level (1-3): 2

DOJ: Yes - In 2011, the FBI approved a strategy for engagement with fusion centers. One aspect of the strategy related to staffing fusion centers with FBI personnel. The strategy, which was shared with DHS, affirmed the FBI's commitment to provide support and resources to fusion centers consistent with the RAC. In 2012, the FBI, informed by the RAC, developed a personnel resource allocation plan to place more Intelligence Analysts into fusion centers.

DoD: No - The Department of Defense does not provide federally funded personnel or financial support dedicated specifically to State and Major urban Area Fusion Centers. However, the National Guard maintains relationships with its state and federal partners which, in some cases, have personnel working in fusion centers. An example is the National Guard Counter Drug Program (NC CDP), which maintains a physical presence in several DHS recognized centers supporting state counter drug programs as authorized under 32 U.S.C. section 112.

Question:
What percentage of State and Major Urban Fusion centers has your agency provided training to in SARs?

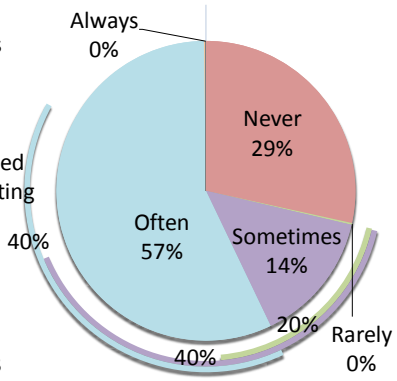


# of Responses: 2

Maturity Level (1-3): 2

DOJ: 81-100% - BJA has trained a total of 291,502 Line officers reaching all 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and Guam. In addition, BJA trained a total of 2196 law enforcement analysts within fusion centers and the federal government. The NSI has partnered with six national and international associations to deploy the Hometown Security Partners Training for Parole/Probation/911 Call Takers/Critical Infrastructure/Fire Service/Emergency Management. The trainings have been endorsed by all six associations. To date, approximately 65,000 people have taken these new trainings. The NSI is working with FDNY to institutionalize the SAR training within their training academy. NSI partnered with the International Association of Campus Law Enforcement Administrators, which has endorsed the line officer training. •The NSI worked with the IACP and other state, local, and federal partners to develop the Unified Message document, stating the importance of SAR reporting and training. This document has been endorsed by 10 agencies/associations and widely distributed across the country including to governors, homeland security advisors, fusion center directors, chiefs of police, sheriffs, and criminal investigative executives. •The NSI is working with the National Maritime Intelligence Office to develop a maritime SAR training, and conducting training at ports regarding port security and SAR awareness.•The NSI conducted more than 70 speaking engagements in 2012, reaching Homeland Security Advisors, Chiefs of Police, State Colonels, Sheriffs, Critical Infrastructure/Key resource partners, Tribal law enforcement executives, Private Sector Security Executives, Probation/Parole/Corrections Executives, Fire/EMS Chiefs and personnel, Fusion Center Directors, and Federal partners.

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



# of Responses: 7

Maturity Level (1-3): 3

DHS: Sometimes - Through agreements facilitated by Preventing and Combating Serious Crime (PCSC) and the Five Country Conference (FCC) DHS ingests international data that matches to existing watchlist records. These matches are also subject to manual review by NPPD/US-VISIT analysts.

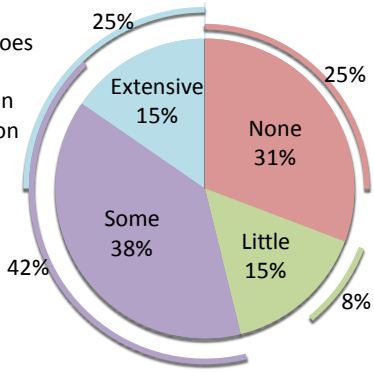
DoD: Often - International partner information provided via formally established information sharing agreements is regularly used to develop DoD watchlist nominations when said information is consistent with national watchlisting policy and guidance requirements. However, special analytic consideration is applied in cases where there is potential for erroneous international partner information targeting foreign political dissidents/activists. In other cases, such as when the U.S. Army generates an eGuardian report that contains information that should go into a watchlist/screening process the servicing Joint Terrorism Task Force (JTTF) or Legal Authority (LEGAT) will add that information.

2013
2012

Question:
To what extent does your agency incorporate fusion center information into its own products and services? Please explain.

# of Responses: 13

Maturity Level (1-3): 3



DHS: Extensive - DHS' Office of Intelligence and Analysis (I&A) is continually working to enhance intelligence support to and analytic collaboration with these partners. These efforts have included the facilitation and development of joint analytic products produced with fusion centers, leveraging State, Local, Tribal, and Territorial (SLTT) subject matter expertise through a variety of fellowships and analytical exchanges, soliciting SLTT input to capture and validate intelligence and information needs, and leveraging SLTT feedback to tailor I&A products and services to better serve our field partners. DHS also heavily leverages the fusion centers to incorporate SLTT information and perspectives into national-level intelligence community assessments pertaining to, for example, southwest border violence, threats, and Mexican cartel influence over U.S.-based gangs. Additionally, over a dozen DHS intelligence reports were cited as sources in the upcoming version of the National Intelligence Estimate titled "Terrorist Threats to the U.S. Homeland to 2016." To provide a state and local perspective on the terrorist threat nationwide for this assessment, DHS also received responses from numerous fusions centers from across the country which ranked the threat actors they view as the most concerning in their jurisdictions. To further expand on these efforts DHS I&A recently stood up the Field Analytic Support Taskforce (FAST). FAST advocates for fusion center intelligence requirements and collaborates with analysts from across I&A's Analysis Directorate and federal interagency partners to identify, develop, and share intelligence products with SLTT partners. Key to this effort is the management and sponsorship joint analysis and production efforts with fusion centers. DHS has recognized that the best way to integrate fusion center information into I&A products is to produce products jointly with SLTT analysts. To that end, dozens of products across I&A's Analysis and Production Directorate that have been produced on everything from border security issues and major special events to suspicious activity reporting (SAR). SAR has been a key SLTT data set that DHS I&A analysts have leveraged for producing products that highlight emerging tactics may provide clarity to trends or patterns in pre-operational terrorist activity.

DOT: Little - In 2011 DOT's Federal Highway Administration (FHWA) worked closely with Fusion Centers as it developed and distributed a publication entitled, "Information-sharing Guidebook for Transportation Management Centers, Emergency Operations Centers, and Fusion Centers." The guidebook provides an overview of the common mission and functions of transportation management centers, emergency operations centers, and fusion centers, and focuses on the types of information these centers produce and manage, and how the sharing of such information among the centers can be beneficial during both day-to-day operations and during incidents.

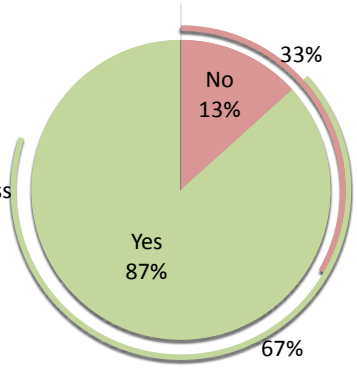
2013
2012

INFORMATION DISCOVERY AND ACCESS THROUGH COMMON STANDARDS

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

# of Responses: 15

Maturity Level (1-3): 1



DHS: Yes - I&A has the lead on the Information Sharing Access Agreements (ISAA) process. This process allows the Department to facilitate information sharing agreements with external partners including the private sector and the intelligence community.

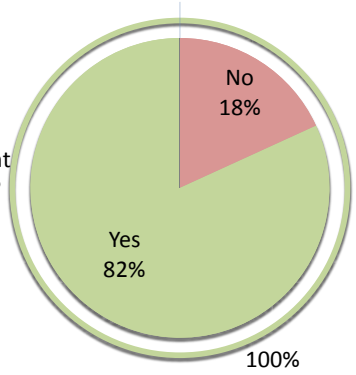
DOJ: Yes - The FBI internal process for developing MOUs/MOAs consists of these steps: Identify appropriate authority; determine need for MOU/MOA; Draft MOU/MOA; and continue to negotiate throughout the process. All finalized MOUs/MOAs are to be registered with the Corporate Policy Office. By corporate policy, all MOUs/MOAs that deal with information sharing are coordinated with or brought to the attention of the Chief Information Sharing Officer.

TREAS: Yes - FinCEN: FinCEN has issued 347 MOUs to allow our partner agencies to access BSA data. The IRS Governmental Liaison Office have defined MOU/MOA development process for proposed business relationships with state, local, and federal agencies.

Question:
Does your agency plan to adopt Federal Identity, Credential, and Access Management (FICAM) standards?

# of Responses: 11

Maturity Level (1-3): 1



DHS: Yes - DHS plans on adopting and implementing FICAM as part of its Information Sharing solution. FICAM standards will be adopted in both the Secret and Unclassified domains.

DOJ: Yes - For Unclassified Systems: The FBI is in the process of evaluating FICAM standards to determine how they would affect current systems and requirements. It is expected that the evaluation will be completed during CY 2013. For Classified Systems: The FBI 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).

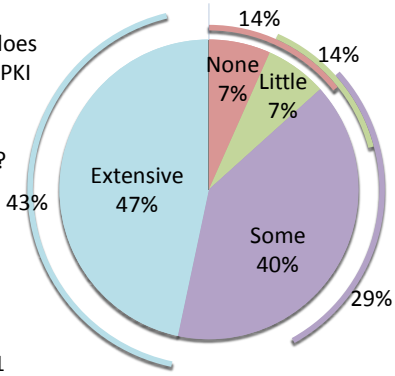
USAF: Yes - The AF has adopted FICAM standards.

DoD: Yes - FICAM standards and segment architecture are being included in our Department level strategic and implementation guidance. FICAM will manifest itself in DoD's implementation of the Joint Information Environment (JIE). JIE looks to establish a secure joint environment across the Department and also include linkage to other DoD agencies, Federal and State partners, and International partners (e.g., Mission Partner Environment (MPE)).

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

# of Responses: 15

Maturity Level (1-3): 1



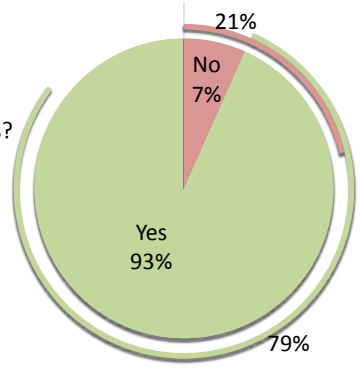
DOC: Some - Commerce participate with the IC for PKI certifications for IC related networks. Commerce is also a Tier I member of the CNSS Secret PKI initiative and anticipates IOC in Q4 FY2013.

HHS: Some - At HHS, the issuance of PIV credentials and their associated PKI digital certificates for application access is complete so individuals at HHS have a credential that could be used for access to ISE related information and mission systems but the implementation of PIV mandatory logins to applications is seeing a slower adoption rate.

NGA: Extensive - PKI is the preferred choice of authentication on all fabrics.

USAF: Extensive - PKI is fully implemented on the unclassified, secret, and top secret general user networks.

Question:
Can members of your agency obtain PKI certificates for ISE-related systems?



# of Responses: 15

Maturity Level (1-3): 1

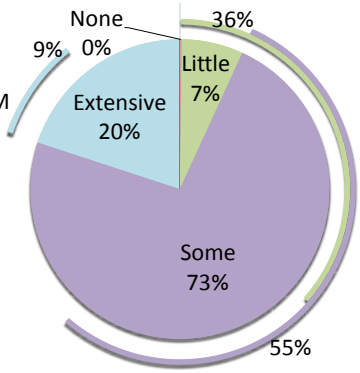
DOJ: Yes - The FBI currently provides PKI certificates to all FBI personnel requiring access to the JWICS community. In addition, PKI certificates are issued to all FBI personnel who have access to the Secret Network for authentication and digital signing of documents. FBI PKI certificates issued were up from 30,000 to 40,000 subscribers for inter-agency email correspondence use for encryption and digital signing via SIPRNet.

NRO: Yes - DoD PKI credentials are issued for unclassified and secret networks. IC PKI and CAD PKI credentials are issued for SCI networks.

DoD: Yes - All DoD employees and some contractors are issued the DoD Common Access Card, which is the DoD PIV. The CAC contains certificates that can be used to access and encrypt ISE related unclassified information and systems. The DoD also issues NSS Secret Fabric tokens to their employees and contractors to access and encrypt classified information and systems. A separate PKI token is issued to DoD employees and contractors for use on JWICS.

DOC: Yes - Commerce participates with the IC for PKI certifications for IC related networks. Secret fabric PKI certificates pending delivery of the CNSS shared PKI solution in June 2013.

Question:
To what extent has your agency implemented FICAM standards? Please explain.



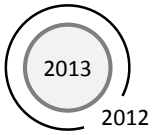
# of Responses: 15

Maturity Level (1-3): 2

DoD: Extensive - DoD has fully implemented identity and credentialing processes and is now improving on dynamic access and accepting federated credentials.

HHS: Some - HHS is aggressively implementing the FICAM standards across the Agency. HHS has a complete and robust PKI infrastructure which is used to issue PIV credentials to all HHS employees and contractors. HHS is moving toward implementing mandatory PIV logins to all Desktop computers and is currently at 48% completion for mandatory desktop logins. The legacy applications across the Agency are also implementing mandatory PIV logins but the adoption rate is slower. HHS has representation on many of the FICAM working groups and is tracking activities in the different FICAM working groups.

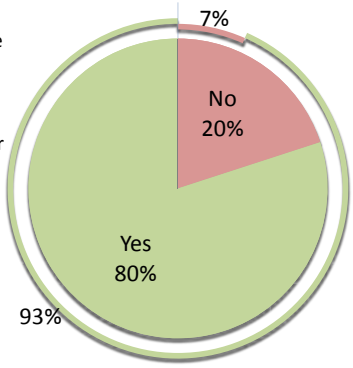
DOJ: Some - Various Components have begun implementing mandatory PIV card login at the desktop. Implementation of digital signing for forms has also begun. DOJ is in the process of rolling out mandatory PIV Card login for desktops and laptops at the hardware level. DOJ is also in the process of deploying identity federation services to allow the sharing of identities among federal law enforcement and across the broader law enforcement community.



Question:
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?

# of Responses: 15

Maturity Level (1-3): 2



DOJ: Yes - During CY 2012, the FBI continued to manage and maintain the Enterprise Directory Service (EDS), an integrated Commercial Off-the-Shelf (COTS) solution, on its Secret enclave known as FBINET. EDS is an automated directory for applications and certain privileged users that retrieves user identity attributes from a centralized service compiled from multiple authoritative sources for access control decisions. This solution has been running successfully for the past two years.

NRO: Yes - has a UAAS federated attribute service providing authoritative authorization attributes via JWICS (SCI) to the IC.

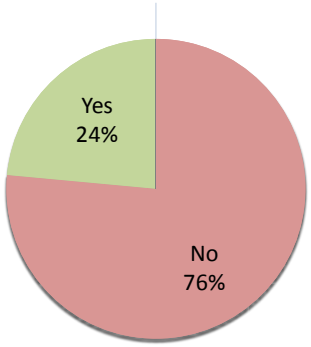
HHS: Yes - has implemented an Agency-wide Access Management System (AMS) to support centralized authentication for many internal and external applications.

USAF: Yes - Public Key Infrastructure (PKI) is implemented on the unclassified, Secret, and Top Secret networks for network access, and access to select network resources (databases, data repositories, etc.).

Question:
Has your agency submitted a data access management Plan of Action and Milestones (POA&M) based on privacy, civil rights and civil liberties attributes, Attribute Based Access Control (ABAC), and Federal Identity, Credential, and Access Management (FICAM)?

# of Responses: 17

Maturity Level (1-3): 2

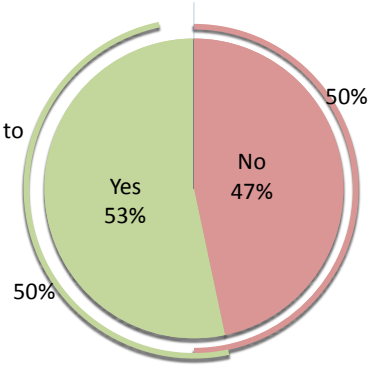


DHS: The ICAM Segment Architecture (Mar 2010) is based on the FICAM and DHS Privacy Impact Assessment (PIA) and System of Records Notice (SORN). The Information Sharing Access Policy Framework (Dec 2011) defines the principles and business architecture for access control. PRIV, CR/CL, and OGC were partners in the development of this document. Work is currently underway to develop a Data Tagging Plan (for Discovery and Access Control) that will be implemented in FY13 on two use cases (pilot programs)—the Common Entity Index (CEI) and Cerberus.

DOJ: No, However, the FBI's Enterprise Data Management Office (EDMO) is developing the FBI strategy and implementation guidance for management of all data stored, used and shared by the FBI and sponsoring the implementation of effective data management practices and stewardship to include a draft data access registry. In addition, the CJIS is working with the ISE to establish a plan and requirements for ABAC. The CJIS will chair the PM/ISE Shared Services group through June 2013 with the goal of addressing Shared Services.

