INFORMATION SHARING ENVIRONMENT

ANNUAL REPORT TO THE CONGRESS

Prepared by the

Program Manager, Information Sharing Environment

August 2016

YEAR IN REVIEW

The Federal Government continues to focus on implementing the Information Sharing Environment (ISE) guided by the core principles, goals, and objectives in Executive Order 13388,[1] "Further Strengthening the Sharing of Terrorism Information to Protect Americans," the 2007 National Strategy for Information Sharing, and reinforced by the 2012 National Strategy for Information Sharing and Safeguarding (NSISS). Implementation progresses apace along three lines of effort.

1. Advance the terrorism-related ISE at the domestic nexus of public safety and national security;
2. Develop and integrate Project Interoperability (PI) and the Information Sharing and Safeguarding Core Interoperability Framework to improve information sharing and safeguarding by ISE partners across their enterprise architectures; and
3. Support federal departments and agencies with their efforts to implement national information sharing objectives via the Strategic Implementation Plan (SIP) published in 2013.

The first line of effort—supporting ISE partners to increasingly align policy, missions, and technology with their information sharing infrastructure at the domestic nexus of national security and public safety—dates back to the inception of the ISE. Noteworthy is the shared role by federal, state, local, tribal, and territorial (FSLTT) ISE stakeholders to operate with each other, and the private sector; to develop, implement, and align information sharing platforms; and to contribute to federal policy conversations. A key forum for coordinating this work is the Criminal Intelligence Coordinating Council (CICC), with representatives from across federal, state, local, and tribal law enforcement agencies.

The second line of effort—aligning, developing, and integrating information interoperability—is advancing core frameworks and standards 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[2]. The forum for coordinating this work is the Standards Coordinating Council (SCC), an advisory group composed of industry and standards development organizations that provides recommendations on matters related to information sharing standards and other issues related to responsible information sharing.

[1] EO 13388, Presidential Guideline 2 – extends the scope of the ISE to law enforcement information related to terrorism or other crimes with a national security concern.

[2] Project Interoperability is a start-up guide for information interoperability to transfer and use information in a consistent, efficient way across organizations and information technology systems.

The third line of effort—performance evaluation—demonstrates how ISE partners are implementing the NSISS through an Administration-led process centered on the 2013 SIP—the government-wide, enterprise management roadmap for implementing the NSISS.

Domestic Nexus of National Security and Public Safety[3]

As emerging threats become more distributed and decentralized, it is essential to define a more aggressive approach to further share terrorism-related information. Accordingly, FSLTT leaders are coming together under the CICC, a committee under Department of Justice's (DOJ) Global Justice Information Sharing Initiative Advisory Committee (Global) to the Attorney General.

The CICC is made up of representatives from national law enforcement associations, with federal participation from leaders across DOJ, Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the Office of the Director of National Intelligence, and the Office of the Program Manager for the Information Sharing Environment (PM-ISE).

The CICC serves as a coordination body for efforts around core law enforcement and criminal intelligence policy and capability development, and specifically to advance the terrorism-related ISE at the domestic nexus of national security and public safety. Federal departments and agencies have responded to the threat environment and need to accelerate ISE-related capabilities through their engagement with the CICC in the past year. The outcome is a list of recommended projects with designated sponsors, all of which are designed to advance collaboration. Recommendations include:

- Further aligning field-based entities such as FBI Joint Terrorism Task Forces, fusion centers, High Intensity Drug Trafficking Areas (HIDTA), and Regional Information Sharing (RISS) Centers.

- Building capacity for state, local, tribal, and territorial agencies to improve cybersecurity and threat information sharing.

- Developing a targeted vision and a roadmap to further align and improve criminal intelligence collection, analysis, and sharing of terrorism-related information.

Separately, in the wake of the Islamic State of Iraq and Levant militants' 2014 attempt to lure three teenage girls from the Denver, Colorado, area to join their terror network, the U.S. Attorney for the District of Colorado requested assistance to implement a program that would leverage FSLTT and private sector capabilities to share information on how to implement prevention and intervention programming in order to reduce violent extremism in Colorado.

FSLTT partners, along with assistance from PM-ISE, are supporting the U.S. Attorney for the District of Colorado with a countering violent extremism (CVE) pilot project to develop an information sharing model that can be used in other regions of the United States. The pilot project is designed to leverage the capabilities between law enforcement officers, community leaders, school resource

[3] *National Strategy to Combat Transnational Organized Crime*, July 2011, p. 6: Crime-Terror-Insurgency Nexus.

officers, and social service providers to create an information sharing network and intervention model related to CVE activities.

