



INFORMATION SHARING ENVIRONMENT

ANNUAL REPORT TO THE CONGRESS

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

EXECUTIVE VERSION

Prepared by the
Program Manager, Information Sharing Environment

30 June 2012



Intelligence
Group
National
centers
share
Departments
including providing report
collaboration
critical
use
public
joint
develop
implement
May
assured
existing
system
facilitate
integration
United
framework
secret
ensure
Initiative
classified
Police
share
common
reporting
providing
existing
system
facilitate
integration
United
framework

ISE.

information



INFORMATION SHARING ENVIRONMENT

ANNUAL REPORT TO THE CONGRESS

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

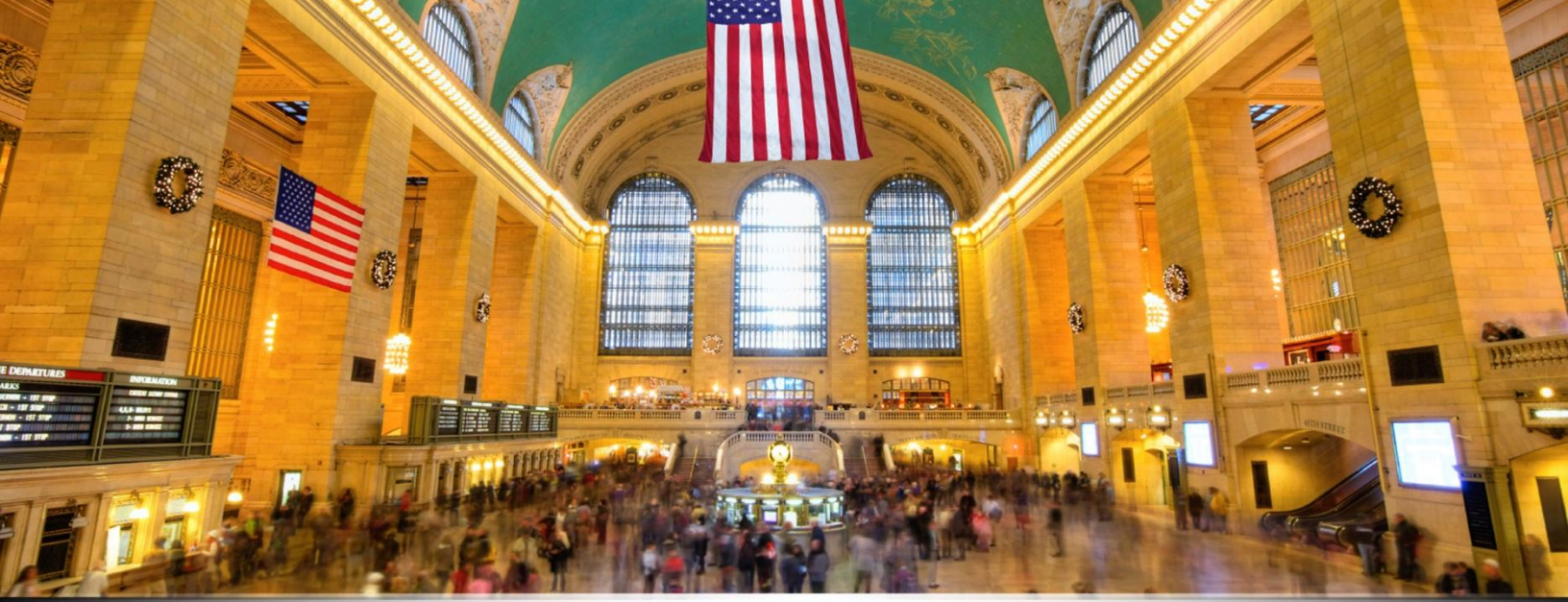
EXECUTIVE VERSION

The full report is available at www.ise.gov

Prepared by the
Program Manager, Information Sharing Environment

30 June 2012

This page intentionally left blank



FOREWORD

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

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

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

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

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

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

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

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

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

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

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



Kshemendra Paul, Program Manager, Information Sharing Environment

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



EXECUTIVE SUMMARY

The ISE is a partnership for responsible sharing of terrorism-related information between the law enforcement, public safety, defense, intelligence, homeland security, and diplomatic communities. It extends to all levels of government – federal, state, local, tribal, and territorial; and incorporates private sector partners and international allies. This Sixth Annual Report to the Congress on the state of the Information Sharing Environment (ISE) examines the extent to which the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) terrorism information sharing mandate is being implemented by agencies that possess or use information about terrorism, operate a system in the ISE, or participate in the ISE.³ This Report, which PM-ISE is submitting on behalf of the President,¹ incorporates input from our mission partners⁴ and uses their initiatives and PM-ISE's management activities to provide a cohesive narrative on the state and progress of terrorism-related responsible information sharing,⁵ including its impact on our collective ability to secure the nation and our national interests.