DOS: The Department has developed and implemented a PIV Card Issuer (PCI) Operations Plan as required under the National Institute of Standards and Technology's Special Publication 800-79-1.

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



# of Responses: 15

Maturity Level (1-3): 2

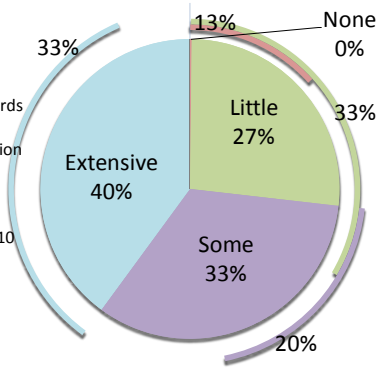
DHS: No - has implemented the Enterprise Architecture Information Repository (EAIR) Technical Reference Model (TRM) for all Technical Standards to include ISE Technical or Functional Standards. The EA IR TRM is currently in early development stages for documenting Technical and Functional Standards. The ISSA identifies the ISE EAF, PAIS, and evolving ISA IPC IISC identified standards as guidance for information sharing related standards.

DOJ: Yes - The FBI Enterprise Standards Profile (ESP) which is based on the Federal Enterprise Architecture Technical Reference Model captures ISE Technical Standards that were adopted by Bureau enterprise and mission systems The ESP is managed by the FBI's Chief Technology Officer.

DoD: Yes - 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.

HHS: Yes - The HHS Enterprise Architecture Repository is the single authoritative repository for technical standards, including those adopted for the ISE.

Question:
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)



# of Responses: 15

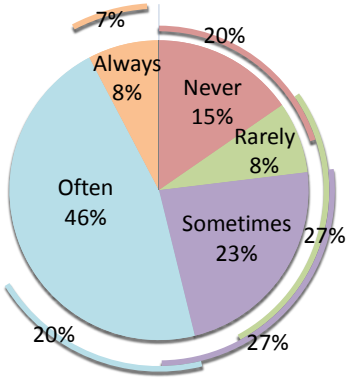
Maturity Level (1-3): 2

DHS: Some - had developed, and is implementing its Information Sharing Segment Architecture (ISSA). The ISSA document provides reference to both the ISE EA Framework and PAIS for direction. Further ISE EAF standards have been incorporated into the DHS Enterprise Architecture Information Repository (EA IR) under the Technical Reference Model (TRM) which is prescribed for use within DHS.

DOJ: Extensive - Specifically, SAR and IdAM. The Department has implemented numerous IEPDs across many platforms including N-DEx, SAR, NGI, and many others. This effort received top priority so as to provide uniform up-to-date platforms for all three enclaves at the FBI to support ISE-related system requirements and standards. As internal processes are upgraded, Common Information Sharing Technical Standards are incorporated into the FBI architectures in phases.

DoD: Extensive - The DoD Senior Architect Engineer is the current Co-Chair of the ISA IPC Information Integration Standards Working Group. The DNI Senior Standards lead Engineer is the other Co-Chair. All Information Sharing standards and interoperability actions in the Joint Enterprise Standards Committee are brought to the IPC Standards Working Group to ensure alignment.

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



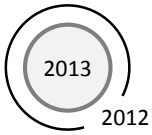
# of Responses: 13

Maturity Level (1-3): 2

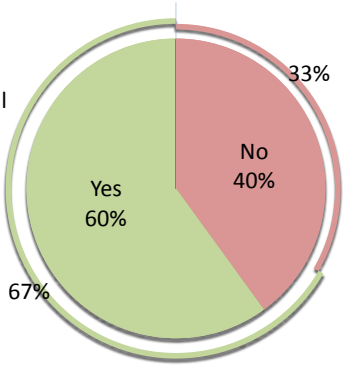
DOS: Often - CA/CST references aspects of ISE standards in the technical section of CA/CST Enterprise Architecture Documentation (i.e. NIEM, and as a guiding principle for data sharing and IT contractual efforts).

DOT: Often - The Department of Transportation (DOT) reviews the ISE mission segments during the development of the annual DOT EA Road Map submission in April. The SAR system is included in the Enterprise Information Management Segment.

DOJ: 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).



Question:
Does your agency have an authoritative council for standards development?



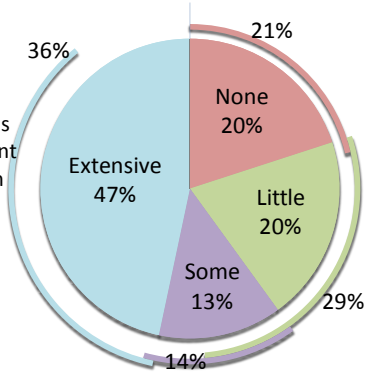
# of Responses: 15

Maturity Level (1-3): 2

NGA: Yes - NGA chairs the Geospatial Intelligence Standards Working Group (GWG) which is a National System for Geospatial-Intelligence (NSG) community forum to govern geospatial standards for the NSG

DOJ: Yes - (1) During CY 2012 the FBI continued to manage the Advisory Policy Board (APB) which serves as the authoritative body for standards development for the FBI's law enforcement (LE) IT systems. (2) The FBI continued to also manage and chair the Electronic Biometric Transmissions Specification (EBTS) Working Group which coordinates ANSI/NIST, NIEM, and APB standards to ensure continued compliance by federal, state, local, and tribal user communities with the EBTS which is the transmission specification for the FBI's Next Generation Identification (NGI) and the Integrated Automated Fingerprint Identification System (IAFIS). Under FBI chairmanship, this working group finalized EBTS Version 9.4, December 2012 and completed the corresponding XML Information Exchange Package Documentation (IEPD) V3.1. (3) The FBI continued to manage a Technology Development and Deployment Board (TDDB) chaired by its Chief Technology Officer (CTO). This Board's Technical Assessment Team serves as an authoritative council for ISE Technical Standard adoption for FBI enterprise and mission systems.

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



# of Responses: 15

Maturity Level (1-3): 2

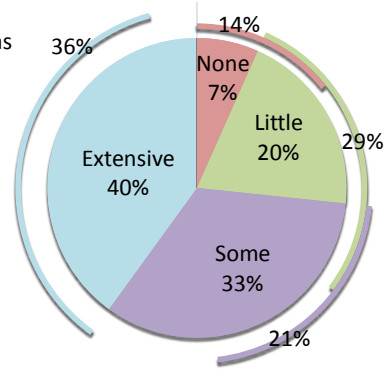
DHS: Extensive - They are a core segment. A next step will be to document the relationship between the ISSA and other segments.

DOE: Some - We follow NIST/CNSSI and IETF standards for networks protocols and guidelines.

DOJ: Extensive - The Department distributes memos that set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business processes.

DOT: None -The Department of Transportation (DOT) has not yet established or included the Information Sharing Environment (ISE) Functional Standards for Information Sharing. However, the plan is to mature our EA governance processes and add ISE Functional Standards to the DOT Data Reference Model (DRM), and ISE Technical Standards to the DOT Infrastructure Reference Model (IRM) and Application Reference Model (ARM) where applicable.

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



# of Responses: 15

Maturity Level (1-3): 2

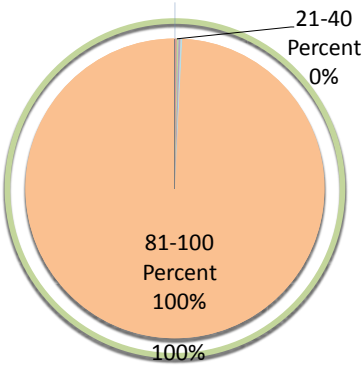
DOJ: Extensive -The Bureau incorporates ISE Technical Standards as part of its IT governance process. There is a Technical Assessment Team under the FBI Technology Development and Development Board that addresses these standards. This technical team assesses candidate and on-going IT projects to ensure alignment with the FBI enterprise architectures. As the FBI IT infrastructure is upgraded in phases for all three enclaves, ISE Technical Standards are incorporated into its IT capability. ISE Technical Standards are referenced in the Enterprise Standards Profile (ESP) maintained by the FBI.

DoD: Extensive - 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. DoD Technical Standards document methodologies and practices to design and implement data sharing and interoperability and interconnectivity. All DoD architectures have to conform to the DoD Architecture Framework which is in alignment with the ISE Architecture Framework. In addition, the new Version DoD IEA published August 2012 had the same design principles as in the ISE EAF which articulates ISE Technical Standards into EA and IT capabilities. New efforts in Information Sharing with other Departments and Agencies are reviewed by the Standards Technical Working Groups as a matter of policy and considered for inclusion in the DoD IT Standards Registry.

Question:
What percentage of TECS-modernization milestones have been successfully hit?

# of Responses: 1

Maturity Level (1-3): 2

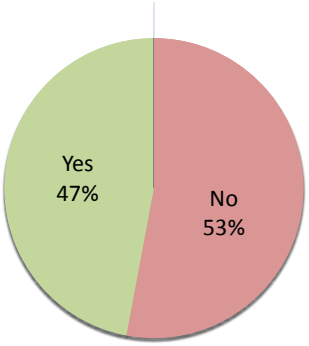


DHS: 81-100 Percent - For the TECS Modernization effort, its activities are divided between two components: CBP is responsible for the development, testing, integration, and deployment of the technology piece, and ICE is spearheading the development and transition of the case management files. To date, both efforts have remained on schedule and are hitting their established milestones (100%).

Question:
Has your agency aligned their SBU architecture authentication consistent with Federal Identity, Credential, and Access Management (FICAM)?

# of Responses: 17

Maturity Level (1-3): 2



DoD: Yes - The DoD is in alignment with the architecture authentication consistent with Federal Identity, Credential, and Access Management (FICAM). DoD CIO has assigned a SES to ensure conformance and to partner in the lead and implementation.

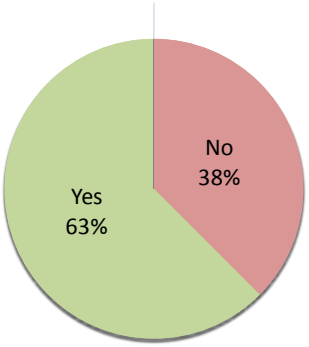
DOC: No - Overall FICAM plan, to include architecture, is under development.

DHS: Yes - HSIN R3 is built using guidance from the DHS ICAM Segment Architecture and the Fed CIO FICAM guidance.

Question:
Has your agency incorporated access policies that protect privacy, civil rights and civil liberties using a common government-wide template for each data source into their SBU architecture?

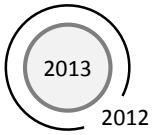
# of Responses: 16

Maturity Level (1-3): 2



DHS: Yes - The Information Sharing Access Policy Framework (ISAPF) defines the access policies for DHS architecture. DHS is in the process of building out externalized access control in two use cases, one on the SBU network, and one in the classified space. Both use cases will apply a unified process for access control and will leverage (and extend where necessary) the Intelligence Community Information Technology Environment (IC-ITE) guidelines for data tagging.

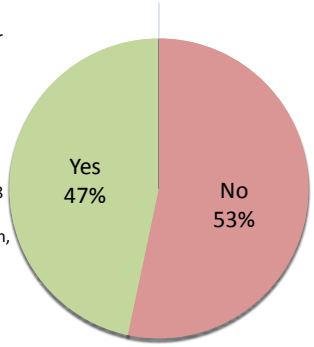
DOJ: Yes - The department and components follow policies to protect privacy, civil rights and civil liberties. A common government-wide template for data sources is in the development stage. When such a template is finalized, the FBI will incorporate it into its access policies for its SBU architecture. In addition, biometric standards, access control standards, authentication standards are all common across the CJIS enterprise for its systems.



Question:
Has your agency aligned their SBU architecture with the publication of geospatial Critical Information Requirements (CIRs) and authoritative source(s) necessary to meet Presidential Policy Directive 8 Mission Areas in open standards available for search, discovery, and access?

# of Responses: 15

Maturity Level (1-3): 2



DHS: Yes - DHS is continuing to align as part of overall maturity

DOC: Yes - NOAA actively participates in the geospatial standards committees.

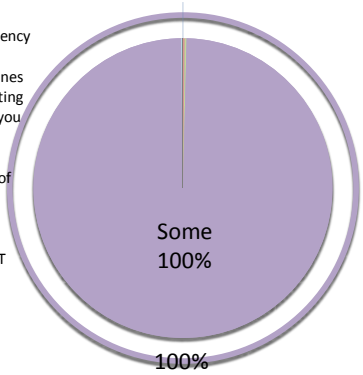
DOI: No - The plan is to use geospatial data within IMARS.

DOJ: Yes - As far as limited responsibility DOJ has for HSPD 8. DOJ submitted a list of Mission Essential Systems to DHS. In addition, DOJ provided HSIP geospatial shape files for the field offices, resident agencies and district court jurisdictions. Also, CJIS has aligned its SBU architecture with NIEM standards for inter-agency information distribution.

Question:
To what extent does your agency have documented policies and/or implementing guidelines on IT security reciprocity stating the conditions under which you will accept the security certification and/or accreditation/authorization of another organization? This refers to agency-specific implementing guidelines for policies such as ICD 503, NIST 800-53 and CNSSI 1253.

# of Responses: 1

Maturity Level (1-3): 3

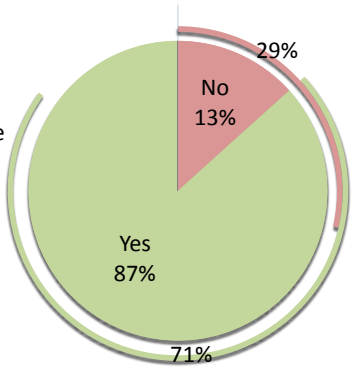


TREAS: The IRM in this case accepts the security certification and/or accreditation/authorization of another organization as part of Interconnection Security Agreements. DO/HQ: Treasury Directive Publication Intelligence Information Systems Security Policy Manual TD P 15-03 fully documents the Office of Intelligence and Analysis' (OIA) position on Reciprocity in Section 2.4 beginning on page 8. TD P 15-03 complies with the Reciprocity requirements from ICD 503, NIST -53, and CNSSI 1253.

Question:
Has your agency implemented an accessible authoritative source at any classification level?

# of Responses: 15

Maturity Level (1-3): 3



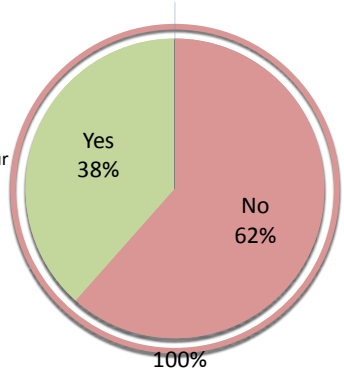
HHS: For applications with a FIPS 199 rating of "High" or "Moderate", HHS requires two factor logins. Of these "High" and "Moderate" applications, currently 15% of all user accounts to applications require the use of PIV credential for two-factor logins. HHS is currently focusing on implementing PIV mandatory logins and for HHS Enterprise application, of which 23 out of 39 "High" and "Moderate" applications are integrated with mandatory PIV logins.

USAF: Yes, the complete infrastructure necessary to support PKI enablement and implementation is in place on the unclassified, Secret, and Top Secret levels. Additionally the AF is a member of DIA's Full Service Directory (FSD) on the TS/SCI network JWICS. FSD is the authoritative source for access controls and PKI certificates.

Question:
Does your agency accept (and make accreditation decisions without retesting) IT security certification bodies of evidence? , i.e., does your agency practice IT security reciprocity, for State, Local, or Tribal (SLT) governments?

# of Responses: 13

Maturity Level (1-3): 3



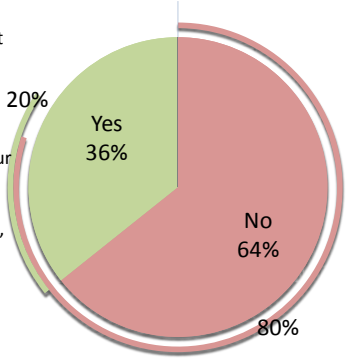
DHS: Yes - HSIN will accept FISMA-certified security accreditations after a review by the program. The DHS CISO is prepared to accept other agencies IT security certification body of evidence on a case by case basis, but to date have not encountered any systems from state, local or tribal governments.

DOJ: Yes - Trust relationships have been established with state, local, and tribal governments without reciprocity and with triennial audits. Certification and accreditation (aka security assessments) requirements are federal mandates only for federal information systems. We are not aware of state, local or tribal requirements to perform certification and accreditation on a scale comparable to what the federal government does. This agency would be hard pressed to accept reciprocity from these agencies regardless of bodies of evidence presented and would require some level of testing, etc. on our part.

Question:
Does your agency accept (and make accreditation decisions without retesting) IT security certification bodies of evidence? , i.e., does your agency practice IT security reciprocity, for other organizations (e.g., private sector, foreign governments)?

