



INFORMATION SHARING ENVIRONMENT
ANNUAL REPORT
TO THE CONGRESS



Prepared by the
Program Manager, Information Sharing Environment

September 2015

“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 on the street.”

— President Barack Obama in his forward to the 2012 National Strategy for Information Sharing and Safeguarding (NSISS)

The terrorism-related Information Sharing Environment (ISE) is a critical initiative to strengthen responsible information sharing across communities, agencies, and levels of government to implement goals set forth by President Obama in the [2012 NSISS](#). This report details the three core lines of effort—pursuing implementation of the NSISS; advancing the domestic ISE architecture; and enhancing the core ISE information interoperability frameworks, standards, and architectures—and identifies opportunities to enhance the ISE.

Federal, state, and local departments and agencies are maturing the ISE across the domestic information sharing and safeguarding architecture while maintaining strong protections for [privacy, civil rights, and civil liberties](#). The vast majority of our Nation’s front line officers, investigators, and analysts, to include approximately 800,000 sworn law enforcement officers, reside with state and local partners. Knitting them all together—federal, state, local, tribal, territorial—into a coherent, coordinated, and ever more effective distributed and decentralized architecture is the Program Manager, Information Sharing Environment’s (PM-ISE) focus. In the past year, PM-ISE has led partner-based delivery of capabilities that successfully align three epochs and 40 plus years of criminal intelligence and law enforcement information sharing: [Regional Information Sharing System](#) (RISS) centers set up in the 1970s with an initial focus on regional organized crime; [High Intensity Drug Trafficking Areas](#) (HIDTA) program created by the Congress with the Anti-Drug Abuse Act of 1988; and [Fusion Centers](#) that arose as an organic state and local response after 9/11. Major accomplishments over the past year are highlighted in Appendix A.

~18,000 federal, state, local, tribal, and territorial law enforcement agencies

9,005 law enforcement and criminal justice agencies are RISS affiliates

2,037 agencies participate in the HIDTA program

40,187 agency and private sector liaisons across the National Network of Fusion Centers

States are demonstrating independent commitment toward advancing the ISE across a growing number of mission areas, and further developing state-wide ISEs as the building blocks for a National ISE. This provides a distributed, decentralized, and coordinated approach to scale the ISE, to reduce fragmentation, and to plan for and oversee the implementation of, and manage, the ISE. The threat and use of technology by threat actors, and the use of technology by agencies is evolving. The broader societal context for this evolution is diffuse and dynamic. Much remains to be done.

Three Lines of Effort

ISE maintains three core lines of effort, each anchored with partners as depicted in Appendix B.

First, ISE partners are pursuing implementation of the NSISS. The [Strategic Implementation Plan \(SIP\)](#)—the government-wide roadmap to implementing NSISS—guides these efforts. PM-ISE expects to close out the SIP as a tracking mechanism in 2016 with substantial completion of remaining milestones and efforts across partner agencies.

Last year’s [annual report to the Congress](#) noted that the department and agency progress toward implementing the NSISS was uneven. As a result, the Office of the Program Manager encouraged federal, state, and local programs within agencies to address their information sharing challenges using ISE tools, management processes, and initiatives. Targeted Communities of Interest (COIs), addressed in the 2014 report, were formed to improve information sharing domestically in the nexus of national security and public safety.

ABOUT THE ISE

This report is submitted on behalf of the President about the state of the Information Sharing Environment (ISE). It is prepared in accordance with the Intelligence Reform and Terrorism Prevention Act (IRTPA) 2004, as amended. IRTPA 2004 (§ 1016) established an ISE for counterterrorism, weapons of mass destruction, and homeland security information.

Over the past 10 years, the ISE has standardized terrorism-related information sharing practices, strengthened the Nation’s Fusion Center network, established effective privacy policies, created a system for suspicious activity reporting, and much more. Learn more about the policy history and accomplishments of the ISE at [ise.gov](#).

Transition to the COI approach is largely complete. This shift is aimed at aligning agency participation in the development of the ISE through specific benefits to their missions. Participating programs realize improved outcomes and additionally demonstrate the value in information sharing and safeguarding for peer programs within agencies. The result is a direct pathway to scaling the ISE through emerging agency-based ISEs. Resulting information sharing is reflected in the progress described above, momentum for completion in 2016, and further described at [www.ise.gov](#).

