# INFORMATION SHARING ENVIRONMENT


## Annual Report to The Congress

Prepared by the
Program Manager, Information Sharing Environment

July 2010

# ISE

## Information Sharing Environment

**Annual Report to The Congress**

Prepared by the
Program Manager, Information Sharing Environment

July 2010

# FOREWORD

*Message from the Program Manager, Information Sharing Environment*

In the five years since the Congress directed the creation of the Information Sharing Environment (ISE), significant steps have been taken towards establishing a strong foundation. Important mission initiatives, such as Suspicious Activity Reporting and ISE core capabilities and enablers, such as fusion centers and the National Information Exchange Model, have produced results and show ongoing promise. The leaders and visionaries that drive these efforts are the mission owners and the frontline personnel—and they did this work while fighting an ever-evolving enemy.

The ISE is realized by the investment of mission partners—the bureaus and agencies of federal, state, and local, and tribal governments and our partners in the private sector and internationally—and made relevant through use by frontline law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel. Ultimately, the ISE is neither more nor less than the contributions of the mission partners—they are the engines that build and operate the ISE. This report reflects their accomplishments and the efforts of the terrorism and homeland security[1] information sharing and access community. It broadly inventories initiatives that, taken together, should be seen as the foundational steps of building the ISE. Information sharing and access capabilities have improved over the past year. Yet, the persistent and evolving threat of terrorism compels us to accelerate delivery of results from a more clearly defined and mission-integrated ISE.

The purpose of the ISE is to exploit the existing strengths within our federated democracy and open society: to innovate and deploy new approaches and tools to effectively share, discover, fuse, and enable timely action on terrorism-related information while protecting our privacy and civil liberties. The scope of the ISE is across federal agencies; spanning all levels of government; between the public and private sectors; and with our international partners to enhance national security and protect the American people from terrorism. The primary focus of the ISE is any mission process, anywhere, which has a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity. The scope of the ISE is best described in terms of end-to-end counterterrorism and homeland security mission processes—such as watchlisting, screening, and suspicious activity reporting—along with supporting core capabilities and enablers.

[1] Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P.L. 108-485, § 1016, 118 Stat. 3638, 3664 (2004), as amended, directs the ISE to improve the sharing of Terrorism and Homeland Security Information. The IRTPA definition of Terrorism Information encompasses all terrorism-related information "whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities," and was explicitly amended in 2007 to include Weapons of Mass Destruction Information. For brevity, these types of information are collectively referred to as "terrorism-related" information.

Mission partners rarely have the ability to segregate their activities to isolate terrorism information. Frontline law enforcement agencies, for example, are more likely to generate suspicious activity reports relating to gang or narcotic crime than crime with a terrorism nexus. Flexibility in the Nationwide Suspicious Activity Reporting Initiative is allowing local, state, tribal, and federal mission partners to capitalize on consistent training, privacy and civil liberty protections, oversight, and change management investments to consider moves toward information-led policing. Such mission partner equities must be considered to avoid deadlock or partial and ineffective solutions. The Program Manager for the ISE (PM-ISE) co-chairs the White House-based Information Sharing and Access Interagency Policy Committee, a forum that balances the ISE's core focus on terrorism and homeland security with ISE mission partners' needs to address the whole of national security-related information sharing and access challenges.

Key to progress in building the ISE, has been a relentless focus on identifying, integrating, and sharing best practices. Broad adoption of best practices raises confidence, lowers risk, and accelerates adoption, use, and reuse resulting in a strong return on investment by mission partners. In particular, the adoption of best practices has utility beyond the terrorism information sharing mission, extending both across complementary missions and into new mission areas unrelated to terrorism. With the ISE, smart management and good policy come together.

The support of mission partners is critical to the success of the ISE. They have mission responsibility and a vital leadership role for delivery, operation, and use of the ISE, and are accountable for delivering value by aligning policy, processes, and information. The role of PM-ISE is to bring ISE mission partners together to collaborate and support shared, cross-organizational solutions based on collective mission equities, to build consensus to prioritize funding and deliver on the shared vision, and to provide a collective management and governance framework to accelerate nationwide results. This is a team effort that requires maintaining engagement and persuading stakeholders to accept the wisdom and value of contributing to the build-out and use of the ISE, while addressing perceptions of risk and lack of control.