# of Responses: 14

Maturity Level (1-3): 3



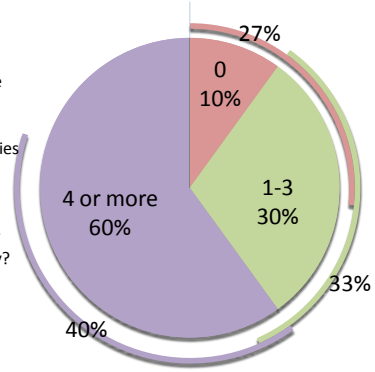
DOT: Yes - The Department practices reciprocity. However if and when DOT accepts accreditation decisions from another organization, the retesting of controls in this environment must be considered.

DoD: Yes - The Department complies with the policy and procedures implemented through the DoD Information Assurance Certification and Accreditation Process (DIACAP) for all entities requesting accreditation. Regarding the private sector, the Department has enabled DIBNet-Unclassified to accept all DoD-approved PKI certificates to include those cross-certified under the Federal Bridge (i.e., private sector certificates that have been through the DoD testing process for approval).

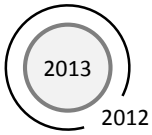
Question:
From how many organizations does your agency accept (and make accreditation decisions without retesting) IT security certification bodies of evidence? , i.e., does your agency practice IT security reciprocity, for other federal agencies or departments - how many?

# of Responses: 10

Maturity Level (1-3): 3



DOI: 4 or more - DOI practices reciprocity and accepts the IT security assessment evidence for information systems that have achieved provisional authority to operate (Provisional ATO) by the Joint Authorization Board (JAB) through the Federal Risk Authorization and Management Program (FedRAMP). Additionally, DOI accepts the assessment body of evidence from other agencies provided it was obtained through one of the FedRAMP approved Third Party Assessment Organizations (3PAOs). DOI may accept assessment results from agencies that have completed Assessment and Authorizations (A&As) for other information systems that relied upon assessors other than those recognized by FedRAMP only after a review of the processes, methods, tools, techniques, and results to help determine whether or not the degree of rigor applied was in alignment with standards issued by the National Institute of Standards and Technology (NIST). Any retesting that may be required would only focus on those areas of perceived inadequacy.

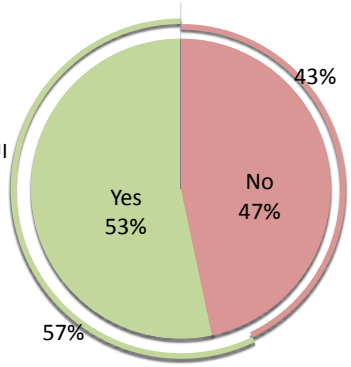


OPTIMIZING MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY

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

# of Responses: 15

Maturity Level (1-3): 1



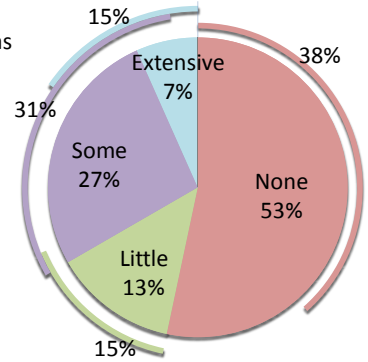
DOJ: Yes, LEO,RISSNet and Federated Identity Broker are now available to SLTs. Also, during CY 2012, the FBI's Criminal Justice Information Service (CJIS) continued to implement interconnected access to its SBU networks for sharing of law enforcement information relevant to terrorism and homeland security with members of the Law Enforcement Community.

DOS: The Department currently provides shared data on its third party shared space provider ODNI's Intelink-U which is part of the ISE SBU/CUI Interoperability initiative. In addition, at the DS Bureau level there is a plan for implementing secure and automated data exchange interfaces on a case-by-case basis with other agencies. This plan cannot commence until the sources systems are redesigned and include the capability for both export of data to NIEM compliant structures and CUI designations. This plan address only point-to-point, system-to-system, level data exchanges and not full integration of networks.

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

# of Responses: 15

Maturity Level (1-3): 1



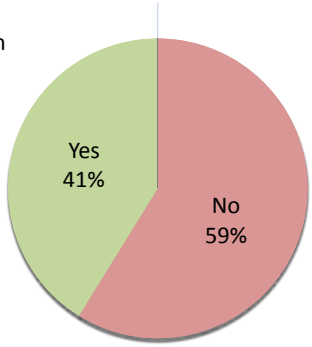
DHS: Some - Technical design is underway with RISS.net to support interoperability this FY.

DOJ: Extensive - The FBI currently shares all ISE SARs from eGuardian to the NSI Shared Spaces. The Counterterrorism Division's (CTD) Guardian Management Unit is working closely with the NSI to facilitate an automatic technological solution to share all Information Sharing Environment (ISE) SARs from the NSI Shared Spaces into eGuardian. During CY 2012, the FBI's Criminal Justice Information Service (CJIS) built and installed the Trusted Broker which allows external users supporting ISE-related missions to federate into CJIS without using a name/password. Agencies on-boarded included Metro Chicago Police Department (PD), INTELINK (Office of the Director for National Intelligence) and Regional Information Sharing System (RISS) (Department of Justice), with access provided to Joint Automated Booking System (JABS), National Data Exchange (N-DEx), Law Enforcement Online (LEO), and National Criminal Information Center (NCIC). The Department of Homeland Security (DHS) has plans to begin using the Trusted Broker in 2013.

DOS: None - Several years ago, DS provided NCTC users with remote access FOB's and the ability to access DoS system via that method. DS personnel currently also access other agency systems and manually enter copies of DS information deemed potentially relevant into those systems; such as the FBI's eGuardian system. Further integrations cannot be initiated until DS source systems have been appropriately modified (underway now), additional physical network interconnection capabilities have been implemented and the CUI standard finalized and incorporated into DoS policy.

Question:
Does your agency plan to fund the integration of CUI requirements into information systems as they are developed and/or upgraded on or before Sep. 30, 2014?
# of Responses: 17

Maturity Level (1-3): 1



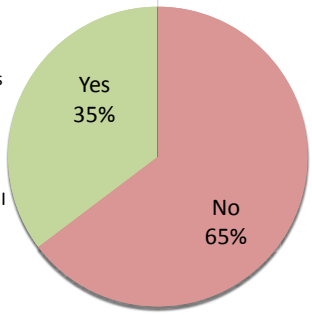
DHS: No - Current HSIN Release 3 development does not include CUI requirements because they were not available or approved when HSIN R3 development began. Plans for CUI requirements will be included in the next major upgrade.

DoD: No - Costs associated with implementing the CUI Program have not been programmed or budgeted for within the Department of Defense. As stated in the DoD CUI Compliance Plan submitted in February 2012 to the National Archives and Records Administration (NARA) as the CUI Executive Agent, the IT systems cost impacts to implement CUI are assessed to be significant. Finally, the DoD looks forward to receipt of OMB guidance addressing programming requirements [for partial, full, and/or phased CUI implementation] and receipt of the national CUI policy through the Federal Register process in order for DoD to properly resource for this program.

DOI: Yes - DOI will wait for the pending Federal CUI Program's implementation timeline and requirements. Following the Federal CUI Program timeline release, the Department of the Interior will execute its existing "Department Of the Interior CUI Implementation Plan, December 2011."

Question:
Does your agency plan to fund the development of CUI self-inspection programs including reviews and assessments to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation on or before Sep. 30, 2014?
# of Responses: 17

Maturity Level (1-3): 1

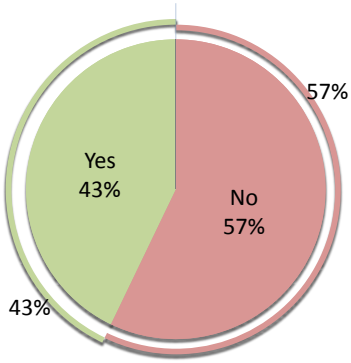


DOJ: No - The FBI intends to develop appropriate CUI self-inspection programs to evaluate program effectiveness and measure compliance. However, no budget requests have yet been made for this funding. Until the specific government-wide CUI standards are set and adopted (by the CUI Office at NARA) in the upcoming Federal CUI implementing directive, cost estimates cannot accurately be assessed and completed. Therefore, it is unlikely that the funding for a CUI self-inspection program will be achieved on or before September 30, 2014.

Question:
Are ISE Functional Standards considered when issuing mission system RFPs and/or Grants (for ISE-related systems)?

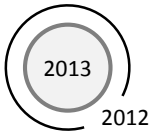
# of Responses: 14

Maturity Level (1-3): 1

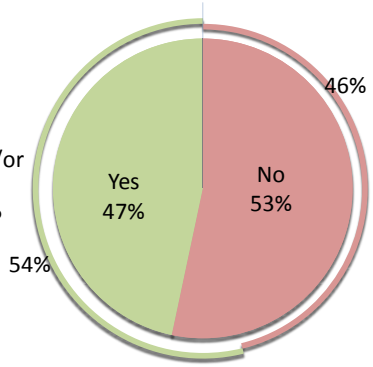


DOJ: Yes - ISE Functional Standards are noted on OMB 300s and Exhibit 53s for Bureau ISE-related systems.

DoD: Yes - ISE Functional Standards are considered as that are incorporated into the DoD Standards Program and the DoD IT Standards Registry (DISR) where and when applicable to support cross domain information sharing. This is accomplished by the Chief Architect and Chief Engineer as part of their Program/Project development and functional/operational review/consideration of the mission/business objectives.



Question:
Are ISE Technical Standards considered when issuing mission system RFPs and/or Grants (for ISE-related systems)?



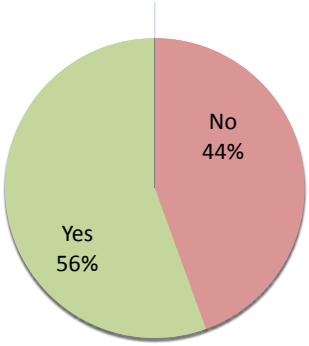
# of Responses: 15

Maturity Level (1-3): 1

DHS: Yes - Technical standards are typically included in the statement of work, which are a part of RFQ. ISE functional standards are also considered as appropriate.(ADM)

DOS: Yes - The Bureau of Consular Affairs, Office of Consular Systems and Technology incorporates ISE/NIEM standard language in all IT relevant RFPs.

Question:
Has your agency provided information sharing and safeguarding standards activities (current or planned, public or private) to PM-ISE and OMB?



# of Responses: 18

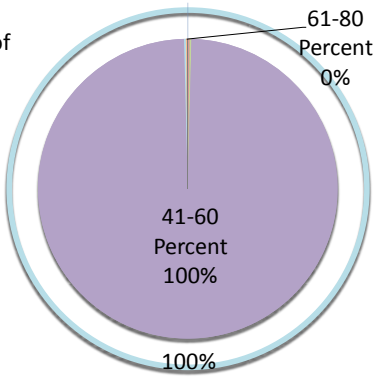
Maturity Level (1-3): 1

DHS: Yes - supported standards-based acquisition efforts by providing a copy of ISSA to PM-ISE. The ISSA works to generates standards and capabilities across DHS.

DOS: Yes - We've responded to all OMB-requested actions, and any data calls emitted by PM-ISE.

DOT: Yes - The Department of Transportation (DOT) has responded to each of the Classified Information Sharing and Safeguarding Office's requests for inputs to the Key Information Sharing and Safeguarding Indicators (KISSI) throughout 2012.

Question:
What percentage of critical milestones has the HSIN integration successfully met?

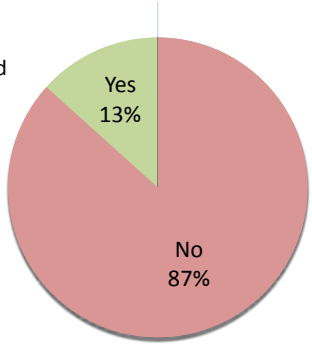


# of Responses: 1

Maturity Level (1-3): 2

DHS: 41-60 Percent - 50%. The capability for entering and searching DHS Suspicious Activity Reports through a SharePoint workflow is dependent upon HSIN 3.2 deployment, scheduled to be completed by Q2 FY13. The SAR workflow design is underway & scheduled to be completed Spring, 2013 with concurrent Critical Infrastructure development also completed. Subsequent System Integration and User Acceptance Testing will be performed within HSIN, and then followed by federated testing with the NOC/COP. Concurrent with this effort; attributes are being defined to ensure SARS are securely accessed by authorized individuals with collaborative work with FICAM Working Groups.

Question:
Has your agency identified and published SBU geospatial data (cataloged and registered) in the Semantic Ontology and Registry on the DHS Geospatial Information Infrastructure?



# of Responses: 15

Maturity Level (1-3): 2

DOJ: Yes - DOJ provided HSIP geospatial shape files for the field offices, resident agencies, and district court jurisdictions. The data includes area of responsibility, name of field office, resident agency, or district court, and the address.

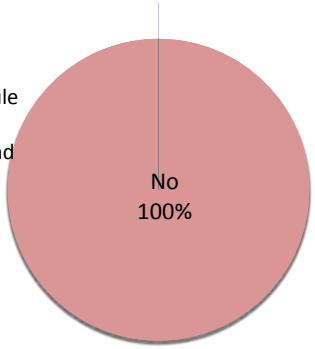
DOT: No - The Department of Transportation has not yet published SBU geospatial data in the Semantic Ontology and Registry on the DHS Geospatial Information Infrastructure.

DHS: Yes - DHS is continuing to align and register its geospatial data holdings to the GII as part of overall maturity.

Question:
Has your agency submitted their implementation schedule for agency-specific production, delivery, and maintenance for each SBU geospatial dataset for registration to the ISA-IPC?

# of Responses: 15

Maturity Level (1-3): 2

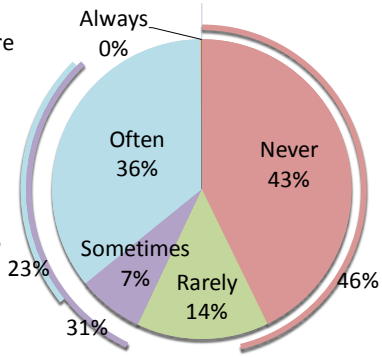


DOT: No - The Department of Transportation has not submitted an implementation schedule for agency-specific production, delivery, and maintenance for each SBU geospatial dataset for registration to the ISA-IPC.

Question:
To what extent are ISE Functional Standards used when issuing mission system RFPs and/or Grants (for ISE-related systems)?

# of Responses: 14

Maturity Level (1-3): 2



DOJ: Often - This practice is dependent on the FBI's IT Program and Project Managers uniformly listing standards on OMB 300s and Exhibit 53s. For example, ISE Functional Standards are extensively and commonly used in RFPs for the Bureau's Law Enforcement systems. In March 2012, the FBI conducted a data call at the request of OMB to identify standards for its system requirements reflected in Exhibit 53s. The results of the data call will be provided to the Finance Division's IT Contracting Unit who issues IT RFPs as well as the FBI CIO's Contract and Acquisition Management Unit (CAMU). CAMU is composed of highly skilled and trained acquisition professionals well versed in IT procurement. CAMU offers acquisition support, requisition processing, and Contracting Officer's Representative (COR) services for enterprise IT Programs and Projects. CAMU has documented and proofed IT acquisition processes where ISE Functional Standards could be incorporated as more than a checkpoint.

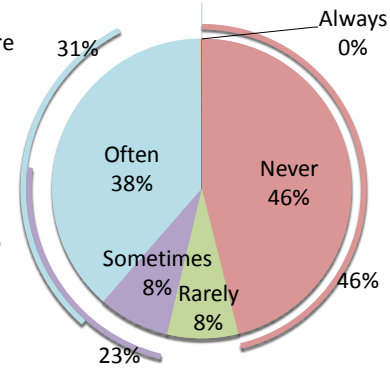
DOS: Often - The Bureau of Consular Affairs, Office of Consular Systems and Technology incorporates ISE/NIEM standard language in all IT relevant RFPs.

DOT: Rarely - Only when a system has been identified as ISE-related, as is the case with the DOT Suspicious Activity Reporting (SAR) system, BlueMercury. Once DOT establishes its Architecture Working Group (see question 30), we will be able to promulgate clearer guidance on the consideration of ISE Functional Standards.

Question:
To what extent are ISE Technical Standards used when issuing mission system RFPs and/or Grants (for ISE-related systems)?

# of Responses: 13

Maturity Level (1-3): 2



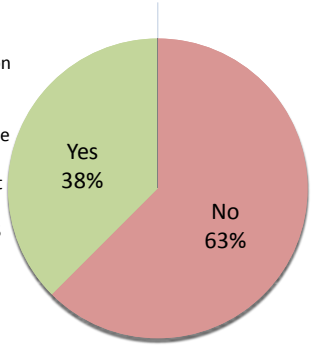
DHS: Sometimes - Technical standards are typically included in the statement of work, which are a part of RFQ. DHS incorporates ISE Technical Standards in conduct of mission system lifecycle activities—to include RFPs and/or grants.