Second, because ISE partners, under their own authorities, leverage and reuse their ISE investments broadly across their mission sets, the ISE’s mission impact continues to enhance national security and public safety. Noteworthy is the shared role in supporting [state and local](#) stakeholders to interoperate with each other, the [private sector](#), and federal agencies; to develop, implement, and align information sharing platforms; and to contribute to federal policy conversations. The forum for this work is the [Criminal Intelligence Coordinating Council \(CICC\)](#).

Through CICC, the [Global Justice Information Sharing Initiative \(Global\)](#), and other forums, PM-ISE is leveraging ISE capabilities to support partners in their efforts to align field-based intelligence

and information sharing capabilities. ISE partners across federal, [state, local, tribal](#), and territorial agencies collaborated on the development of the [2015 National Heroin Threat Assessment](#)—a comprehensive strategic assessment of the many facets of the heroin threat impacting communities across the United States.

ISE partners have also worked to align the Nation’s sensitive but unclassified (SBU) networks. These networks—the [Homeland Security Information Network](#), [Regional Information Sharing Systems](#), [Law Enforcement Enterprise Portal](#), and [Intelink](#)—are now interoperable, providing an array of services and information through a simplified sign-on using existing credentials by over [400,000 registered users](#). These efforts are realizing the ISE through interoperable, secure collaboration and are resulting in the construction of a national information sharing platform.

ISE partners are working to increase effective [information sharing and deconfliction of cyber-related information](#), leveraging existing agency-based [deconfliction](#) capabilities across their organizations. As [cyber](#) operations increase, there is an amplified need for shared information across institutions and domains. ISE partner agencies are working through their authorities and investments to recommend applicable policies and connect users with essential tools. One such tool is the [Cyber Integration for Fusion Centers](#), an appendix to Global’s [“Baseline Capabilities for State and Major Urban Area Fusion Centers,”](#) which provides fusion centers with a road map for building cyber capability. The priority remains to coordinate the efforts of national and homeland security agencies with law enforcement and intelligence resources at all levels of government.

Additionally, ISE partners are collaborating in the [maritime domain](#) to identify challenges and enhance information sharing that could impact the security, safety, economy, or environment of the Nation. As a premier example of a maturing community of interest, the [Maritime Operational Information Sharing Analysis project](#) is an examination of current practices and information sharing challenges facing the Puget Sound community. The analysis will contribute to more efficient use of resources and increased effectiveness of ongoing national,

ADVANCING THE DOMESTIC ARCHITECTURE

The [2014–2017 National Strategy for the National Network of Fusion Centers](#) (NNFC)—a primary outcome of the 2013 “Majority Staff Report on the National Network of Fusion Centers”—builds a framework for initiatives aimed to improve interdisciplinary, cross-jurisdictional sharing of information to effectively implement strategies in information-driven and risk-based major crime and terrorism prevention, protection, response, and recovery. ISE agencies support most of the 37 NNFC initiatives, working in coordination to leverage information sharing capabilities. Some examples of work supporting these initiatives include:

1. Formation of a National Fusion Center Association (NFCA) Social Media Working Group to collaborate on the development of policies, processes, methodologies, training, and a de-confliction platform to support analysis of open source social media for terrorism-related and other threats to officers, uniformed military, and public safety
2. Initial development of a Northeastern Regional Intelligence Group coordination plan to enhance coordination between fusion centers, RISS centers, HIDTAs, field intelligence groups, and law enforcement criminal intelligence units
3. Support implementation of statewide ISEs, which provide secure access to appropriate systems and enhance the responsible flow of information in support of statewide law enforcement, homeland security, and emergency management missions
4. Development of a fusion center cyber strategy that incorporates state, local, tribal, and federal partners to address how cyber-related crimes and threats will be addressed within the center’s AOR
5. Enhanced information sharing among law enforcement officers in the field, fusion centers, and the Terrorist Screening Center to enhance analysis and to strengthen the understanding and awareness of the current threat environment

regional, and local efforts aimed at improving maritime security, safety, and economic resiliency. It will also guide and align future investments and inform key decisions. Finally, it will help the maritime COI develop the best pathways to scaling the ISE in their distributed and decentralized domain.