Going forward, we will continue working with mission partners and expand our aperture to address end-to-end terrorism-related mission processes across all levels of government, while tightening our focus on the technology-enabled, mission partner-based, network-centric vision of the ISE described in the Intelligence Reform and Terrorism Prevention Act of 2004. Over the next year, the following steps will build on, reinforce, and help accelerate the initiatives profiled in this report:

- Strengthen governance, engagement, and alignment across ISE stakeholders;
- Refresh the National Strategy for Information Sharing;
- Build capacity through increased emphasis on agency-based centers of excellence;
- Promote a culture of continuous improvement and innovation; and
- Clarify and deepen relationships with other government-wide organizations and leaders.

Several events this past year—the Fort Hood Shooting and the attempted bombings on Christmas Day and in Times Square—highlight challenges, successes, and gaps in our ability to effectively share and access information. Looking back to the events of September 11, 2001, we have come far in our sharing of and access to information across boundaries organizational boundaries and mission domains. Yet much remains to be done to support the frontline. Whether they are countering violent extremists overseas, protecting our borders and waterways, or patrolling the streets of American cities, the brave men and women of the frontline that fight terrorism and protect our homeland need timely, accurate, and relevant information to do their jobs effectively. We have work to do.

**Kshemendra N. Paul**

Program Manager, Information Sharing Environment

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

> To prevent acts of terrorism on American soil, we must enlist all of our intelligence, law enforcement, and homeland security capabilities. … We are improving information sharing and cooperation by linking networks to facilitate federal, state, and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate.
>
> — President Obama's National Security Strategy, May 2010

## Introduction

This Fourth Annual Report to the Congress on the Information Sharing Environment (ISE) reflects the collective accomplishments of the terrorism and homeland security[2] information sharing and access community, and highlights successful strategic partnerships between the Office of the Program Manager for the Information Sharing Environment (PM-ISE) and a host of mission partners, at all levels of government, mutually committed to making information more accessible to the men and women on the frontline who are keeping our country safe.

The scope of the ISE can be described as a collection of end-to-end mission processes and supporting core capabilities, enabled by standards, architecture, security, access, privacy protection, policy, governance, and management. End-to-end mission processes are operated by ISE mission partners and directly support frontline law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel. For more information on the scope of the ISE and the ISE business model, see the Introduction to this report.

## Spotlight on Information Sharing

A number of major events over the last year helped reinforce the importance of a robust Information Sharing Environment in keeping America safe. The failed attempt to bomb Northwest Airlines Fight 253—to cite one important example—shows the need to go beyond merely making information accessible to those who need it and shows the importance of presenting this information in ways that make the key facts stand out, i.e., that the signals are discernable through the noise. Cases like this, and the Fort Hood and Times Square incidents, show that the ISE cannot be a static environment, but must

[2] Section 1016 of IRTPA, as amended, directs the ISE to improve the sharing of Terrorism and Homeland Security Information. The IRTPA definition of Terrorism Information encompasses all terrorism-related information "whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities," and was explicitly amended in 2007 to include Weapons of Mass Destruction Information. For brevity, these types of information are collectively referred to as "terrorism-related" information.

continually adapt to the challenges posed by violent extremists. To succeed, the ISE must promote a culture of continuous improvement and innovation, routinely challenging our assumptions and implementing measurable improvement.

The President's National Security Strategy also emphasizes important ISE initiatives—including integrating and leveraging state and major urban area fusion centers; establishing a nationwide framework for reporting suspicious activity; and adopting an integrated approach to counterterrorism information systems, to ensure that the analysts, agents, and officers who protect us have access to all relevant intelligence throughout the government. As a partnership of five primary communities—Intelligence, Foreign Affairs, Homeland Security, Law Enforcement, and Defense—the ISE embraces the President's "Whole of Government" approach for strengthening national capacity. For the ISE to succeed, the predisposition to share information must be incorporated into the day-to-day activities, investments, management processes, and cultures of all participating ISE agencies and communities.