The Denver-based pilot is one of several such efforts being coordinated with the newly formed, interagency CVE Task Force hosted by DHS with overall leadership provided by DHS and DOJ. PM-ISE's focus, in collaboration with the CICC, is to promote the leveraging of ISE capabilities by agencies, to both accelerate the Denver effort, and to provide for nationally scaling the project.

Denver-area teenagers were the target of the Islamic State of Iraq and Levant terrorist recruitment in 2014.

Frameworks and Standards

As partners move forward to implement a robust nationwide ISE, one of the greatest challenges faced in aligning the core frameworks is enabling a wide variety of information sharing and access agreements among information sharing partners.

Through a grant from the National Institute of Standards and Technology under the National Strategy for Trusted Identities in Cyberspace (NSTIC), and with support from PM-ISE, the non-profit Georgia Tech Research Institute (GTRI) has developed one potential solution to trust and identity frameworks. As part of an NSTIC-funded project, GTRI has begun to pilot a trustmark framework within the U.S. law enforcement and justice communities—specifically, within the National Identity Exchange Federation. The trustmark framework is designed to scale secure sensitive but unclassified information sharing by ensuring interoperability to verified identity credentials and by supporting attribute-based access control.

Further, PM-ISE is working to advance PI to integrate and align advances enabled by GTRI's efforts. Over a two to five year timetable, the vision is to expand PI on a wider scale across the ISE. The benefits include: maturing information sharing and safeguarding practices; working with industry and standards organizations to integrate agency enterprise architectures; and providing greater support for integrated risk management. A key deliverable by ISE partners, in collaboration with the SCC, is the Information Sharing and Safeguarding Playbook. This guide builds on the U. S. Digital Services Playbook, and provides a means to leverage ISE frameworks, best practices, resources, and capabilities.

Performance Evaluation

Over the past ten years in its biennial High-Risk List updates to each new Congress, the Government Accountability Office (GAO) has noted continued and steady progress in implementing the ISE. In their most recent February 2015 biennial High-Risk List update, GAO recognized sustained and substantial Executive Branch progress in terrorism-related information sharing.[4] Highlighted here are examples of continued ISE implementation progress and the value added to the ISE and terrorism-related information sharing by FSLTT partners.

[4] GAO High Risk Series: An Update, GAO-15-290, February 11, 2015, p. 224.

Implementing Milestones in the NSISS SIP

Departments and agencies have continued to advance NSISS goals by enabling the sharing of terrorism-related information, within the context of their efforts to support, integrate, use, and develop ISE capabilities, and through agency and community of interest efforts outside the ISE aligned with the NSISS.

The Administration has led the implementation of the NSISS with PM-ISE acting as the executive agent supporting closeout of the NSISS SIP within the scope of the terrorism-related ISE. Implementation has enabled departments and agencies to discover, retrieve, and share critical terrorism-related information, as well as further their mission requirements beyond the terrorism-related ISE, thereby driving decisions to advance national security and public safety.

Closeout of the SIP as the primary tracking mechanism is expected by the end of 2016. This closeout reflects three outcomes: the majority of initially identified milestones are complete; a smaller number have been retired as no longer relevant after consultation via inter-agency governance structures; and specific ongoing work deemed essential is being completed by mission partner agencies.

Homeland Security Information Network's National Situational Awareness Room

Amid crises or periods of heightened security, Homeland Security Information Network's (HSIN) National Situational Awareness Room capabilities are now utilized routinely. HSIN has been used during planned and unplanned events such as National Football League Super Bowl games, state inaugurations, active shooter situations, and severe weather. In the past two years, HSIN event and incident support has more than doubled, with approximately 47,000 emergency managers, law enforcement officers, intelligence analysts and other public safety officials relying on HSIN to support critical information sharing.

DHS Homeland Security Information Network (HSIN) National Situational Awareness Room

Northeast Regional Integration and Coordination Plan Project

With the continued institutionalization of the National Network of Fusion Centers, FSLTT and private sector partners are developing a plan to better understand and enhance communication and coordination requirements. Various efforts have been completed, providing a foundation for this effort, including work by the Fusion Process Technical Assistance Program and the National Fusion Center Association's mass casualty response policy. To fully address this need, PM-ISE is partnering with field-based partners, including HIDTAs, and RISS Centers, as well as other federal partners, including DHS and FBI, to develop a plan with the Northeast Regional Intelligence Group. Once the plan is assessed, it will be reviewed by appropriate partners, and distributed to other fusion center regions.