This Report describes how agencies have fared against established performance measures and highlights accomplishments, including illustrative examples of ISE progress toward the responsible information sharing goals derived from IRTPA, presidential guidelines in support of the ISE⁶, and the National Strategy for Information Sharing. It covers PM-ISE's reporting responsibilities pertaining to the Interagency Threat Assessment and Coordination Group (ITACG).⁷ PM-ISE also supports aspects of information sharing in other domains, such as maritime, primarily to promote cross-domain information integration in the pursuit of strengthening national security through responsible information sharing.

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

³ Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, P.L. 108-458 (December 17, 2004), Sec. 1016(h) and (i).

⁴ IRTPA Section 1016 (i)(4).

⁵ As defined in Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, P.L. 108-458 (December 17, 2004), Sec. 1016(a)(5).

⁶ White House Memorandum for the Heads of Executive Departments and Agencies, Guidelines and Requirements in Support of the Information Sharing Environment (December 16, 2005).

⁷ Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, sec. 210D(c), codified as amended at 6 U.S.C. 124k(c).

ORGANIZATION

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

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

MATURING INFORMATION SHARING ACROSS THE ISE

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

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

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

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

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

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

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

OPTIMIZING MISSION EFFECTIVENESS

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

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

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

STANDARDS DEVELOPMENT AND IMPLEMENTATION

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

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

STRENGTHENING SAFEGUARDING TO SUPPORT RESPONSIBLE INFORMATION SHARING

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

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

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

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

IMPLEMENTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTIONS

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

MANAGING AND FOSTERING A CULTURE OF RESPONSIBLE INFORMATION SHARING

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

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

HOW THE 2012 REPORT DIFFERS FROM PAST REPORTS

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

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

PM-ISE’S CONTRIBUTIONS OVER THE LAST YEAR

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

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

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

TOOLS OF THE PM-ISE

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

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

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

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

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

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

- Served on the National Security Staff's (NSS) post-WikiLeaks Structural Reforms IPC and helped draft E.O. 13587 to improve the sharing and safeguarding of classified information and systems;
- Established the Classified Information Sharing and Safeguarding Office (CISSO) in concert with E.O. 13587 structural reforms, affirming PM-ISE's cross-cutting leadership role in both information sharing and safeguarding;
- On behalf of the Senior Information Sharing and Safeguarding Steering Committee, led the development of the 90-day Report to the President on the status of information sharing and safeguarding of classified information on computer networks;
- Issued ISE Implementation Guidance that provides more specific direction for agency activities in order to achieve the priorities defined in joint Office of Management and Budget (OMB) and NSS programmatic guidance, and serve as the basis for objective system-wide performance goals for the following year;
- Hosted an international training event to help implement NIEM-conformant exchanges for North American pilots for public health and public safety information sharing;
- Partnered with Canadian government representatives to discuss NIEM adoption for Canada's law enforcement and public safety communities;
- Created a set of illustrative, mission-based scenarios to translate White House strategic goals and initiatives into mission-specific narratives, to assist agencies in planning for and executing goal-based initiatives;
- Supported, with DHS, the Centers of Analytical Excellence Workshop to identify fusion centers that have developed expertise in topical areas, and to benefit the National Network of Fusion Centers; and
- Partnered with the NSI PMO and relevant professional organizations to develop the Hometown Partners training materials aimed at 911 operators, fire and emergency medical service personnel, emergency management personnel, private sector security personnel, and probation, parole, and corrections personnel.

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

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

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

MEETING THE LEGAL REQUIREMENTS FOR ISE PERFORMANCE MANAGEMENT REPORTS

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

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

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

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

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

⁸ See Appendix A for more detail.