In the coming year, the ISE will further strengthen efforts to increase alignment across the domestic architecture. This work will add to efforts to align and leverage [SBU networks](#); increase momentum with field-based intelligence and information sharing entities; foster interoperability with first responders and other partners, including FirstNet and NextGen 911; and support state and local agencies in their efforts to establish state-wide and regional ISEs that are locally driven but plug into the national ISE architecture. This work builds upon comprehensive policies that protect privacy, civil rights, and civil liberties. Aligning the domestic architecture based on coordinated approaches, aligned policies, procedures, guidance, and local control is the key ISE frontier.

Third, the ISE is enhancing and advancing the core frameworks developed, refined, and tested through more than a decade of terrorism-related information sharing. The focal point for this line of work is [Project Interoperability](#), which distills, advances, and packages for easier use core ISE information interoperability frameworks, standards, and architectures. Examples include previously noted progress with [data standards](#) and semantic interoperability leveraging the [National Information Exchange Model](#) and efforts sponsored under the [National Strategy for Trusted Identities in Cyberspace](#), the [Federal Chief Information Officers Council](#), and the [National Association State CIOs](#) to advance modern multi-factor identity authentication and attribute-based access control.

These efforts are coordinated via the [Standards Coordinating Council](#) (SCC), an advisory group that is aligning these frameworks with the mainstream of international voluntary consensus standards and best practices. Standards-based and shared approaches are an absolute requirement given that the vast majority of targeted agencies are small and lack capacity to participate in the ISE any other way. For example, 90% of the approximate 18,000 law enforcement agencies in the Nation have 50 or fewer sworn officers. PM-ISE sees its goal of aligning public and private efforts as the best and only sustainable way to scale adoption and use of Project Interoperability as key support for scaling the ISE, and expects to see clear, credible, and transparent evidence of Project Interoperability in the [domestic architecture](#) efforts described above, augmented by other [domain awareness](#) and terrorism-related efforts.

Opportunities and the Way Forward

Responsible information sharing is a journey, not a destination. Requirements for responsible information sharing evolve in response to evolution of the threat landscape; to continually evolving public opinion, including those driven by the immediate and unstructured availability of information via social media; to societal context; and, to the progressions of technology in the commercial and government sectors. As mission requirements evolve, ISE partners enhance capabilities.

The 9/11 commission report states, “The U.S. government has access to a vast amount of information. But it has a weak system for processing and using what it has ... no agency can solve the problems on its own-to build the network requires an effort that transcends old divides”

Scaling of the ISE is the response to this finding, enabling cross boundary information sharing and safeguarding. However, there are constant challenges in utilizing technologies and assuring the appropriate use of vast amounts of information, further complicated by competing priorities for limited resources and the acceleration of change across the tens of thousands of public and private constituencies. Efforts to align agency-based policies and management processes across myriad stakeholders are continuous and evolving.

During the last decade, as has been discussed in [prior annual reports](#) to the Congress, the Nation's capabilities to share information have matured. The ISE has demonstrated the power of responsible information sharing through specific programmatic outcomes across jurisdictional boundaries and disciplines, and with [international partners](#) on transnational initiatives—efforts causally linked to the collective work to advance the ISE as depicted in Appendix C. Furthermore, the lessons learned throughout the government through the maturation of the ISE extend beyond terrorism-related issues to the sharing of information more broadly to enhance national security and safety, such as opioid threats, [human trafficking](#), and violent extremism.

Still, the U.S. Government Accountability Office (GAO) maintains government-wide terrorism-related information sharing (development of the ISE) on its [High Risk List](#) (HRL). GAO's criteria in this regard focuses on governance, strategy, policy, supporting enterprise architecture and related technical frameworks, management processes, and performance outcomes. The [GAO's 2015 report](#) noted sustained and substantial Executive Branch progress. The ISE's lines of effort address GAO's recommendations. Next year, the ISE expects to report substantial implementation of the 2012 NSISS SIP, demonstrate scaling of Project Interoperability, and highlight continued government-wide program outcomes causally linked to these efforts.