## Progress Highlights

This report describes information sharing progress in the context of: (1) key end-to-end mission processes that are the central focus of ISE development; (2) ISE core capabilities that support but cut across the individual mission processes; and (3) ISE enablers that are integral to both ISE mission processes and the core capabilities. Although the focus of this report remains on ISE initiatives that address the specific requirements set forth in the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, (IRTPA), the report also describes mission partner accomplishments, some of which may not have been developed explicitly to support counterterrorism, but which do end up supporting the counterterrorism mission in some cases or may ultimately become "best practices" with applicability to information sharing and collaboration government-wide, including the ISE.

The fact that the ISE is both driving and leveraging these achievements is consistent with one of its key attributes identified in IRTPA—to build upon existing systems capabilities currently in use across the government.

The following selected highlights demonstrate the breadth of agency-based ISE related activities.

### ISE Mission Processes

#### *Law Enforcement Information Sharing*

***Law Enforcement Information Sharing expanded significantly across all levels of government, improving our ability to use law enforcement information to detect, prevent, and respond to acts of terrorism***

Federal, state, local, and tribal law enforcement officers are major players in the efforts to combat terrorism and keep America safe. Since 9/11 law enforcement agencies at all levels of government have worked collaboratively to detect and prevent terrorism-related and other types of criminal activity. At the federal level, the Department of

Justice (DOJ) is integrating "OneDOJ" regional partnerships with the Law Enforcement National Data Exchange (N-DEx) program, illustrating the value of using standards to exchange information. OneDOJ leverages ISE common standards which enable it to be used and interoperate with other federal, state, local, and tribal information sharing efforts.

Other agencies have also undertaken efforts to improving sharing and collaboration of law enforcement information. The Department of Homeland Security (DHS) Law Enforcement Information Sharing Service (LEISS) project—an effort funded in part by the PM-ISE—has directly contributed to improving the quality and quantity of information available at fusion centers. LEISS has expanded significantly, covering all major geographic regions in the U.S. The number of participating agencies, now at 489, is expected to more than triple over the next year. LEISS is interoperable with OneDOJ and its state, local, and tribal (SLT) partners.

State, local, and tribal agencies have also taken strides in information sharing and collaboration with the Federal Government and with other states or localities. Numerous state and major urban areas have adopted local solutions that are now being linked together through common standards and practices.

### *Suspicious Activity Reporting (SAR)*

#### *Unified SAR process demonstrated clear, positive impact on local counterterrorism efforts while protecting privacy and civil liberties*

The Nationwide SAR Initiative (NSI) is the nation's neighborhood watch—where hometown and homeland security meet. A unified NSI process has a clear, positive impact on local counterterrorism efforts and enhances privacy and civil liberties protections. The NSI builds on what law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents indicative of criminal activity—and establishes a standardized process to share SAR information among agencies to help detect and prevent terrorism-related activity. The ISE-SAR Evaluation Environment was formally concluded in September 2009. In February 2010, DOJ established a Program Management Office (PMO) to support nationwide implementation of the SAR process. The NSI continues to be one of the ISE's most significant accomplishments, helping to address deficiencies highlighted by the 9/11 Commission.

### *Alerts, Warnings, and Notifications*

#### *Interagency Threat Assessment and Coordination Group reviewed, provided comments, or proposed language to more than 400 Intelligence Community (IC) products intended for SLT partners*

The ability of participants to generate, disseminate, and receive alerts, warnings, and notifications of potential or impending terrorist activities in near-real time is a fundamental ISE capability. The Interagency Threat Assessment and Coordination Group (ITACG) continues to be an effective mechanism for facilitating the dissemination of intelligence products, to which state, local, tribal, and private sector partners may not

otherwise have access. Now fully integrated into the production processes at DHS, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC), the ITACG Detail—a team of fire, investigative, tribal, law enforcement, and health first responders—provides a valuable perspective by identifying topics of interest to state, local, and tribal entities and nominating products to be written or rewritten at the unclassified level or at the lowest possible classification-level. Over the last year, the ITACG contributed to the publication of 34 Roll Call Releases; reviewed, provided comments, or proposed language changes to more than 400 IC products; and requested downgrading of 78 classified IC products.