⁹ Implementation Guidance for FY 2013 Programmatic Guidance for the Information Sharing Environment (ISE), PM-ISE memo dated August 8, 2011.

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

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

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

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

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

OTHER GAPS, CHALLENGES, AND OPPORTUNITIES

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

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

- Opportunity with Cybersecurity Information Sharing
 - **Finding:** *Given the increasing frequency, impact, and sophistication of attacks on information and information systems in the United States, cybersecurity is a national security priority. Cybersecurity can be improved if agencies more effectively share cyber-vulnerability and intrusion incident information. The application of the ISE's proven information sharing techniques and processes to the cyber information sharing problem set can enable this. As new legislation emerges in this area, information sharing related to cybersecurity functions will play an increasingly important role in the ISE.*
- Opportunity to Strengthen Collaboration and Coordination Between Federal, State, Local, Tribal, and Private Sector Entities
 - **Finding:** *To further accomplish the goals of the ISE as stated in IRTPA and Presidential Guidelines,¹⁰ PM-ISE and its mission partners are exploring new mechanisms for enhancing collaboration and coordination between federal, state, local, tribal, and private sector entities. Although significant information sharing relationships have been institutionalized between these organizations, it is anticipated that a dedicated forum is needed to fully bring the accountability, oversight, and governance capabilities of the ISE to bear on lingering information sharing gaps between federal agencies and non-federal partners by enhancing understanding of one another's missions, the respective policy and legal hurdles each faces, and the benefits each will realize through senior-level interaction.*

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



WAY FORWARD

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

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

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

Leadership from federal, state, local, tribal and private sector organizations with operational, investigative, and/or analytic missions have a voice through the ISA IPC working group and sub-committee governance processes to propose improvements to information sharing.¹¹ Through this collective engagement and leadership commitment from the White House, PM-ISE, agencies, and other ISE stakeholders, we collectively accelerate responsible information sharing to strengthen our Nation's security.

¹¹ IRTPA Sec 1016(b)(2)(C).

MANAGING IMPLEMENTATION OF RESPONSIBLE INFORMATION SHARING

PM-ISE’s capability-focused Implementation Guidance provides the basis for an objective, system-wide set of performance goals for the following year as required by the IRTPA.¹² Annually, in collaboration with the ISA IPC, PM-ISE issues Implementation Guidance that is sequentially derived from, and reinforces, White House programmatic guidance. The Implementation Guidance contains actions assigned to specific federal agencies, with milestones and timeframes that align programs, systems, and initiatives with requirements to improve responsible information sharing. Annual performance assessments against these actions are included in PM-ISE’s Annual Report to Congress, providing accountability and progress over time, and enabling leadership to make informed program and budget decisions in subsequent years. Overall, the annual planning cycle moves agencies closer to the target vision of responsible information sharing. The annual planning cycle is depicted in Figure 3.