Targeted outcomes will address GAO's recommendations. Progress is setting the groundwork for agency leadership—federal, state, and local—to make effective and independent calculations and support scaling the ISE. Adoption by departments and agencies, under their own authorities to integrate effective government-wide responsible information sharing, is the required critical support for scaling the ISE. The result will be creation of a self-sustaining cycle of responsible information sharing to protect the American people and enhance national security.

PM-ISE continues to plan, oversee, and manage the implementation of the ISE as envisioned by the Congress in IRTPA. The attributes of the ISE are about broad [responsible information sharing](#) aspirations. There is wide interest and adoption with Project Interoperability, creating options for policy makers by lessening friction, reducing cost, and speeding agility around horizontal and inter-governmental collaboration. The ISE has made significant progress executing policy guidance, aligning the domestic architecture, and advancing information interoperability frameworks. The stage is set for scaling and sustained maturation of the ISE as partners continue to respond to a constantly changing threat environment.

Appendix A



ISE. FY15 MILESTONES

September	<ul style="list-style-type: none"> ● Puget Sound Maritime Domain Awareness Implementing Project Interoperability and increasing maritime security through common standards. 	
October	<ul style="list-style-type: none"> ● Launch of the Common Profile Interagency group published the Common Profile to standardize the way an information interoperability profile is documented with the ISE Information Interoperability Framework (I2F). 	
November	<ul style="list-style-type: none"> ● Sensitive But Unclassified Interoperability The release of single sign on (SSO) and federated search capability between RISS, HSIN, Intelink, and LEO—all Sensitive but Unclassified (SBU) networks. 	
December	<ul style="list-style-type: none"> ● New Jersey's Real Crime Center Launched The State of New Jersey, in conjunction with the New Jersey ISE, launches a real-time crime center. 	
January	<ul style="list-style-type: none"> ● Data Aggregation Reference Architecture Office launches the Data Aggregation Reference Architecture and publishes interagency document on www.ise.gov. 	
February	<ul style="list-style-type: none"> ● ASCIA Human Trafficking Summit PM-ISE coordinated a meeting of the Association of State Criminal Investigative Agencies (ASCIA) to discuss fighting human trafficking through information sharing. 	
February	<ul style="list-style-type: none"> ● Release of ICAM Summit Final Report ISE partners released a formal report about the FirstNet ICAM Summit. 	
March	<ul style="list-style-type: none"> ● Standards Coordinating Council Hosted WIS3 Conference Government and industry leaders came together to discuss the future for architecture and standards frameworks for the national information sharing environment. 	
April	<ul style="list-style-type: none"> ● ISE Celebrated 10th Anniversary The office looked back at a decade of progress in information sharing. 	
April	<ul style="list-style-type: none"> ● NIEM Turned 10 The National Information Exchange Model (NIEM), a key ISE partner, celebrated 10 years since its charter. 	
May	<ul style="list-style-type: none"> ● Nationwide Event Deconfliction System Law enforcement partners launched the Partner Deconfliction Interface (PDI) to deconflict events across three separate information systems. 	
June	<ul style="list-style-type: none"> ● Launch of Geospatial Framework The office published the Geospatial Interoperability Reference Architecture (GIRA) to aid government with sharing mapping and other geospatial data. 	
July	<ul style="list-style-type: none"> ● Common Profile Used by Maritime and Geospatial Sectors A key part of Project Interoperability, the Common Profile has worked as a stand-alone document to improve technical governance in interagency working groups across government. 	