DoD: Often - 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. This is accomplished by the Chief Architect and Chief Engineer as part of their Program/Project development and functional/operational review/consideration of the mission/business objectives.

Question:
Has your agency provided updated grant or acquisition policies, standards-based requirements, and grants references where applicable to account for federal best practices, policy and toolkit recommendations, and alignment with the ISE CISS to PM-ISE?

# of Responses: 16

Maturity Level (1-3): 2



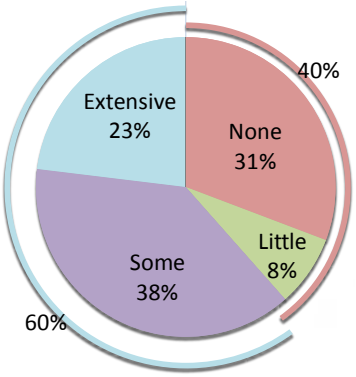
DHS: Yes - In FY2012, the NIEM PMO provided a supplemental resource for NIEM as part of the Homeland Security Program.

HHS: No - HHS' Office of Grants and Acquisition Policy and Accountability has not updated its grants or acquisition policies for ISE related-matters, and therefore has not provided updates to PM-ISE. HHS' policies reflect the implementation of federal-wide policy guidance (such as the OMB circulars governing grants administration) or regulations (such as the Federal Acquisition Regulation) and where appropriate, implement HHS' unique requirements that are based in statute (such as Appropriation Acts). Until such time that ISE-related standards are required by such federal-wide regulation or guidance or by statute, HHS does not foresee updating its grants or acquisition policies to address ISE-related standards.

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

# of Responses: 13

Maturity Level (1-3): 3



DOJ: Extensive - To date, over 26,000 SAR entries have been submitted by stakeholders to the NSI, including the FBI, and tens of thousands of queries of that data have been made by analysts. The entries have been successfully leveraged from an investigative perspective by the FBI, and analysts are utilizing this information to advance their situational awareness and produce intelligence products related to suspicious activity reporting.

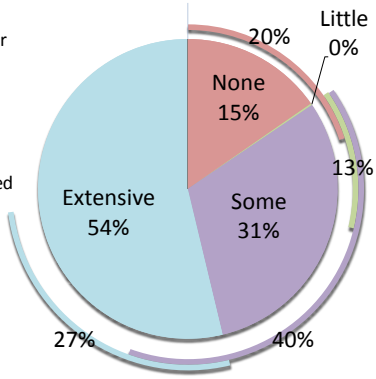
DoD: Extensive - The NGB indicates that NGB now shares threat related information with over 8000 law enforcement agencies.

DOI: Extensive - Our ability to become more aware has improved through the use of eGuardian. Shared spaces containing SAR information makes it easier to connect situations or events that need closer inspection or investigation.

Question:
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? Please provide examples.

# of Responses: 13

Maturity Level (1-3): 3



DHS: Extensive - In the TS/SCI domain, the ability to discover, access, and retrieve information has improved. DHS has been able to retrieve, access, and discover information through community shared resources, such as LNI. DHS has also deployed H-Space, which has helped the department in facilitating information sharing of terrorism-related information. H-Space is available in the Secret domain.

DOJ: Extensive - The department and components utilize N-DEx, NSI, LEO,RISSNet, HSIN, Intelink-U, NLETS, NGI, NCIC, and NICS. A specific example of this is the deployment of Advanced Fingerprint Technology (AFIT) for NGI. This allowed for 129.3 million transactions since implementation on 2/25/11. IAFIS has also been upgraded to handle 98,000 Ten Print Rap Sheet transactions per day.

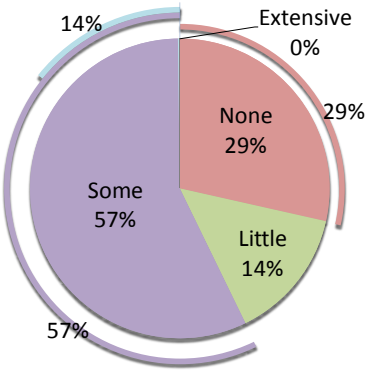
2013

2012

Question:
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? Please explain.

# of Responses: 14

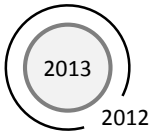
Maturity Level (1-3): 3



DHS: Some - The implementation of the NSI has improved the flow of SARs between USCG and DHS I&A. Another example, NPPD/US-VISIT participated in a PM-ISE pilot for information sharing between the SBU environment and the intelligence community. Specifically, this involved the exchange of information between NPPD/US-VISIT, ADIS, and two intelligence community partners (Data Aggregation Pilot). Last example, USSS has implemented 22 fixed HSDN systems and 13 tactical HSDN systems over the last two years, expanding our ability to conduct information sharing at the Secret Level at fixed field offices, protective divisions and during NSSE's. Additionally, a Cross Domain/Multi Level Security system has been implemented increasing our ability to collaborate from a single work stations across classification levels.

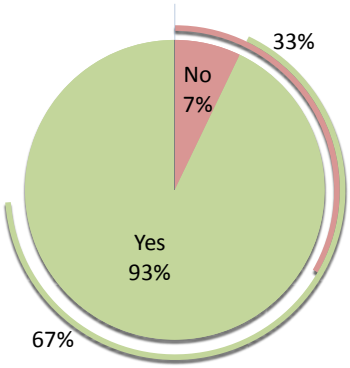
DOJ: Some - To date, over 13,900 unclassified incidents have been pushed from Guardian to eGuardian and the NSI Shared Spaces. In addition, during late 2012/early 2013, technical advancements took place in that has led to the implementation of an auto-push feature that is now employed in 50 fusion centers. This auto-push allows SAR data entered in the Shared Space to be seamlessly transmitted to eGuardian.

DoD: Some - As of the end of 1st Qtr FY 13, U.S. Army CID has 100% of CID Battalions with eGuardian access and 52 of 72 reported Provost Marshal Offices have 100% implementation of eGuardian. The NGB reports that all states & territories are now online with nationwide SAR programs.



PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

Question:
Is your agency operating under an approved privacy policy consistent with the ISE Privacy Guidelines?

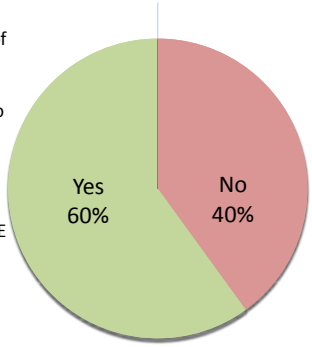


# of Responses: 14

Maturity Level (1-3): 1

DHS: Yes - The DHS Privacy Office and Office for Civil Rights and Civil Liberties issued a joint Privacy and Civil Liberties Policy Guidance Memorandum, Memorandum Number: 2009-01 entitled, "The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy."

Question:
Has your Agency (outside of the Privacy Act) developed and provided an ongoing training program specific to the implementation of the ISE Privacy Guidelines to personnel authorized to share protected information through the ISE and for reporting violation



# of Responses: 15

Maturity Level (1-3): 1

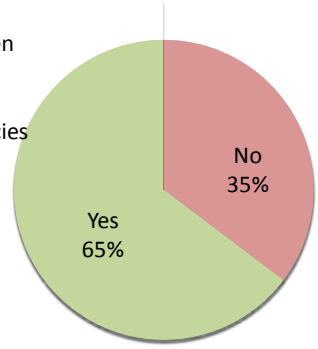
DHS: Yes - I&A intelligence professionals assigned to a State and Major Urban Area Fusion Center also receive training on their responsibilities to protect privacy within the ISE—the Privacy Office also provides a great deal of ISE privacy training at State and Major Urban Area Fusion Centers as well.

DOJ: Yes - All employees are required to take annual training which includes a privacy component. In addition, other training is provided specifically on how to appropriate share information. The Terrorist Screen Center contains information about the ISE Privacy Guidelines in its training.

DoD: Yes - Annual privacy training is required for the DoD workforce and future iterations of this training will identify ISE requirements.

DOC: Yes - Commerce utilizes the ISE training "ISE Core Awareness Training" to provide a common understanding of the ISE to all employees who need to access the ISE.

Question:
Has your Agency taken steps to facilitate appropriate public awareness of its policies and procedures for implementing the ISE Privacy Guidelines?



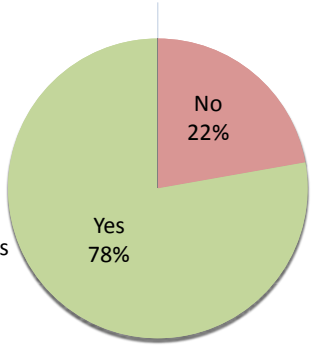
# of Responses: 17

Maturity Level (1-3): 1

DHS: Yes - DHS has taken a number of steps to foster public awareness of our ISE Privacy and Civil Liberties Protection Policy. First, the policy is available to the public at the DHS Privacy Office website at www.dhs.gov/privacy. Second, the Privacy Office's work to implement ISE privacy protections is detailed in each of the Privacy Office's Annual Reports to Congress since the creation of the requirement. Finally, ISE requirements are mentioned in appropriate Privacy Impact Assessments and other material produced by the Privacy Office including training and public presentations.

Question:
Does the agency's ISE Privacy and Civil Liberties Official receive reports of errors in cases involving information which may impact the privacy or civil liberties of individuals?
# of Responses: 18

Maturity Level (1-3): 1

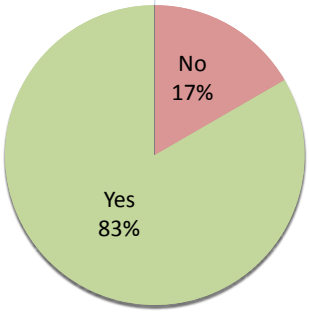


DOS: Yes - The Department does not have an ISE Privacy and Civil Liberties Official. The process to address an error involving information which may impact the privacy or civil liberties of individuals is administered by the Department's Senior Agency Official for Privacy together with the Office of the Legal Adviser and, where appropriate, with the Bureau of Diplomatic Security. In the case of litigation, legal process is served on the Executive Director of the Office of the Legal Adviser.

HHS: No - We do not have this as a routine practice. However, we do have multiple methods available for members of the public to contact HHS and register objections if information is complete and inaccurate. Our Office for Civil Rights, in particular, is charged with receiving such concerns not only for HHS systems, but for any information held by a HIPAA-covered entity (including almost all health care plans and providers in the United States).

Question:
Is your agency's P/CL office (led by a P/CL officer or Senior Agency Official for Privacy) actively involved in planning, development, and oversight of information sharing and safeguarding activities? Please give examples.
# of Responses: 18

Maturity Level (1-3): 2

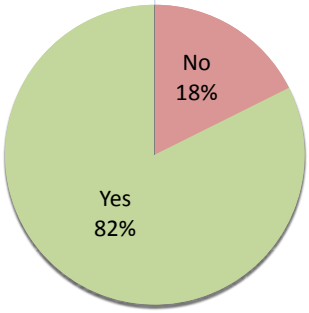


DHS: Yes - The DHS Chief Privacy Office and the Officer for Civil Rights and Civil Liberties serve as the agency's ISE Privacy and Civil Liberties Officials. Each is actively involved in planning, development, and oversight of sharing and safeguarding activities. For the Privacy Officer, this includes conducting and publishing Privacy Impact Assessments (PIAs) on systems that utilize information covered by the ISE Privacy Guidelines. PIAs are undertaken during the planning and development staged and includes an examination of privacy issues and implementation of the Fair Information Practice Principles, which also serve as the basis for our ISE Privacy Protection Policies. Where ISE covered information is shared under an MOU, the Privacy Office is involved in reviewing compliance with ISE Protection and general privacy protection policies. The Privacy Office also participates in oversight activities. This includes, for instance, participating in reviews of compliance with information sharing access agreement terms and conditions, including ISE requirements. This further includes conducting Privacy Compliance Reviews (PCR); the Privacy Office recently completed a review of DHS's participation in the National SAR Initiative, which is part of the Department's ISE information sharing program.

Question:
Does your Agency review protected information for accuracy before it is made available to the ISE?

# of Responses: 17

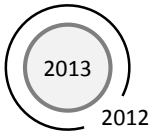
Maturity Level (1-3): 2



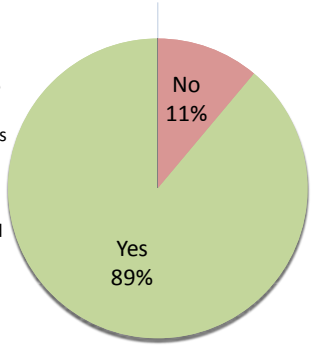
DHS: Yes - Data Quality is one of the DHS Fair Information Practice Principles. Each system that maintains ISE covered information must take steps to ensure data is appropriately timely, relevant and complete.

DOT: Yes - The Department of Transportation's (DOT) Privacy Officer along with the DOT ISE Program Manager conducts reviews of protected information for accuracy before it is made available to the ISE.

DOI: Yes - The DOI Privacy Policy for the ISE outlines requirements to ensure data is accurate in accordance with Federal laws and the Code of Fair Information Practice Principles, and also requires action to correct inaccurate information and notify appropriate officials. First line supervisors review information before it is entered into IMARS, and can also cross check information in the system for accuracy before it is entered.



Question:
Has your Agency adopted and implemented procedures to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE?
# of Responses: 18

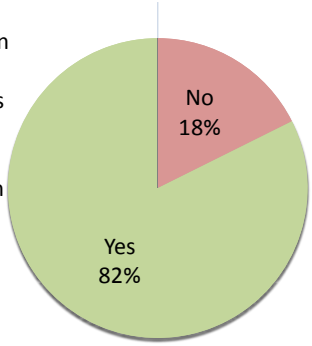


Maturity Level (1-3): 2

DHS: Yes - The DHS Fair Information Practice Principles and ISE Privacy Protection Policy outline the procedures designed to prevent, identify, and correct protected information. These protections are also reflected in appropriate PIAs and include Data Quality, Individual Participation, Access, Redress, and Accountability. ISAAs establishing terms and conditions for sharing under the ISE also include provisions for parties notify each other if information they learn calls into question the accuracy of the data of the other.

DOJ: Yes - Both the department and components have a robust audit capability as well as an Inspection Division and Office of Integrity and Compliance which assist in preventing and correcting any errors.

Question:
Has your Agency put in place internal procedures to address complaints from persons regarding protected information about them that is under the Agency's control?
# of Responses: 17



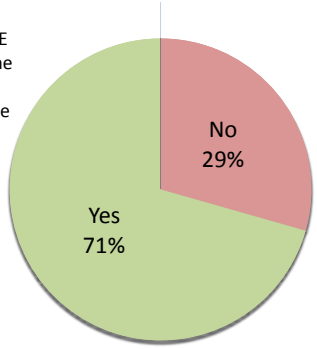
Maturity Level (1-3): 2

DHS: Yes - Part of our ISE Privacy Protection Policy included information on how to file a complaint or requests for corrections. Access and Redress are part of the DHS Fair Information Practice Principles.

HHS: Yes - Individuals can register complaints via a number of channels, including exercising Privacy Act rights; appealing decisions related to the receipt of benefits; or by registering a complaint with the Secretary for HIPAA-related violations. Also, under HIPAA, individuals have the right to request amendments to their health care records, and HIPAA covered entities (including HHS) are required to accept such requests if they are reasonable and appropriate.

NGA: Yes - NGA Privacy and Civil Liberties Office published a policy and accompanying manuals in February 2013 that outlines procedures for addressing complaints from individuals regarding their protected information.

Question:
Does your Agency notify ISE participants who receive the Agency's protected information of all applicable access, use, retention, or disclosure limitations in cases where personally identifiable information of individuals is being shared (i.e. "protected information")?
# of Responses: 17



Maturity Level (1-3): 3

DHS: Yes - Such notice, for instance, appears as terms and conditions in Information Sharing Access Agreements.

DOJ: Yes - The FBI takes steps to protect its information - this is accomplished through some automatic caveats as well as MOUs. The FBI also reviews information being shared and provides provisions to protect its information as appropriate to comply with the Privacy Act and EO 12333.

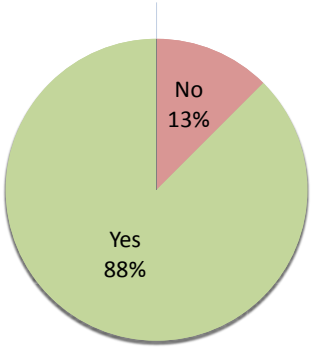
DOC: No - There are no sharing agreements in place

HHS: No - We intend to facilitate this once the ISE policy is final. In general, however, the system HHS uses to share PI and PII (eGuardian) is not structured to specifically prompt the inclusion of information related to access, use, retention, or disclosure limitations. Users will be encouraged to provide this information, if there is any. Note that the only ISE participant with whom HHS shares PI and PII is the FBI, which makes assessments related to such aspects of the data before further sharing the information with participants in the ISE.