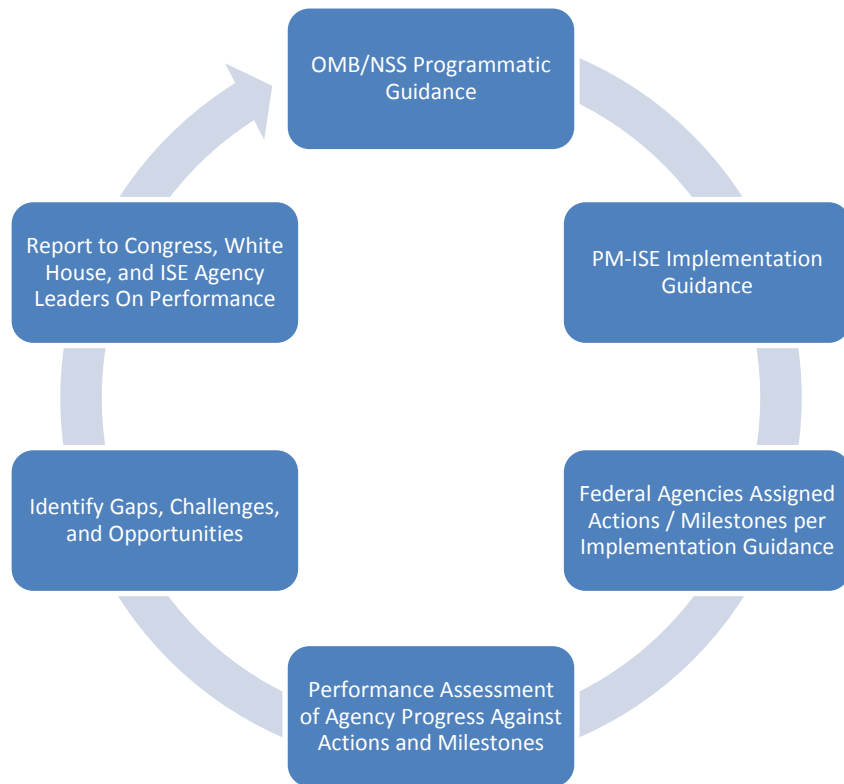


Figure 3. Annual Planning Cycle

IMPLEMENTATION ROADMAP

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

¹² IRTPA Sec 1016 (h)(2)(B).

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

PM-ISE'S VISION, MISSION, AND OBJECTIVES

“PM-ISE is working hard at embracing common operating models and shared services - that implies greater integration horizontally across community stovepipes, as well as vertically – from federal, state, local, tribal and private sector partners, and our allies.”

- DNI Clapper, 26 January 2012, Center for Strategic and International Studies Forum on Information Sharing

While the White House provides a strategy for information sharing and safeguarding, and agencies are largely responsible for implementing specific actions based on White House and PM-ISE guidance, PM-ISE has updated the vision and mission for responsible information sharing in order to continue to advance the ISE consistent with existing legal authorities and Executive Orders.¹³ PM-ISE’s updated vision and mission are shown below:

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

PM-ISE’s Mission:

- I. Advance responsible information sharing to further counterterrorism and homeland security missions
- II. Improve nationwide decision making by transforming from information ownership to information stewardship
- III. Promote partnerships across federal, state, local, and tribal governments, the private sector, and internationally

DELIVERING CAPABILITIES

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

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

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

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

¹³ Pursuant to IRTPA Section 1016; EO 13388; and EO 13587.

At its core, **establishing trusted interoperable networks** to efficiently and effectively share and safeguard controlled unclassified information across government networks serves to fully protect the privacy, civil rights, and civil liberties of individuals, and **to facilitate the discoverability and accessibility of information by individuals and organizations at the local, state, tribal, and federal levels of government who are responsible for decision making** to prevent harm against the United States and its people. This objective is illustrated in mission-based test Scenario #5 – Enabling Deconfliction to Promote Officer Safety – which deals with improving the mechanisms to perform case and event deconfliction in the public safety arena to improve mission effectiveness and officer safety.¹⁴

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

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

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

PM-ISE supports the Steering Committee for Information Sharing and Safeguarding and ISA IPC to refine and crystallize policy decision points, clarify potentially competing priorities to ease resource competition, streamline governance, and improve accountability. This improved, results-oriented, Executive-level support **enables transformation of domestic information sharing architecture and the capability to make sense of the vast stores of information made available through its transformation; it prioritizes interoperability, standards-based acquisition, and information-access management standards, while at the same time protecting P/CR/CL**. It looks beyond the Federal Government and encourages a cultural change of governance throughout other echelons of government—state, local and tribal—as well as throughout the private sector. Scenario #7, which deals with modernizations to the SAR process in the CIKR domain, highlights work in the ISE corresponding to this objective.¹⁵

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

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

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

¹⁴ See Appendix B: Scenario 5 – Enabling Deconfliction to Promote Officer Safety.

¹⁵ Appendix B: Scenario 7 – Using SARs to Detect CIKR Threats.

approach and aligning acquisition requirements across the ISE community: ***facilitates identification and leverages existing capabilities; creates broader awareness and understanding of initiatives; maximizes purchasing power when acquiring new products or services; decreases risk while integrating common solutions; promotes standardization of agency-level services as they align across the enterprise; and enables accountability in purchasing decisions.*** In sum, an open development approach and standards-based acquisition not only saves taxpayer dollars, but it can also drive the development of more open industry-wide standards and technologies, and have a broader impact on national economic development. Standards-based acquisition not only enhances efficiency, it enhances operational effectiveness as seen in Scenario #4, where work towards modernizing the acquisition process shows concrete improvement in the government's ability to procure effective information sharing mission systems.¹⁶