WWW.ISE.GOV

Appendix C



ISE

— BY THE NUMBERS —

17

Total members of the Standards Coordinating Council (SCC)

4,800

Suspicious Activity Reports (SAR's) filed in the last year

522

Intersystem conflicts prevented by the law enforcement Partner Deconfliction Interface

23

States represented at the 2015 NGA Summit on State Cyber Security

400,000

Registered users of SBU networks who can now access federated search

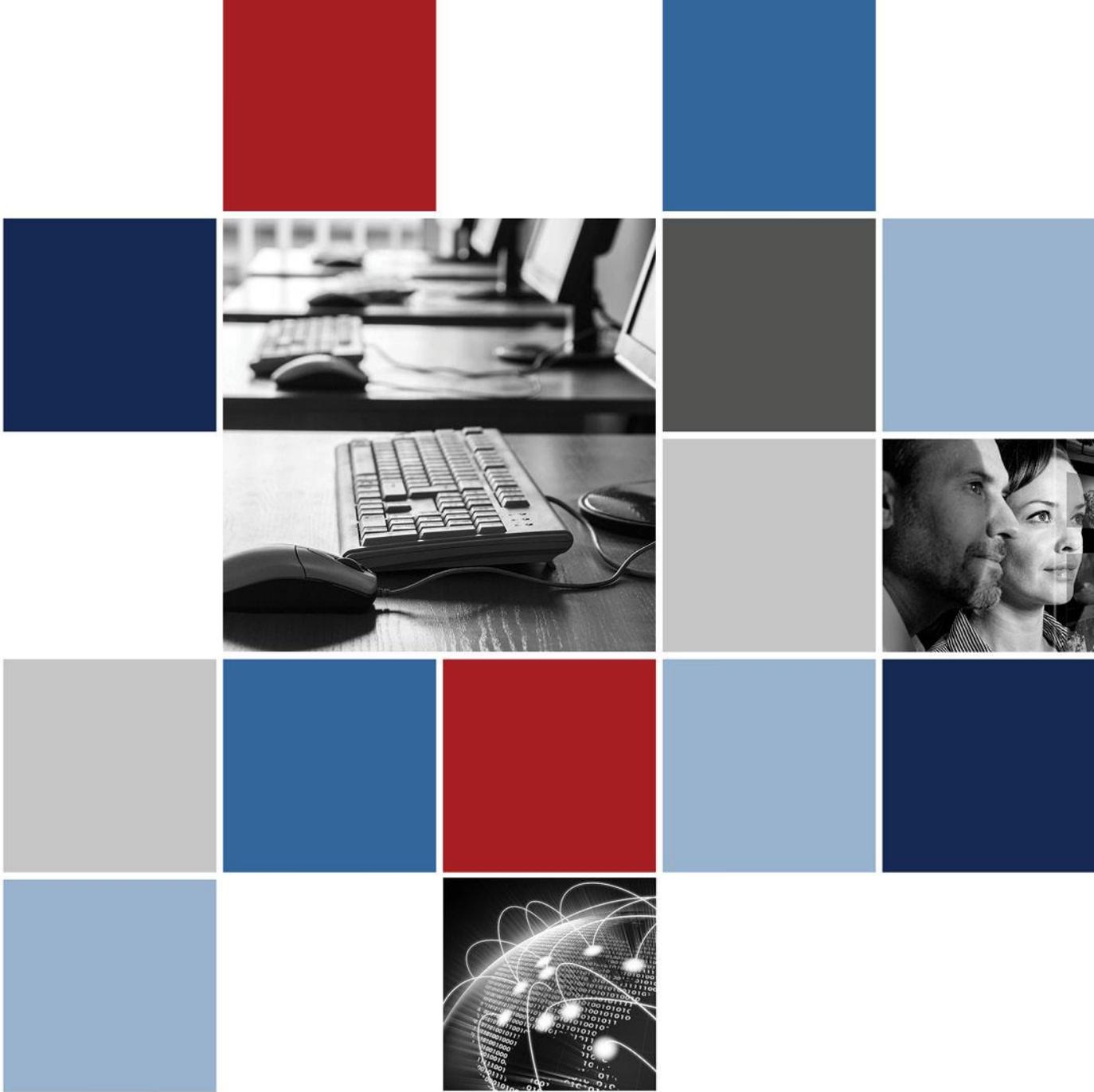
21 of 37

Initiatives supported by ISE from the NFCA National Strategy

19

States represented at the 2015 ASCIA Human Trafficking Summit





Program Manager, Information Sharing Environment
Washington, D.C. 20511

202.331.2490

www.ise.gov