2013
2012

Question:
Has your Agency implemented adequate review and audit mechanisms to enable the Agency's ISE PCL Official and other authorized officials to verify that the Agency and its personnel are complying with the ISE Privacy Guidelines? Please provide examples.
# of Responses: 16

Maturity Level (1-3): 3



DHS: Yes - The Privacy and Civil Rights and Civil Liberties Offices at DHS are negotiating, implementing, and reviewing information sharing agreements and other mechanisms for information sharing in order to meet compliance with ISE privacy requirements. DHS regularly meets with National Counter-Terrorism Center (NCTC) to review implementation of all information sharing agreements. For example, the Privacy Office recently conducted a Privacy Compliance Review of DHS's participation in the National SAR Initiative. The Privacy Office also reviews DHS intelligence reporting—either finished intelligence or raw reporting—that is to be shared within the ISE, before that information is disseminated to ISE partners.

DOJ: Yes - The FBI is able to determine whether individuals have taken the required trainings; PCLU reviews privacy impact assessments and privacy threshold analyses to ensure proper compliance. The FBI has also created Division Privacy Officers to assist in the review of day to day issues that may arise. DOJ's policy is reviewed when information sharing initiatives are proposed and associated documentation created.

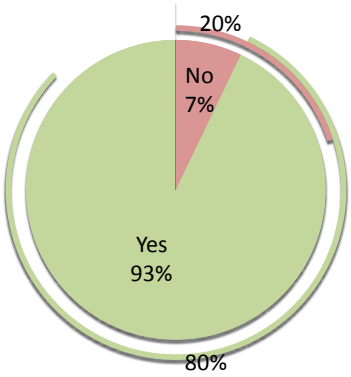
DOE: Yes - Management reviews are conducted quarterly and managers must document compliance.

DOI: Yes - The DOI Office of Law Enforcement and Security has a Compliance Division that conducts internal audits of intelligence systems, and with support from an ISE Privacy Official checks to ensure privacy and civil liberties are appropriately protected. DOI recently conducted a privacy review of IMARS, DOI's law enforcement system to evaluate adequacy of privacy protections and compliance with privacy laws and policies. Departmental policy requires DOI bureaus and offices to ensure that intelligence files are reviewed on an ongoing basis, but, at a minimum, reviewed annually, and to purge information not needed for retention. Doing this purging; only administrative records are kept, not records of the names of individuals or organizations.

2013
2012

MANAGING AND FOSTERING A CULTURE OF RESPONSIBLE INFORMATION SHARING

Question:
Does your agency have a dedicated Senior Information Sharing Executive per E.O. 13587?



# of Responses: 14

Maturity Level (1-3): 1

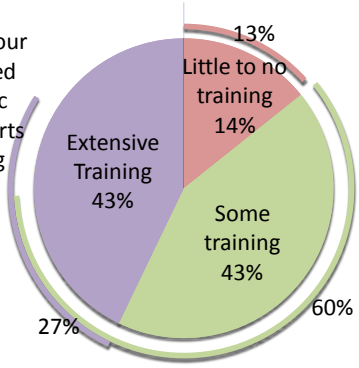
DHS: Yes - The Under Secretary of Intelligence and Analysis is the designated Senior Information Sharing Executive for DHS.

DOJ: Yes - The Chief Information Sharing Officer (CISO) is the dedicated FBI Senior Information Sharing Official required by E.O. 13587, and also serves as the FBI representative on the ISA IPC. Under the terms of a recent internal realignment, the CISO is now a direct report to the FBI Chief Knowledge Officer (CKO). The CKO reports directly to the Associate Deputy Director of the FBI and has Bureau-wide responsibility and authority. The CKO has been designated as the Principal FBI Official for Information and Intelligence Sharing Policy, and chairs the FBI Information Sharing Policy Board.

DoD: Yes - The DoD CIO currently fulfills this role. Additionally, the Joint Staff has a chair on the Information Sharing and Access Interagency Policy Committee (ISA-IPC).

DOC: Yes - The Senior Advisor for National Security and Critical Infrastructure Protection has been designated as the Senior Official for Information Sharing and Safeguarding.

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



# of Responses: 14

Maturity Level (1-3): 1

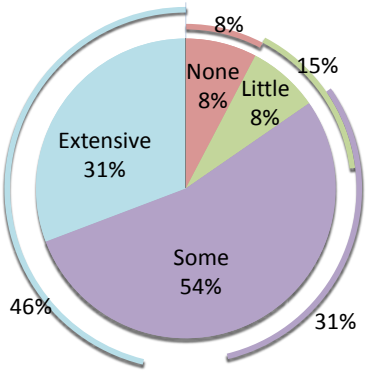
DOJ: Extensive Training - Training is completed at the Program level. (i.e. N-DEx, BATS, etc.) For instance, the N-DEx Program Office engages in best practices and professional standards to market, outreach, and conduct training events with local state, regional, tribal, and federal criminal justice agencies. N-DEx training opportunities support the mission to achieve and maintain the projected level of commitment of participation and fully expand the footprint of N-DEx as the only nationally-scaled information sharing system. N-DEx offers self-paced Computer Based Training supported by user training as needed. N-DEx personnel also provide Train-the-Trainer courses and materials and offer specific training to assist agencies with managing administrative duties related to N-DEx, conducting 20 training events in the past year. Mission-specific training for information sharing and collaboration exists on multiple levels. Agents and Intelligence Analysts are introduced to these concepts within their first weeks of employment through New Agents' Training and the Intelligence Basic Course. The Bureau promotes and facilitates external training opportunities for FBI and IC employees in analytic techniques, working groups, tabletop exercises (including international Weapons of Mass Destruction simulations) The Counterterrorism Division has instructed more than 600 Task Force Officers since 2011 in information-sharing protocols in response to the Fort Hood shootings, and maintains a close relationship with state and local law enforcement through annual training symposia. During the reporting period, the FBI provided Data Exploitation, Targeting and Integration for Results (DEXTIR) training to students from the National Geospatial-Intelligence Agency, Department of Homeland Security, Greensboro North Carolina Police Department and U.S. Air Force Office of Special Investigations.

DOS: Some Training - The Department currently offers many types of training through the Foreign Service Institute that support aspects of the Information Sharing Environment, specifically Safeguarding. Examples of these courses are as follows: Classified and SBU Info: ID and Marking; Information Sharing Environment 101; Cybersecurity Awareness; Information Assurance for Systems Managers.

HHS: Some Training - The Office of Security and Strategic Information (OSSI), Directorate of Counterintelligence and Intelligence has created a Department wide mandatory CI and Intelligence awareness training on HHS U for all employees, and CI training for a cadre of CI professionals throughout the department.

2013
2012

Question:
What degree of success have these trainings produced improvements to information safeguarding and stewardship?



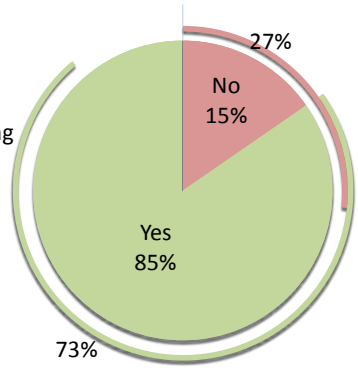
# of Responses: 13

Maturity Level (1-3): 2

DOJ: Some - The FBI requires all employees to complete annual training requirements regarding information sharing and safeguarding of information. Success is measured by employees completing mandated training and being held accountable for all aspects of content in the performance of their duties. In the WMDD realm, these trainings have better prepared individuals in handling any type of CBRN threat or incident. The WMDD has also certified approximately 30 WMD Coordinators to date. During 2012, the FBI's VA received up to 14,000 individual hits a month—nearly half of the Bureau employee workforce. During 2012, approximately 40,000 readers signed up for e-mail alerts to notify them about upcoming content on the LEB website. The training courses offered by CTD have educated Agents, Analysts, Task Force Officers, and the FBI's federal/state/local law enforcement partners about current domestic and international terrorist groups' ideologies, techniques, and threat levels. This ongoing exchange of information and knowledge continues to serve as a vital link in the FBI's ability to prevent and deter terrorist attacks against the United States and its citizens. The training educates our partners about federal laws, policies, and procedures to ensure that our partners have the requisite knowledge, training and tools needed to work with FBI Agents to infiltrate domestic and international terrorist organizations, thwart impending attacks, and obtain justice against those who participate in attacks against the United States. The training has produced a high degree of success, as evidenced by the efficient and appropriate information-sharing that occurred following the Boston Marathon bombing. Federal, State and local authorities were collocated at various facilities; further investigation into protocols confirmed that 'lessons learned' from prior security situations had been implemented properly.

DHS: Some - Some components have reported that these trainings have been successful; however, other components reported that there were no formal metrics in place to capture the data.

Question:
Do employees that support ISE-related priorities have "information sharing and collaboration" as a component of their performance appraisals?



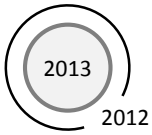
# of Responses: 13

Maturity Level (1-3): 1

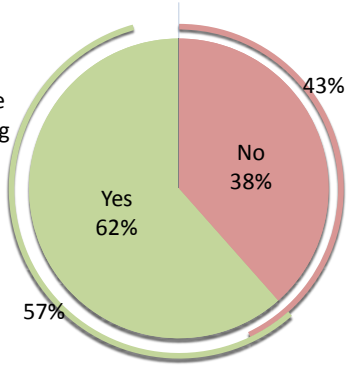
DoD: Yes - Several Assistant Secretary of Defense for Homeland Defense employees have information sharing/collaboration as an evaluation component of their performance appraisals and employees under the Defense Civilian Intelligence Personnel System have a mandatory performance element that emphasizes collaboration, teamwork and information sharing.

HHS: Yes - All personnel within the HHS Office of Security and Strategic Information (OSSI), the office coordinating ISE for the Department, have integrated within their performance plans a critical element capturing ISE information sharing and collaboration objectives.

DOJ: Yes - FBI Senior Executives are rated on "Collaboration and integration" as part of their performance evaluations. In addition, one of the critical elements within an Intelligence Analyst's performance appraisal is Engagement and Collaboration. This critical element measures the analyst's ability to "provide information and knowledge to achieve results" and "build and leverage diverse collaborative networks of coworkers, peers, customers, stakeholders, and team, within an organization or across the IC." Employees supporting ISE-related priorities do have 'information sharing and collaboration' as part of their performance appraisals. Special Agents and Intelligence Analysts have elements of information sharing and collaboration in their very job descriptions and are two of the core competencies to which all FBI employees are expected to adhere. In addition, most Performance Plans include a Critical Element (CE) entitled, "Acquiring, Applying, and Sharing Job Knowledge."



Question:
Do employees without direct ISE responsibilities have "information sharing and collaboration" as a performance objective?



# of Responses: 13

Maturity Level (1-3): 1

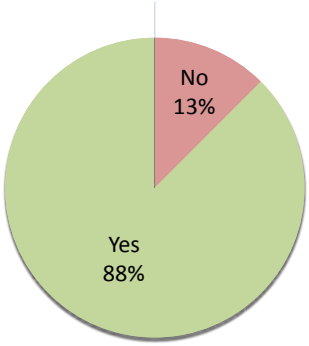
DHS: Yes - This is a requirement for Customs and Border Protection (CBP), Transportation Security Administration (TSA), Immigration and Customs Enforcement (ICE), United States Secret Service (USSS), United States Citizenship and Immigration Services (USCIS), and NPPD/IP.

DOJ: Yes - DEA has incorporated this as a component of their performance appraisal for all DEA I/As.

DOI: Yes - DOI law enforcement personnel have performance standards that include collaboration and information sharing. However, the vast numbers of our 73,000 employees do not.

NGA: No - There is no agency mandate that employees without ISE- related priorities have 'Engagement and Collaboration' (as defined in Question 3) as a Performance Objective.

Question:
Does your agency update the workforce on new information sharing agreements/initiatives? If YES, how?



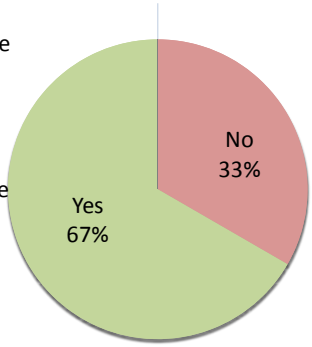
# of Responses: 8

Maturity Level (1-3): 1

USAF: Yes - Formal Briefings and posting of policy guidance and directives.

NGA: Yes - New information sharing agreements and initiatives are shared primarily via the Information Sharing Working Group (ISWG) whose members will disseminate it to their respective organizations.

Question:
Does your agency have a governance body responsible for information sharing and safeguarding that plans and oversees the agency self assessment process per E.O. 13587?



# of Responses: 18

Maturity Level (1-3): 2

DHS: Yes - The Information Sharing and Safeguarding Governance Board is the DHS Enterprise-wide body for information sharing and safeguarding.

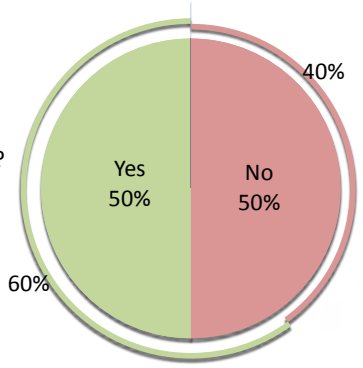
DOJ: Yes - The department is in the process of reestablishing a department wide governance body to ensure responsible sharing and safeguarding of information.

The ATF has internal Governance Board.

The FBI Access Policy Group, with oversight by the Information Sharing Policy Board, oversees the FBI insider threat self-assessment process.

DoD: No - The DoD does not use a formal governance body to oversee the self-assessment process. Instead of a governance body, the DoD holds meetings led by the DoD CIO/Cybersecurity Directorate with POCs from OUSD(I), Security, and USD(P) to coordinate on EO 13587 actions including the self-assessment. Since the DoD CIO/Cybersecurity Directorate reports to the principals there is a tight linkage with existing DoD governance entities.

Question:
Does your agency offer information sharing related awards (monetary or non-monetary)?



# of Responses: 14

Maturity Level (1-3): 2

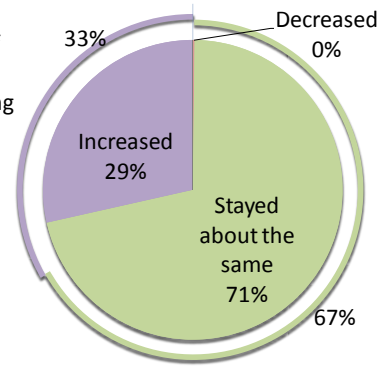
DHS: Yes - NPPD, ICE, CBP, and Coast Guard, offer awards (monetary and non-monetary) for information sharing achievements.

HHS: Yes - ISE is an element of OSSI employees PMAPs and to obtain qualifying scores for a monetary award, success in information sharing and collaboration is required.

DOT: Yes - Members of the Intelligence Division receive both monetary and non-monetary awards for their work in information sharing.

DOJ: Yes - The FBI, through its Office of the Chief Knowledge Officer, conducts a yearly canvass for nominations for the Knowledge Awards. The goal of this program is to "Increase people-to-people connectivity by sharing best practices, establish partnerships across the FBI by connecting people with common issues and interests; provide support by recognizing issues/gaps and providing solutions identified through submissions and incentivize and recognize excellence in knowledge management and sharing."

Question:
Has nomination of candidates for information sharing and collaboration awards increased, decreased, or stayed the same since it was first offered?



# of Responses: 14

Maturity Level (1-3): 2

DOJ: Increased - Additional recognition for outstanding DIBs and other outstanding writing of reports to the IC from the Chief of Intelligence (monetary).

FBI - The CISO recognizes individuals or groups for information sharing awards, and the nomination of candidates for FBI information sharing awards has steadily increased since the inception of the program. The Information Sharing Awards Program is being integrated into the FBI Knowledge Awards Program under the purview of the Office of the Chief Knowledge Officer. Submissions for these awards have increased since they were first offered in 2010; specific data regarding candidate numbers are unavailable at this time.

HHS: Increased - Inasmuch as OSSI has been established as an integrated security organization within the past couple of years, it is with this past year's performance cycle that we have seen the capturing of this element. As such, those efforts to underscore the collaboration and information sharing mandate, are now being recognized in the PMAPs for employees.

This page intentionally left blank.

APPENDIX B – MISSION-BASED TEST SCENARIOS

Test scenarios are used to demonstrate information sharing capabilities in a mission context; the use of test scenarios allows the enterprise to determine if the ISE is achieving its desired capabilities. PM-ISE also encourages agencies to create scenarios independently and has provided a "cookbook" to assist with agency development of a complete performance framework. Additional information for developing scenarios was provided to agencies on the ISE Blog.[75] These resources allow agencies to possess and develop their own compatible performance frameworks to further capabilities in key ISE mission areas. These integrated performance frameworks, with line-of-sight from program to agency to ISE-level metric tracking, help guide ISE performance management, which will expand as the ISE collectively matures.