Development Completed on the Interagency ISE Core Awareness Training for Federal Personnel

In collaboration with federal and state partners, PM-ISE has successfully developed an interactive, 45-minute, online expansion and update of the ISE Core Awareness Training (CAT). This foundational course will assist agencies to fulfill the 2008 ISE-Guidance-104, “Implementation of the ISE Core Awareness Training.” The course development was a collaboration of federal and state partners managed by an interagency working group.

The completed current version of the course is designed for federal agency ISE partners and provides a broad overview of the underpinnings of the ISE, its mission partners, its impact on the Nation’s security, and includes a significantly expanded discussion on privacy, civil rights, and civil liberties protections for the ISE. The online course is supplemented by a standalone web portal with quick overviews of the many ISE mission partners. This web portal provides, for the first time, an essential quick reference tool with a practical orientation to the many partners and operational groups within the ISE.

As we move forward, PM-ISE will ensure the course is offered for implementation through federal partner agency learning management systems. PM-ISE is also exploring options for adapting the CAT for use by state, local, tribal, and territorial partners, in particular for use by training liaison officers working across the country with the state and major urban area fusion centers.

Protecting Privacy, Civil Rights, and Civil Liberties in the ISE

The protection of the privacy, civil rights, and civil liberties (P/CRCL) of individuals is a core tenet, foundational element, and enabler of the ISE. Mission partners periodically engage in outreach to P/CRCL advocates and stakeholder groups. At the federal level, fourteen federal ISE agencies have ISE privacy policies, with the Department of Defense opting to rely on the existing directives and orders in place to provide the functional equivalent of a stand-alone ISE privacy policy. Moreover, state, local, tribal, and territorial partners continue to demonstrate their commitment to protecting P/CRCL by prioritizing the development and implementation of their own privacy policies that are at least as comprehensive as the federal privacy guidelines. All fusion centers have privacy policies in place that have been reviewed by an interagency P/CRCL subcommittee. Recent highlights of ISE partner activities related to the protection of P/CRCL include:

- Issuing a framework which defines and supports a common methodology for developing information sharing and access agreements (ISAAs). The framework identifies key process steps, stakeholders, and P/CRCL issues to be considered early in the development of ISAAs; and

- Developing a host of useful P/CRCL related guidelines recommended by the CICC.

WAY FORWARD

Implementing the terrorism-related ISE is fundamentally a response to terrorism-related threats to our Nation (a response motivated by the need to improve coordination and collaboration among public sector agencies) and complements FSLTT agency-specific responses. The terrorism-related ISE brings a networked response to a networked adversary, and bridges legal, policy, programmatic, and jurisdictional stovepipes.

While the Federal Government has made significant progress to advance responsible information sharing, including substantial government-wide implementation of the 2012 NSISS priority objectives, more work remains to ensure implementation of the best mechanisms to effectively share terrorism-related information to protect the homeland.

The threat is evolving at an accelerating rate; is driven by geo-political factors and rapidly innovating technology capabilities; and is putting pressure on ISE partners. The evolving terrorist threat highlights a fundamental question—are the capabilities in place today—ISE-related and agency-specific—keeping pace with the increasingly complex threat?

A specific answer to this question is less useful than acknowledging that the role of—and balance towards—interoperable, distributed, decentralized, yet coordinated capabilities has never been more important. Across the Federal Government there has been a concerted effort to improve coordination and collaboration between FSLTT agencies at the domestic nexus of national security and public safety.

The primary goal for the coming year is to support and strengthen partners to sustain gains in collaboration across FSLTT agencies, while supporting ISE partners in their efforts to advance recommended CICC priorities in an integrated fashion. The secondary goal is to continue work with the SCC to develop and support adoption, integration, and use of PI and the Information Sharing and Safeguarding Core Interoperability Framework by agencies, standards organizations, and industry. Emphasis will be placed on re-use of ISE capabilities by ISE partners under their own authorities.

The stage is set for sustained maturation of the ISE as FSLTT partners continue to respond to a constantly changing threat environment.

Please visit the ISE website at www.ise.gov for ISE mission partner success stories, blogs, and other content that amplify this report.

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

202.331.2490

www.ise.gov