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

A federation of interconnected networks represents the strongest, most efficient architecture for mission support. PM-ISE promotes strong policies and practices for identity, credential, and access management, implemented at a granular level using common standards to ensure interoperability. ***Common data-level standards provide for improved information security through shared audit and cyber-threat information on interconnected networks, improved information discoverability, and improved information sharing.*** Consistently-applied policies and practices for tagging people and information form the foundation for securely sharing information across the broadest community of federal, state, local, tribal, private sector and international mission partners. Consistent tagging also makes it possible to increase protections for privacy, civil rights, and civil liberties, even as sharing of information increases. Finally, consistent tagging and standards promote efficiency through standards-based acquisition, shared services, and re-use. Progress towards improving the ISE's capabilities in this area can be seen in Scenario #3, which deals with federated search and discovery over interconnected networks to improve the ability of investigators to accomplish their missions.¹⁷

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

While implementation of common standards, policies, and practices promotes information sharing efficiencies through re-use of best practices and capabilities across federal, state, local, tribal, public sector, and international communities of action, the ISA IPC will promote the development of ***re-usable standards and practices that ensure protections for privacy, civil rights, and civil liberties.*** Common processes, such as a model for developing information sharing agreements, ***enable mission partners to reduce the amount of time needed to build sharing agreements and focus more attention on sharing information with the appropriate users in a timely and trusted manner.*** As federal, state, local, tribal, and private sector communities leverage common standards, the ability to increasingly streamline processes may be realized at some point in the future through technology, where audit and control mechanisms govern the enforcement of privacy, civil rights, and civil liberties protections. An example of the ISE's path forward in this area is shown through one of the mission-based scenarios, which deals with improving role-based access to SAR information based on repeatable standards and practices for sharing and policy automation.¹⁸

¹⁶ Appendix B: Scenario 4 – Accelerating Federal Acquisition.

¹⁷ Appendix B: Scenario 3 – Improving Secure Access through Federated Search.

¹⁸ Appendix B: Scenario 1 – Improving Role-Based Access to SAR Information.

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

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

Through the ISA IPC, PM-ISE will incentivize responsible information sharing through in-place governance processes by promoting the *sourcing of best-practices innovation and expanded re-use of existing information sharing tools and technologies that optimize information sharing across federal, state, local, tribal, and public sector domains*. Additionally, in coordination with federal agencies, PM-ISE will ensure an optimized and properly aligned governance structure that enables information sharing goals, objectives, and strengthened partnerships with international partners. This is demonstrated in one of the mission-based scenarios, where efforts to improve the international sharing of gang-related and terrorism-related information are highlighted.¹⁹

Objective: Encourage cultural change through communities of action

PM-ISE, along with the NSS, through the ISA IPC governance processes, promotes ISE implementation actions that foster change toward a culture of greater information sharing across federal, state, local, tribal, public sector, and international boundaries. *Developing the instinctive desire to share terrorism, homeland security, and weapons of mass destruction-related information* between communities of action within federal, state, local, tribal, private sector, and international partners *provides for improved fidelity of information on which decision makers rely*. Transforming the domestic information sharing architecture with capabilities that make sense of vast amounts of information originating from the federal, state, local, tribal, and private sector inherently encourages a culture of change toward greater information sharing, which is shown in our scenarios, where cross-governmental insider threat information sharing demonstrates a cultural shift in how the government does business.²⁰

¹⁹ Appendix B: Scenario 8 – Globalizing NIEM to Enable International Sharing.

²⁰ Appendix B: Scenario 6 – Incentivizing Insider Threat Information Sharing.

ENDNOTES

ⁱ IRTPA Sec. 1016 (h)(1), (h)(2)(A)

ⁱⁱ IRTPA Sec. 1016(h)(2)(I)

ⁱⁱⁱ IRTPA Sec. 1016(h)(2)(I)

^{iv} IRTPA Sec. 1016(h)(2)(J)

^v IRTPA Sec. 1016(h)(2)(G)

^{vi} IRTPA Sec. 1016(h)(2)(F)

^{vii} IRPTA Sec. 1016(h)(2)(B) and (f)(2)(A)(3)



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](mailto:ise.gov@email) 

Intelligence
National
Information
Sharing
Environment
collaboration
system
centers
departments
report
including
providing
framework