The annual ISE Performance Assessment Questionnaire assesses ISE-level functions that enable the delivery of mission services and capabilities against a spectrum of maturity. Table B-1 below describes the capability areas targeted by the ISE performance assessment and how they relate to each stage of maturity.

Table B-1. ISE Capability Areas and Maturity Spectrum.

	MATURITY STAGE 1 2012-2013 ENVIRONMENT	MATURITY STAGE 2 2-3 YEAR TIME HORIZON	MATURITY STAGE 3 5-7 YEAR TIME HORIZON
COMMUNITY	Community **Awareness**	Community **Involvement**	Community **Integration**
PROCESS	Process **Exploration**	Process **Adoption**	Process **Harmonization and Compliance**
TECHNOLOGY	Technology & Standards **Awareness**	Technology & Standards **Exploration**	Technology & Standards **Integration**

Test scenarios remain 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.

Last year's report references the ten test scenarios developed in 2011. This year, six of those scenarios are used to assess the progress of the ISE with respect to information sharing capabilities in specific high-value mission areas:

[75] "Improving the Performance of Info Sharing Programs: A Guide to Building Performance Test Scenarios," October 26, 2012; http://www.ise.gov/blog/adrienne-l-walker/improving-performance-info-sharing-programs-guide-building-performance-test

- Improving role-based access to ISE-suspicious activity reports (SAR) and underlying case file content—implementation of privacy policy automation (1)
- Improved law enforcement maritime response to a weapon-of-mass-destruction threat by enhancing first responders' situational awareness (2)
- Improving cross-domain access to distributed information through federated search (3)
- Removing impediments to federal acquisition and enabling out-of-the-box future interoperability through standards (4)
- Using machine generated SARs to aid detection of threats to critical infrastructure and key resources (CIKR) (7)
- Using the National Information Exchange Model (NIEM) as an enabler to share international counterterrorism data on gang-related activity for watchlisting and screening (8)

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 in the future. Each response demonstrates the analysts', operators', and investigators' improved ability to execute their mission objectives based on investments in information sharing. The remaining four scenarios are used by the office of the PM-ISE to shape conversations around the definitions for future capabilities within shared mission areas among ISE agencies. These scenarios are:

- Enabling event deconfliction through common standards to promote officer safety (5)
- Incentivizing information sharing of insider threat information within agencies and throughout government (6)
- International humanitarian aid and disaster relief coordination efforts (9)
- Improving public health response to biological threats with increased information to first responders (10)

With agency participation, PM-ISE staff crafted an additional scenario driven by National Security Staff and Office of Management and Budget (OMB) priorities. With cybersecurity being one of the primary focus areas for this Administration, addressing challenges in information sharing among federal cyber centers, as well as with state and local partners, is a key element to improving our nations' security.

- Driving enhanced shared situational awareness for cyber threat information among federal partners and fusion centers (11)

The following graphics represent the six scenarios used to assess ISE progress based on the results of the 2013 performance assessment questionnaire, followed by the four used to define future capabilities, and the newest scenario referencing cybersecurity.

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 vehicle. 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.

MATURITY STAGE 1 (NOW)			MATURITY STAGE 2 (2-3 YEARS)			MATURITY STAGE 3 (5-7 YEARS)		
	Manual approval to access data based on unreliable, un-standardized "need-to-know"	**Community Awareness** Process Exploration Technology & Standards Awareness		Policies and procedures in place to allow expedited sharing	Community Involvement **Process Adoption** Technology & Standards Exploration		Role-based access to ISE-SAR, including privacy policy automation	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

Community is **Aware**	**Process Adoption** with standardized information sharing agreements are still required to enable the capabilities described in this scenario

RELATED METRICS FROM 2013 ISE PERFORMANCE ASSESSMENT QUESTIONNAIRE, SCENARIO: PRIVACY

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	Is your agency operating under an approved privacy policy consistent with the ISE Privacy Guidelines?	A	N/A	N/A
Process	Does your agency's ISE Privacy and Civil Liberties (P/CL) Official receive reports of errors in cases involving information which may impact the privacy or civil liberties of individuals?	A	N/A	N/A
Process	Does your agency notify ISE participants who receive the agency's protected information of all applicable access, use, retention, or disclosure limitations in cases where personally identifiable information of individuals is being shared?	N/A	N/A	A
Process	Does your agency review protected information for accuracy before it is made available to the ISE?	N/A	A	N/A
Process	Does your agency use a government-wide template in developing information sharing agreements?	N/A	B	N/A
Process	Has your agency (outside of the Privacy Act) developed and provided an ongoing training program specific to the implementation of the ISE Privacy Guidelines to personnel authorized to share protected information?	A	N/A	N/A
Process	Has your agency adopted and implemented procedures to facilitate the prevention, identification, and correction of any errors in protected information to ensure accuracy and that it has not erroneously been shared?	N/A	A	N/A
Process	Has your agency implemented adequate review and audit mechanisms to enable the agency's ISE P/CL Official and other authorized officials to verify that the agency and its personnel are complying with the ISE Privacy Guidelines?	N/A	N/A	A
Process	Has your agency put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control?	N/A	A	N/A
Process	Has your agency taken steps to facilitate appropriate public awareness of its policies and procedures for implementing the ISE Privacy Guidelines?	A	N/A	N/A
Process	Is your agency's P/CL office (led by a P/CL officer or Senior Agency Official for Privacy) actively involved in planning, development, and oversight of information sharing and safeguarding activities? Please give examples.	N/A	A	N/A

Legend: **A** = Meets expectation of the ISE. **B** = Partially meets expectations of the ISE. **C** = Does not meet expectation of the ISE. **N/A** = The question is not applicable at this level of maturity.

SCENARIO #02: Improved Law Enforcement Maritime Response to a WMD Threat by Enhancing First Responders' Situational Awareness

SITUATION

The vast Great Lakes region along the northern border is a favored area for illicit smuggling. Interdiction is especially difficult due to the fact that at different intervals along the border, various federal, state, local, tribal, and/or territorial law enforcement agencies hand off or share jurisdiction. In addition to local authorities, the Coast Guard, Customs and Border Protection, and Immigration and Customs Enforcement conduct operations across jurisdictions in the Great Lakes region. An intelligence analyst at federal Agency X receives credible reporting that a cargo ship transiting Lake Superior is carrying a WMD device.

MATURITY STAGE 1 (NOW)			MATURITY STAGE 2 (2-3 YEARS)			MATURITY STAGE 3 (5-7 YEARS)		
	Manual coordination through local Fusion Center with point-to-point communications and a non-integrated response	**Community Awareness** Process Exploration Technology & Standards Awareness		Integrated response directed by Fusion Centers through common operating models and procedures	Community Involvement **Process Adoption** Technology & Standards Exploration		Total situational awareness through integrated systems, accelerated responses, and a safer interdiction process	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

Community moving from **Awareness** to **Adoption**	Process Exploration and **Adoption** are ongoing with efforts around improving training, governance, and access

RELATED METRICS FROM 2013 ISE PERFORMANCE ASSESSMENT QUESTIONNAIRE, SCENARIO: MARITIME

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	Does your agency have a dedicated Senior Information Sharing Executive per Executive Order (EO) 13587?	A	N/A	N/A
Community	Does your agency update the workforce on new information sharing agreements/initiatives? If YES, how?	A	N/A	N/A
Community	Does your agency offer information sharing related awards (monetary or non-monetary)?	N/A	B	N/A
Community	Has nomination of candidates for information sharing and collaboration awards increased, decreased, or stayed the same since it was first offered?	N/A	B	N/A
Process	Do employees that support ISE-related priorities have "information sharing and collaboration" as a component of their performance appraisals?	A	N/A	N/A
Process	Do employees without direct ISE responsibilities have "information sharing and collaboration" as a performance objective?	B	N/A	N/A
Process	To what degree has your agency implemented any mission-specific training that supports information sharing and collaboration? Please provide examples.	B	N/A	N/A
Process	Does your agency have a governance body responsible for information sharing and safeguarding that plans and oversees the agency self-assessment process per EO 13587?	N/A	B	N/A
Process	To what extent is your agency utilizing the Library of National Intelligence (LNI)?	N/A	B	N/A
Process	What degree of success has training produced improvements to information safeguarding and stewardship?	N/A	B	N/A

Legend: **A** = Meets expectation of the ISE. **B** = Partially meets expectations of the ISE. **C** = Does not meet expectation of the ISE. **N/A** = The question is not applicable at this level of maturity.

SCENARIO #03: Improving Cross-domain Access to Distributed Information through Federated Search

SITUATION

Employees at an insurance company have noticed suspicious behavior from one of their co-workers. A group of employees reported to a terrorist hotline that they noticed one of their associates repeatedly going to terrorist-leaning websites and printing out bomb making schematics from a company shared printer. Upon receipt of this tip, a tactical intelligence analyst from Agency X must then assess if there is enough credible information to open a full anti-terror investigation.

MATURITY STAGE 1 (NOW)			MATURITY STAGE 2 (2-3 YEARS)			MATURITY STAGE 3 (5-7 YEARS)		
	Individual checks through databases from sensitive to top secret, manual collation and analysis of data	**Community Awareness** Process Exploration Technology & Standards Awareness		Common identity standards enable easier access and search through disparate networks and databases	Community Involvement **Process Adoption** Technology & Standards Exploration		Single point of entry for each classification level, federated search and easy analysis	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

Community Adoption and **Integration** are ongoing with efforts in security reciprocity	**Process Exploration** and **Adoption** are ongoing with integration of FICAM planning efforts	**Technology & Standards Involvement** and **Integration** efforts still required in security reciprocity and attribute exchanges

RELATED METRICS FROM 2013 ISE PERFORMANCE ASSESSMENT QUESTIONNAIRE, SCENARIO: FEDERATED SEARCH

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	From how many organizations does your agency accept (and make accreditation decisions without retesting) IT security certification bodies of evidence? i.e., does your agency practice IT security reciprocity.	N/A	N/A	B
Community	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? Please provide examples.	N/A	N/A	B
Process	Does your agency have a defined Memorandum of Understanding or Agreement (MOU/MOA) development process that covers discovery and access to data by external partners and systems?	A	N/A	N/A
Process	Does your agency plan to fund the development of Controlled Unclassified Information (CUI) self-inspection programs including reviews and assessments to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation on or before Sep. 30, 2014?	B	N/A	N/A
Process	Does your agency plan to fund the integration of CUI requirements into information systems as they are developed and/or upgraded on or before Sep. 30, 2014?	B	N/A	N/A
Process	Has your agency aligned their Sensitive but Unclassified (SBU) architecture with the publication of geospatial Critical Information Requirements and authoritative source(s) necessary to meet Presidential Policy Directive 8 Mission Areas in open standards?	N/A	B	N/A
Process	Has your agency incorporated access policies that protect privacy, civil rights and civil liberties using a common government-wide template for each data source into their SBU architecture?	N/A	A	N/A
Process	Has your agency submitted a data access management Plan of Action and Milestones based on privacy, civil rights and civil liberties attributes, Attribute Based Access Control, and Federal Identity, Credential, and Access Management (FICAM)?	N/A	C	N/A
Process	Has your agency submitted their implementation schedule for agency-specific production, delivery, and maintenance for each SBU geospatial dataset for registration to the ISA IPC?	N/A	C	N/A
Technology	Does your agency plan to adopt FICAM standards?	A	N/A	N/A
Technology	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?	N/A	A	N/A
Technology	Has your agency aligned their SBU architecture authentication consistent with FICAM?	N/A	B	N/A
Technology	Has your agency identified and published SBU geospatial data (cataloged and registered) in the Semantic Ontology and Registry on the DHS Geospatial Information Infrastructure?	N/A	C	N/A
Technology	To what extent has your agency implemented FICAM standards? Please explain.	N/A	B	N/A
Technology	Has your agency implemented an accessible authoritative source at any classification level?	N/A	N/A	A
Technology	To what extent does your agency have documented policies and/or implementing guidelines on IT security reciprocity stating the conditions under which you will accept the security certification and/or accreditation/authorization of another organization?	N/A	N/A	B

Legend: **A** = Meets expectation of the ISE. **B** = Partially meets expectations of the ISE. **C** = Does not meet expectation of the ISE. **N/A** = The question is not applicable at this level of maturity.

SCENARIO #04: Removing Impediments to Federal Acquisition and Enabling Out-of-the-Box future Interoperability through Standards

SITUATION

Investigative efforts, such as undercover operations, create the potential for conflict between agencies which are unknowingly working in close proximity to each other or agencies which may be coordinating an event on the same suspect at the same time. .A Project Manager from Agency X plans to acquire an event registry solution to aid with officer deconfliction to determine if there are event conflicts with any new police action at the federal, state, local, and tribal levels of government.

MATURITY STAGE 1 (NOW)		MATURITY STAGE 2 (2-3 YEARS)		MATURITY STAGE 3 (5-7 YEARS)	
Decentralized standards governance	Community Awareness **Process Exploration** **Technology & Standards Awareness**	Government-wide standards oversight gives a common point of entry to acquisition and accelerates future interoperability	Community Involvement **Process Adoption** **Technology & Standards Exploration**	Single standards repository with common governance integrated with GSA policies streamline acquisition and enable out of the box interoperability	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

Process Exploration and **Adoption** efforts proceeding with the increasing usage of open standards in grants and acquisitions	**Technology & Standards Awareness** and **Exploration** efforts ongoing through standards policy updates

RELATED METRICS FROM 2013 ISE PERFORMANCE ASSESSMENT QUESTIONNAIRE, SCENARIO: STANDARDS-BASED ACQUISITION

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Process	Are ISE functional standards considered when issuing mission system requests for proposals (RFPs) and/or grants (for ISE-related systems)?	B	N/A	N/A
Process	Does your agency have a single authoritative repository related to ISE Technical or Functional Standards?	N/A	B	N/A
Process	Has your agency provided updated grant or acquisition policies, standards-based requirements, and grants references where applicable to account for federal best practices, policy and toolkit recommendations, and alignment with the ISE common information sharing standards to PM-ISE?	N/A	B	N/A
Process	To what extent are ISE functional standards used when issuing mission system RFPs and/or grants (for ISE-related systems)?	N/A	C	N/A
Technology	Are ISE technical standards considered when issuing mission system RFPs and/or Grants (for ISE-related systems)?	B	N/A	N/A
Technology	Has your agency provided information sharing and safeguarding standards activities (current or planned, public or private) to PM-ISE and OMB?	B	N/A	N/A
Technology	To what extent are ISE technical standards used when issuing mission system RFPs and/or grants (for ISE-related systems)?	N/A	C	N/A

Legend: **A** = Meets expectation of the ISE. **B** = Partially meets expectations of the ISE. **C** = Does not meet expectation of the ISE. **N/A** = The question is not applicable at this level of maturity.

SCENARIO #05: Enabling Event Deconfliction through Common Standards to Promote Officer Safety

SITUATION

Law enforcement agencies use an intranet-based Officer Safety Event Deconfliction System to store and maintain data on planned law enforcement events. Often, investigative efforts such as undercover operations, arrests, raids and other high risk situations create the potential for conflict between federal, state, local and tribal law enforcement agencies. They unknowingly work in close proximity to each other or may be coordinating an event on the same suspect at the same time. Federal law enforcement officers from Agency X are planning a raid on a home where it is believed a group of suspected drug traffickers are in possession of a large amount of illegal drugs.

MATURITY STAGE 1 (NOW)		MATURITY STAGE 2 (2-3 YEARS)		MATURITY STAGE 3 (5-7 YEARS)	
Point-to-point event conflict resolution	Community Awareness Process Exploration Technology & Standards Awareness	Standards oversight and common operating models enable a more efficient manual process	Community Involvement Process Adoption Technology & Standards Exploration	Standards-compliant, automated deconfliction enables total situational awareness	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

No related ISE-level metrics from 2013 ISE Performance Assessment.

PROGRAM-LEVEL METRICS, SCENARIO: OFFICER DECONFLICTION

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	% of involved agencies that have conflict resolution plans with include information sharing	A	Inc	Inc
Community	% of involved agencies that have individual event resolution plans	A	Inc	Inc
Community	% of involved agencies have consolidated and coordinated conflict resolution plans	N/A	A	Inc
Process	# of officer conflict incidents	N/A	N/A	A
Process	Avg. required time to conduct event conflict assessments (includes system checks and personal communications)	N/A	A	Dec.
Process	% of involved agencies with standards-compliant information sharing MOUs	N/A	N/A	A
Technology	% of system owners compliant with ISE technical/functional standards	A	Inc	Inc
Technology	% of involved agencies with FICAM compliant system access	N/A	N/A	A

Legend:
A = This metric is first applicable at this stage of maturity.
Dec = This metric is supposed to decrease as maturity increases.
Inc = This metric is expected to increase as maturity increases.
N/A = This metric is not yet applicable at this level of maturity.

SCENARIO #06: Incentivizing Information Sharing of Insider Threat Information within Agencies and Throughout Government

SITUATION

Federal Agency X employee has become aware of anomalous behavior by an employee from Federal Agency Y on Agency X's classified network that potentially could compromise national security information. Agency X employee must begin a structured engagement with Agency Y and involve senior personnel from both agencies to analyze behavior on this and other networks to which the employee has access.

MATURITY STAGE 1 (NOW)			MATURITY STAGE 2 (2-3 YEARS)			MATURITY STAGE 3 (5-7 YEARS)		
	Impediments to information sharing result in heterogeneous responses to insider threats	Community Awareness Process Exploration Technology & Standards Awareness		Increased incentives lower the barriers to sharing, enabling integrated insider threat responses	Community Involvement Process Adoption Technology & Standards Exploration		Incentivized sharing of insider threat information enables efficient, automated, cross-domain protection of government networks and systems	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

No related ISE-level metrics from 2013 ISE Performance Assessment.

PROGRAM-LEVEL METRICS, SCENARIO: INSIDER THREAT

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	% of agencies that have a senior official accountable for classified information	A	Inc	Inc
Community	# of nominations for information sharing awards per agency	A	Inc	Inc
Community	% of personnel who have received mission training on information sharing	N/A	A	Inc
Process	% of agencies with formalized processes for sharing classified information	A	Inc	Inc
Process	% of incident response programs coordinated with ISE functional standards	N/A	A	Inc
Technology	% of agencies that have implemented personal identity verification (PIV) compliant programs	A	Inc	Inc

Legend:
A = This metric is first applicable at this stage of maturity.
Dec = This metric is supposed to decrease as maturity increases.
Inc = This metric is expected to increase as maturity increases.
N/A = This metric is not yet applicable at this level of maturity.

SCENARIO #07: Using Machine Generated SARs to Aid Detection of Threats to CIKR

SITUATION

There is a concentration of Critical Infrastructure and Key Resource (CIKR) facilities in Virginia's Hampton Roads region, including shipping, transportation, rail, power, communications, emergency services, banking & finance, chemical, and many others. Recently, there has been an unusual spike in physical perimeter breach warnings at high-value chemical, telecommunications, and shipping facilities, all located closely in Norfolk, Portsmouth, Chesapeake, and Virginia Beach. Additionally, the Chesapeake power plant is experiencing increases in network security warnings and potential data breaches.

MATURITY STAGE 1 (NOW)		MATURITY STAGE 2 (2-3 YEARS)		MATURITY STAGE 3 (5-7 YEARS)	
Distributed, heterogeneous response to threats depend on CIKR sector and law enforcement jurisdictional factors	Community Awareness Process Exploration **Technology & Standards Awareness**	Policies and procedures in place to allow expedited sharing	**Community Involvement** **Process Adoption** Technology & Standards Exploration	Role-based access to ISE SAR, including privacy policy automation	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

Community Integrating through participation in common task forces and mission functions	**Process Adoption** efforts are ongoing with continuous training	**Technology & Standards Awareness** efforts still required to interconnect the intelligence enterprise

RELATED METRICS FROM 2013 ISE PERFORMANCE ASSESSMENT QUESTIONNAIRE, SCENARIO: SAR 2.0

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	Does your agency participate in the National Joint Terrorism Task Forces?	N/A	A	N/A
Community	Does your agency participate in the National Network of Fusion Centers (state and major urban areas)?	N/A	B	N/A
Process	Does your agency have a process in place to validate SARs?	B	N/A	N/A
Process	Has your agency delivered a plan to align resource decisions to the Resource Allocation Criteria policy to DHS?	N/A	C	N/A
Process	To what extent has your agency incorporated ISE functional standards into the management and implementation of its ISE-related mission business processes?	N/A	B	N/A
Process	To what extent does your agency incorporate fusion center information into its own products and services? Please explain.	N/A	N/A	C
Process	To what extent is information gathered from international partners integrated into the watchlisting and screening process?	N/A	N/A	C
Technology	Does your agency have a live SAR database?	B	N/A	N/A
Technology	Does your agency have a plan to implement a capability to interconnect SBU/CUI networks in order to share terrorism and homeland security information?	B	N/A	N/A
Technology	Does your agency provide SAR training (either directly or indirectly)?	A	N/A	N/A
Technology	Does your agency utilize eGuardian (FBI)?	B	N/A	N/A
Technology	To what extent has your agency implemented interconnection plans for SBU/CUI networks supporting ISE-related missions?	C	N/A	N/A
Technology	To what extent has your agency incorporated ISE technical standards into enterprise architectures and IT capability?	N/A	B	N/A

Legend: **A** = Meets expectation of the ISE. **B** = Partially meets expectations of the ISE. **C** = Does not meet expectation of the ISE. **N/A** = The question is not applicable at this level of maturity.

SCENARIO #08: Using the National Information Exchange Model (NIEM) as an Enabler to Share International Counterterrorism Data on Gang-related Activity for Watchlisting and Screening

SITUATION

Gang-related activities are prevalent near border regions of the United States. Drug trafficking, human trafficking, smuggling, and other serious crimes by gangs are often used by terrorist organizations as a means to finance their activities. Governments on both sides of the border are increasing their focus on gang-related activity, not only to reduce crime, but to stem funds destined for terrorist groups. While analyzing stolen vehicle trends, a tactical intelligence analyst from border state Fusion Center X notices that there is a very low recovery rate of stolen automobiles. A tactical intelligence analyst at state Fusion Center Y is analyzing trends of stolen automobiles and notices that there is little to no information on a significant portion of these vehicles, making him think they may no longer be in the United States.

MATURITY STAGE 1 (NOW)			MATURITY STAGE 2 (2-3 YEARS)			MATURITY STAGE 3 (5-7 YEARS)		
	Manual coordination with point-to-point communication between international partners	**Community Awareness** **Process Exploration** Technology & Standards Awareness		Bridging manual coordination with agreed-upon automated sharing of key data to international partners	**Community Involvement** **Process Adoption** Technology & Standards Exploration		Automated transfer of applicable data between countries with feedback loops in place to improve future watchlisting and screening efforts	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

Community Awareness and **Involvement**	**Process Exploration** and **Adoption** efforts proceeding with the increasing usage of enterprise and segment architectures	**Technology & Standards Exploration** and **Integration** efforts ongoing via PKI and the use of common standards

RELATED METRICS FROM 2013 ISE PERFORMANCE ASSESSMENT QUESTIONNAIRE, SCENARIO: GLOBALIZING NIEM

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	Does your agency engage with industry Standards Development Organizations to further voluntary consensus standards?	A	N/A	N/A
Community	Does your agency have an authoritative council for standards development?	N/A	B	N/A
Process	Can members of your agency obtain public key infrastructure (PKI) certificates for ISE-related systems?	A	N/A	N/A
Process	How often does your agency reference 'mission segment architectures' (e.g. SAR) when implementing ISE mission business processes?	N/A	B	N/A
Technology	To what extent does your agency use PKI for ISE-related information and mission systems?	A	B	N/A
Technology	To what extent has your agency incorporated Common Information Sharing Technical Standards into your architectures?	N/A	B	N/A
Technology	To what level has access to terrorism information from ISE partners improved by utilizing their designated ISE Shared Space?	N/A	N/A	C

Legend: **A** = Meets expectation of the ISE. **B** = Partially meets expectations of the ISE. **C** = Does not meet expectation of the ISE. **N/A** = The question is not applicable at this level of maturity.

SCENARIO #09: International Humanitarian Aid and Disaster Relief Coordination Efforts

SITUATION

It is common for multiple organizations, including U.S. and foreign government organizations, NGOs, and private relief organizations, to respond to the same humanitarian disaster recovery efforts around the globe. Success in coordinating efforts between all of these organizations is dependent upon efficiently sharing the right information with the right people in a format that allows them to act in time to do the most good. A natural disaster occurs in Foreign Country X and their government requests humanitarian aid and disaster relief from the international community.

MATURITY STAGE 1 (NOW)		MATURITY STAGE 2 (2-3 YEARS)		MATURITY STAGE 3 (5-7 YEARS)	
Manual coordination of disaster relief efforts run through mobile MEU command with multiple international and NGOs	Community Awareness Process Exploration Technology & Standards Awareness	On the fly Community of Interest (COI) for coordination run through the MEU; manual access processes and coordination required for verification	Community Involvement Process Adoption Technology & Standards Exploration	Pre-built COI run through the local embassy with many responders pre-integrated	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

No related ISE-level metrics from 2013 ISE Performance Assessment.

PROGRAM-LEVEL METRICS, SCENARIO: HUMANITARIAN AID AND DISASTER RELIEF

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	% of involved groups relying on manual, point-to-point communications	A	Dec	Dec
Community	% of involved agencies that have individual event resolution plans	A	Inc	Inc
Process	# of responder conflict incidents	A	Dec	Dec
Process	# of deconfliction incidents required during humanitarian aid/disaster relief effort	A	Dec	Dec
Process	MEU medical and engineering team response time	N/A	A	Dec
Process	Community of Interest startup time	N/A	A	Dec
Process	Coordination level of effort (man-hours)	A	Dec	Dec
Technology	% of responders with verified identities during aid efforts	N/A	N/A	A
Technology	# of access problems within community of interest	N/A	A	Dec

Legend:
A = This metric is first applicable at this stage of maturity.
Dec = This metric is supposed to decrease as maturity increases.
Inc = This metric is expected to increase as maturity increases.
N/A = This metric is not yet applicable at this level of maturity.

SCENARIO #10: Improving Public Health Response to Biological Threats with Increased Information to First Responders

SITUATION

In order to protect both first responders and safeguard the population during a terrorist threat, public health information and decisionmaking must be integrated into the incident response. Credible information of a terrorist threat against a bio-technology firm specializing in infectious disease research has been discovered by Federal Agency X.

MATURITY STAGE 1 (NOW)		MATURITY STAGE 2 (2-3 YEARS)		MATURITY STAGE 3 (5-7 YEARS)	
	Lack of cleared health personnel and non-uniform relationships between state justice and health groups require a high level of manual coordination Community Awareness Process Exploration Technology & Standards Awareness		Policies and procedures in place to allow expedited sharing and integrate health response Community Involvement Process Adoption Technology & Standards Exploration		Automated system access along with policy frameworks allow for quicker, integrated responses Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

No related ISE-level metrics from 2013 ISE Performance Assessment.

PROGRAM-LEVEL METRICS, SCENARIO: PUBLIC HEALTH RESPONSE

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	% of state health agencies with cleared personnel	A	Inc	Inc
Community	% of state health and state justice agencies with jointly agreed-upon CONOPS for chemical/bio threat response	N/A	A	Inc
Community	% of state health agencies with access to federal information systems for chemical/bio threat intelligence sharing	N/A	A	Inc
Community	% of state health agencies with personnel having direct physical access to Fusion Centers	N/A	A	Inc
Community	% of state health agencies with system access at Fusion Centers	N/A	A	Inc
Process	Avg. Fusion Center threat notification time	A	Dec	Dec
Process	Avg. federal health agency notification time	A	Dec	Dec
Process	Avg. state health agency notification time	A	Dec	Dec
Process	% of relevant information that cannot be released to state health officials during response	N/A	A	Dec

Legend:
A = This metric is first applicable at this stage of maturity.
Dec = This metric is supposed to decrease as maturity increases.
Inc = This metric is expected to increase as maturity increases.
N/A = This metric is not yet applicable at this level of maturity.

SCENARIO #11: Driving Enhanced Shared Situational Awareness for Cyber Threat Information Among Federal Partners and Fusion Centers

SITUATION

Cyberspace is a growing avenue for threats—including terrorism-related threats—to the national security of the United States. Media reports on the Stuxnet and Flame viruses have highlighted the capability of cyber-based attacks on critical infrastructure to result in physical damage. This and other nearly daily revelations have raised public concerns regarding the vulnerability of U.S. critical infrastructure. A key mitigation for these cyber-based threats is the ability to securely share sensitive and classified cyber threat and incident information quickly, using commonly understood terminology, among a broad constituency of federal and non-federal partners, while maintaining important privacy and civil liberties protections.

MATURITY STAGE 1 (NOW)			MATURITY STAGE 2 (2-3 YEARS)			MATURITY STAGE 3 (5-7 YEARS)		
	Human-speed, fractured sharing processes leave gaps in coverage and response	Community Awareness Process Exploration Technology & Standards Awareness		Expedited sharing between federal cyber centers as well as fusion centers drives enhanced decision-making ability	Community Involvement Process Adoption Technology & Standards Exploration		Standard cyber sharing processes in place with the ability for true federated common operational pictures among federal, state, and local partners	Community Integration Process Harmonization & Compliance Technology & Standards Integration

OVERALL ASSESSMENT

No related ISE-level metrics from 2013 ISE Performance Assessment.

PROGRAM-LEVEL METRICS, SCENARIO: CYBERSECURITY INFORMATION SHARING

CAPABILITY	QUESTION	STAGE 1	STAGE 2	STAGE 3
Community	% of physical CIKR facilities in Fusion Center area of responsibility (AOR) reporting and participating in cyber incident sharing	A	Inc	Inc
Process	% of fusion centers using Cyber Threat information standard to share information	A	Inc	Inc
Process	Avg. time to disseminate incident information from Fusion Centers to all relevant CIKR facilities in AOR	N/A	A	Dec
Process	% of involved agencies with formalized processes for sharing classified information	A	Inc	Inc

Legend:
A = This metric is first applicable at this stage of maturity.
Dec = This metric is supposed to decrease as maturity increases.
Inc = This metric is expected to increase as maturity increases.
N/A = This metric is not yet applicable at this level of maturity.

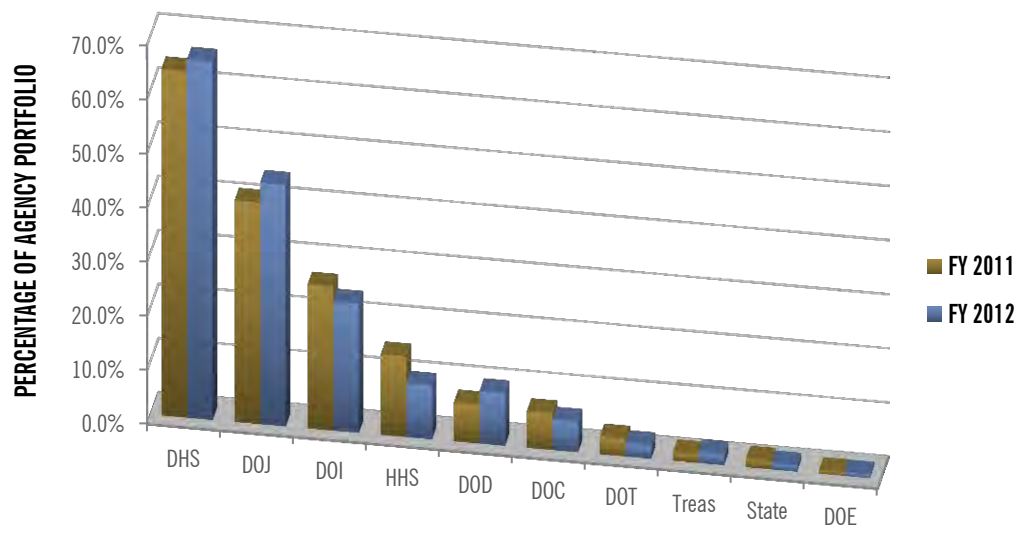
This page intentionally left blank

APPENDIX C – ISE INVESTMENTS

Partner agencies continue to make strategic information technology (IT) investments. Investment data captured via OMB's Exhibit 53 reporting provides a means to examine overall IT spending across the Federal Government as well as agency-level IT spending. It also provides visibility into IT investments aligned with strategic information sharing.

At the Federal Government-level, IT spending aligned with one or more ISE priorities remained consistent with FY 2011 spending at approximately 14%. Figure C-1 depicts the percentage of IT budgets aligned with at least one of the ISE priorities broken out by agency and presents a comparison between last and this year's ISE-aligned IT investments. The Department of Homeland Security (DHS), Department of Justice (DOJ), and the Department of Interior (DOI) are the agencies with the largest percentage of IT spending aligned with ISE priorities, which is also consistent with last year's reporting.

While this rank ordering remains nearly unchanged from last year's reporting, there are changes within individual agencies. For example, compared to last year, the Department of Defense (DoD) increased its ISE-aligned IT investment by 2.5%, DHS by 2.0%, and DOJ by 3.7% representing the largest increase within an agency.



Source: FY 2011 and FY 2012 funding data as reported via the IT Dashboard.

Figure C-1. Agency IT Portfolios Aligned to ISE Priority Areas (year to year comparison)

Similar to last year's reporting, three quarters of IT investments aligned to ISE priority areas directly supported agency-specific missions, indicating that agencies remain focused on supporting their respective mission objectives that further the value of information sharing and safeguarding. Figure C-2 depicts this along with other allocations.

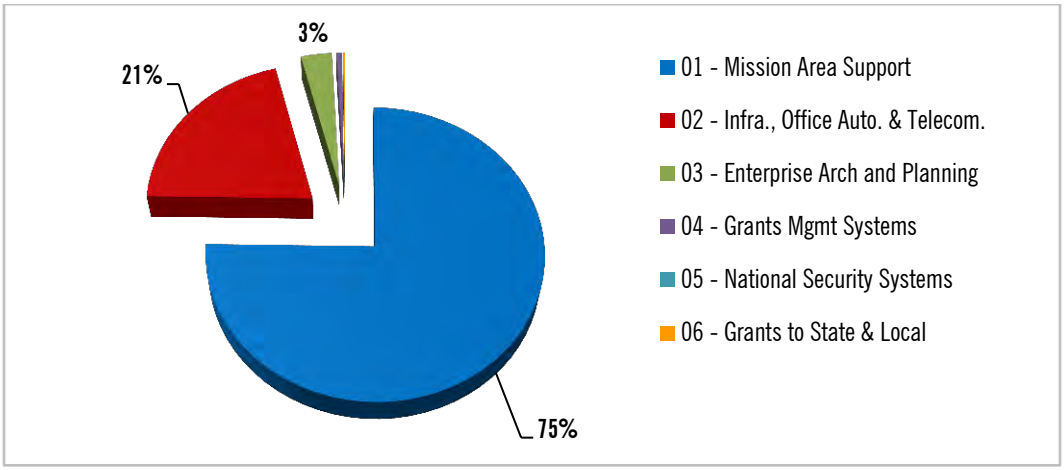


Figure C-2. ISE IT Investment Alignment to Parts of the Exhibit 53

The Exhibit 53 reporting allowed for an examination and analysis of federal IT spending alignment to the ISE priority areas focused around the primary lines of business (LOB) within the Federal Enterprise Architecture Business Reference Model (FEA BRM).

As highlighted in Figure C-3 below, the FEA BRM IT Infrastructure Maintenance LOB accounted for over one-third (35%) of IT investments. The analysis also showed significant primary mapping to other mission LOBs such as Access to Care (6%); Intelligence, Surveillance, and Reconnaissance (6%); Border and Transportation Security (6%); Criminal Investigation and Surveillance (5%); and, another health-related LOB, Health Care Delivery Services (3%). Combined, the five health-related LOBs comprised over 10% of total ISE priority-related IT spending. Healthcare IT expenditures aligned to ISE-related priorities are dominated by Health and Human Services (HHS) and the DoD and are mostly related to their efforts with electronic healthcare records systems and information systems supporting the delivery of care.

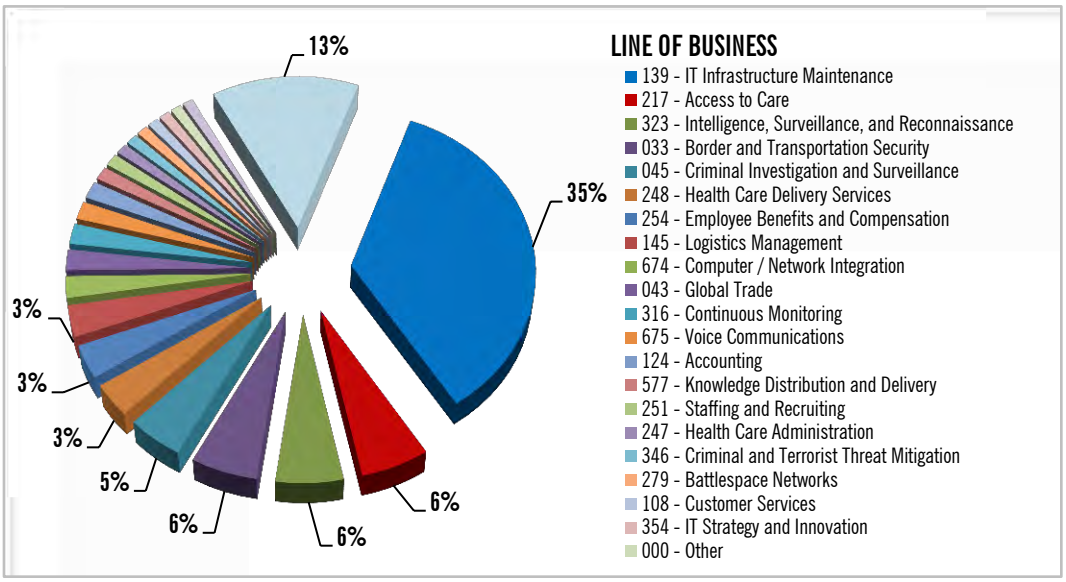


Figure C-3. ISE IT Investment Alignment – FEA Mapping

Through OMB's Exhibit 53, federal agencies continue to report on and the office of the PM-ISE conducts analysis of ISE-related IT spending. Year-to-year comparisons provide insight to data consistency, evolving priorities, and overall trends. Going forward, PM-ISE will continue to work with OMB during subsequent reporting cycles to maintain data quality and data relevancy. PM-ISE will also continue to support innovative opportunities to further responsible information sharing and safeguarding.

This page intentionally left blank.

APPENDIX D – ACRONYMS

ABAC	Attribute-Based Access Control
ACT-IAC	American Council for Technology – Industry Advisory Council
ADA	Air Domain Awareness
ADIIE	Air Domain Intelligence Integration Element
ADIS	Arrival Departure Information System
AEISS	Air Event Information Sharing Service
AFI	Analytic Framework for Intelligence
AHC	All Hazards Consortium
AKIAC	Alaska Information Analysis Center
APB	Advisory Policy Board (FBI)
ATS	Automated Targeting System
AWN	Alerts, Warnings, and Notifications
BAE	Backend Attribute Exchange
BCOT	Building Communities of Trust
BIA	Bureau of Indian Affairs
BJA	Bureau of Justice Assistance
BRIC	Boston Regional Intelligence Center
BSA	Bank Secrecy Act
BSA SAR	Bank Secrecy Act Suspicious Activity Report
CAC	Common Access Card
CBP	U.S. Customs and Border Protection (DHS)
CBRN	Chemical, Biological, Radiological, and Nuclear
CCD	Consular Consolidated Database
CDC	Cleared Defense Contractors or Centers for Disease Control and Prevention
CFIX	Central Florida Intelligence Exchange
CIKR	Critical Infrastructure and Key Resources
CICC	Criminal Intelligence Coordinating Council
CIO	Chief Information Officer
CIS	Citizenship and Immigration Services
CJIS	Criminal Justice Information Services (FBI)
CMS	Centers for Medicare and Medicaid Services
CNCI	Comprehensive National Cybersecurity Initiative
COC	Critical Operational Capabilities
CONOP	Concept of Operations
COP	Common Operating Picture
CPI	Crime Problem Indicator

CPSC	Consumer Product Safety Commission
CS/IA	Cybersecurity and Information Assurance
CSET	Cybersecurity Self-Evaluation Tool
CSP	Common Service Provider
CSS	Coastal Surveillance System
CT	Counterterrorism
CTAC	Commercial Targeting Analysis Center
CTAU	Cyber Threat Analysis Unit
CTCEU	Counterterrorism and Criminal Exploitation Unit (DHS ICE)
CTO	Chief Technology Officer
CTR	Currency Transaction Report
CUI	Controlled Unclassified Information
CYFS	Children, Youth, and Family Services
DAWG	Data Aggregation Working Group
DCMP	Domestic Common Maritime Picture
DEA	Drug Enforcement Administration
DECS	Defense Industrial Base (DIB) Enhanced Cybersecurity Services
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DICE	De-confliction and Information Coordination Endeavor
DISA	Defense Information Systems Agency
DIVS	Data Integration and Visualization System (FBI)
DNDO	Domestic Nuclear Detection Office
DOC	Department of Commerce
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOT	Department of Transportation
DSAC	Domestic Security Alliance Council
DSEA	Domestic Security Executive Academy
EA	Enterprise Architecture
ECS	Enhanced Cybersecurity Services
EO	Executive Order
EPA	Environmental Protection Agency
ESSA	Enhance Shared Situational Awareness
ESTA	Electronic System for Travel Authorization
FAA	Federal Aviation Administration
FACA	Federal Advisory Committee Act
FASS	Federated Attribute Sharing on the Secret Fabric

FAST	Field Analytic Support Task Force (DHS)
FBI	Federal Bureau of Investigation
FCCX	Federal Cloud Credential Exchange
FCPP	Fusion Center Performance Program (DHS)
FDA	Food and Drug Administration
FEAF	Federal Enterprise Architecture Framework
FICAM	Federal Identity, Credentialing and Access Management
FIG	Field Intelligence Group
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FIWG	Federated Identity Working Group
FLO	Fusion Liaison Officer
FRAC	First Responder Authentication Credential
GAC	Global Advisory Committee
GADCOI	Global Air Domain Community of Interest
GAO	Government Accountability Office
GENC	Geopolitical Entities, Names, and Codes
GEOINT	Geospatial Intelligence
GFIPM	Global Federated Identity and Privilege Management
GIRA	Geospatial Interoperability Reference Architecture
GISAC	Georgia Information Sharing and Analysis Center
GLOBAL	The Global Justice Sharing Initiative
GML	Geospatial Markup Language
GMU	Guardian Management Unit (FBI)
GNDA	Global Nuclear Detection Architecture
GSA	General Services Administration
GWG	Geospatial Intelligence Working Group
HHS	Department of Health and Human Services
HIDTA	High Intensity Drug Trafficking Area
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HOBAS	Hostage Barricade Database System
HSDN	Homeland Secure Data Network
HSGP	Homeland Security Grant Program
HSI	Homeland Security Investigations
HSIN	Homeland Security Information Network (DHS)
HSIN-CS	Homeland Security Information Network – Critical Sectors
HSPD	Homeland Security Presidential Directive
HSTC	Human Smuggling and Trafficking Center
HVDS	High-Valued Data Set
I&A	Intelligence and Analysis (DHS)
I2F	ISE Interoperability Framework

IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System
IALEIA	International Association of Law Enforcement Intelligence Analysts
IAS	Intelligence Analyst Symposium
IATF	Integrated Analysis Task Force (DHS HITRAC)
IC	Intelligence Community
ICE	U.S. Immigration and Customs Enforcement (DHS)
IC ITE	Intelligence Community Information Technology Enterprise
IC3	Internet Crime Complaint Center
ICAM	Identity, Credential, and Access Management
IC-IRC	Intelligence Community Incident Response Center
IdAM	Identity and Access Management
iDATA	Intelligence Data Association and Tagging Application
IDEx	Indiana Data Exchange
IDW	Investigative Data Warehouse
IEPD	Information Exchange Package Documentation
IFC	Identity Federation Coordination
IFS	Intelligence Fusion System
IIR	Institute for Intergovernmental Research
IISC	Information Integration Sub-Committee
IJIS	Integrated Justice Information Systems Institute
ILD	Innocence Lost Database
IMARS	Incident Management Analysis and Reporting System (DOI)
ONDCP	Office of National Drug Control Policy
IP	National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (DHS)
IPM	Identity Protection and Management (DoD)
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISC	Investigative Support Center
ISE	Information Sharing Environmen
ISE PAQ	Information Sharing Environment Performance Assessment Questionnaire
ISO	International Standards Organization
ISSA	Information Sharing Segment Architecture
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
JABS	Joint Automated Booking System
JACCIS	Joint Analysis Center Collaborative Information System
JC3	Joint Counterterrorism Coordination Cell
JCAT	Joint Counterterrorism Assessment Team
JIOC	Joint Intelligence Operations Center

JOC	Joint Operations Center
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
LEEP	Law Enforcement Enterprise Portal
LEISP	Law Enforcement Information Sharing Program (DOJ)
LEIU	Law Enforcement Intelligence Units
LEO	Law Enforcement Online (FBI)
LEO-EP	Law Enforcement Online – Enterprise Portal
MACC	Multi-Agency Coordination Center
MISE	Maritime Information Sharing Environment
MOU	Memorandum of Understanding
MPD	Milwaukee Police Department
myFX	my File Exchange (DOJ)
NAD	North American Day
NAS	National Alert System
NBD	NIEM Biometrics Domain
NCCIC	National Cybersecurity Communications and Integration Center
NCI-JTF	National Cybersecurity Investigative Joint Task Force
NCMEC	National Center for Missing Exploited Children
NCRIC	Northern California Regional Intelligence Center
NCTC	National Counterterrorism Center
NCTC/DOS	National Counterterrorism Center Directorate of Operations Support
N-DEx	Law Enforcement National Data Exchange (FBI)
NDSLIC	North Dakota State and Local Intelligence Center
NGA	National Geospatial-Intelligence Agency
NGI	Next Generation Identification System (FBI)
NHTSA	National Highway Traffic Safety Administration
NIAC	National Infrastructure Advisory Council
NIEF	National Information Exchange Federation
NIEM	National Information Exchange Model
NIEM-M	National Information Exchange Model – Maritime
NIEM-UML	National Information Exchange Model – Unified Modeling Language
NIH	National Institutes of Health
NGIC	National Gang Intelligence Center
NIM-CT	National Intelligence Manager for Counterterrorism
NJ ISE	New Jersey Information Sharing Environment
NJ ROIC	New Jersey Regional Operations and Intelligence Center
NLE	National Level Exercise
Nlets	The International Justice and Public Safety Network
NMIO	National Maritime Intelligence-Integration Office
NORAD	North American Aerospace Defense Command

NPPD	National Protection and Programs Directorate (DHS)
NPPS	National Palm Print System (FBI)
NSA	National Security Agency
NSBAC	National Security Business Alliance Council
NSG	National System for Geospatial-Intelligence
NSI	Nationwide Suspicious Activity Reporting (SAR) Initiative
NSI PMO	Nationwide Suspicious Activity Reporting (SAR) Initiative Program Management Office
NSISS	National Strategy for Information Sharing and Safeguarding
NTOC	NSA Threat Operations Center
OBIM	Office of Biometric Identity Management (DHS)
ODNI	Office of the Director of National Intelligence
OBIM	Office of Biometric Identity Management
OGC	Open Geospatial Consortium
OGPL	Open Government Platform
OMB	Office of Management and Budget
OMG	Object Management Group
OPS	Office of Operations Coordination and Planning (DHS)
ORCON	Originator Controlled
ORION	Operational Response and Investigative Network
OSIN	Oregon State Information Network
OSSI	Office of Security and Strategic Information (HHS)
OTJ	Office of Tribal Justice (DOJ)
P/CL	Privacy and Civil Liberties
P/CR/CL	Privacy, Civil Rights, and Civil Liberties
PCLOB	Privacy and Civil Liberties Oversight Board
PCSC	Preventing and Combating Serious Crime
PDMP	Prescription Drug Monitoring Program
PITWG	Privacy and Information Technology Working Group
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification-Interoperable
PKI	Public-key Infrastructure
PM-ISE	Program Manager – Information Sharing Environment
PMIX	Prescription Drug Monitoring Program (PDMP) Information Exchange
PMO	Program Management Office
PPD	Presidential Policy Directive
RFI	Request for Information
RFP	Request for Proposal
RISC	Repository for Individuals of Special Concern
RISS	Regional Information Sharing System
RISSafe	Regional Information Sharing System's Officer Safety De-confliction System

RISSNET	Regional Information Sharing Systems Network
RMAS	Regional Movement Alert System
RMS	Records Management System
RMT	RFI Management Tool
ROIC	Regional Operations and Intelligence Center
S&T	Science and Technology
SAFENet	Secure Automated Fast Event Tracking Network
SAR	Suspicious Activity Report(ing)
SARBAR	Suspicious Activity Report Batch Analysis Review
SBU	Sensitive But Unclassified
SCC	Standards Coordinating Council
SDFC	South Dakota Fusion Center
SDO	Standards Development Organization
SEOC	State Emergency Operations Center
SEVIS	Student Exchange and Visitor Information System
SEVP	Student and Exchange Visitor Program
SIG	Special Interest Group
SIPRNET	Secret Internet Protocol Router Network
SISSC	Senior Information Sharing and Safeguarding Steering Committee
SLPO	State and Local Program Office (DHS)
SLTT	State, Local, Tribal, and Territorial
SOA	Service Oriented Architecture
SPS	Single Point of Service
SSO	Simplified Sign-On
STAC	Southeastern Wisconsin Threat Analysis Center
STIX	Structured Threat Information eXpression
SWG	Standards Working Group
TASPO	Targeting and Analysis Systems Program Office (DHS CBP)
TDDB	Technology Development and Deployment Board (FBI)
TFC	Tennessee Fusion Center
TISW	Tribal Information Sharing Working Group
TLOA	Tribal Law and Order Act
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
UCore	Universal Core (DoD)
UML	Unified Modeling Language
UMTT	Unified Message Task Team (IACP)
US-CERT	Cyber Emergency Response Team
USCG	United States Coast Guard
USNORTHCOM	United States Northern Command
USSS	United States Secret Service

VA	Department of Veterans Affairs
ViCAP	Violent Criminal Apprehension Program
VWP	Visa Waiver Program
WIS3	Workshop on Information Sharing and Safeguarding Standards
WMD	Weapons of Mass Destruction
WSIN	Western States Information Network
XML	Extensible Markup Language

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