## *Cargo and Person Screening*

### *The Federal Government is moving toward adoption of common biometric standards to improve person screening processes*

Screening of cargo and people is a major part of the effort to protect our people against threats from violent extremists. The sharing of information among all parties involved is an essential ingredient of a successful screening process. In 2009, the PM-ISE and a number of mission partners conducted an analysis of radiological and nuclear threat information sharing within the cargo screening environment. This analysis identified specific opportunities for improved information sharing among all levels of government to improve our Nation's defenses against acts of nuclear or radiological terrorism.

The National Science and Technology Council Subcommittee on Biometrics and Identity Management led an interagency effort to develop policy for enabling biometric standards and an associated registry of recommended biometric standards. This work ensures that common biometric standards are adopted across all federal systems, that they support interoperability, and that they are potentially extensible to non-federal partners and systems.

## *Terrorist Watchlisting*

### *Completed development of "Encounter Service" to support analysis and information sharing in fusion centers*

As part of the President's tasking following the attempted terrorist attack on Northwest Flight 253, the National Security Staff led an effort to update terrorism watchlisting guidance. The Terrorist Screening Center (TSC) has also undertaken several initiatives to improve the way that terrorist watchlists are processed and shared. The TSC input to DHS's *Secure Flight* program was implemented using the National Information Exchange Model (NIEM)-compliant Terrorist Watchlist Person Data Exchange Standard (TWPDES). Since late 2009, TWPDES has been used daily to share the list of No Fly- and selectee-designated Known or Suspected Terrorists for screening of airline passengers. TWPDES is now available as an unclassified standard with no prohibitions on dissemination. As a result, international partners and vendors can now freely access and develop software that supports this NIEM-compliant standard for data sharing.

In late 2009, DOJ (Bureau of Justice Assistance [BJA]), DHS, and TSC jointly developed an "Encounter Service" that allows designated fusion centers to share positive encounter

data with both TSC and other centers to support analysis and information sharing about terrorist activities.

### *Sharing with International Partners*

#### *U.S. and E.U. adopt 2010 Declaration on Counterterrorism*

Robust and regular two-way information sharing and collaboration with international partners continue to be cornerstones of our effort to thwart terrorist attacks. A hallmark achievement in international collaboration was the adoption by the U.S. and the European Union (E.U.) of the *2010 Declaration on Counter-Terrorism*. This declaration stresses that an effective and comprehensive approach to diminishing the long term threat of violent extremism is a vital component of U.S. and E.U. efforts to combat terrorism. DOJ played a key role in these negotiations on behalf of the U.S. Government.

In addition, the Department of State and the TSC have concluded non-binding arrangements or formal agreements with 18 foreign partners encompassing commitments for the reciprocal exchange of terrorism screening information

## ISE Core Capabilities

### *Fusion Centers*

#### *Nationwide Baseline Capabilities Assessment underway; Critical Operational Capabilities Strategy will assure an integrated, national network of fusion centers*

The ability to analyze and quickly draw appropriate inferences from multiple and sometimes disparate information sources lies at the heart of the challenge the ISE was established to address. In the aftermath of 9/11, states and localities established fusion centers, developing local and regional capabilities that previously existed only at the federal level. In 2010, federal, state, and local officials launched the first nationwide, in-depth assessment of fusion center baseline capabilities in order to strengthen and mature the national network of state and major urban area fusion centers.

Fusion center directors prioritized four “Critical Operational Capabilities” which are the focus of gap mitigation. This strategy will assist fusion centers in more quickly adapting to their roles as the primary focal points within the state and local environment for the receipt and sharing of homeland security-related information, in partnership with the Federal Government. A proposed multiagency National Fusion Center Program Management Office at DHS, will lead the Federal Government’s efforts to support fusion centers with this gap mitigation.

A study of the current state of fusion center connectivity to federal Secret networks identified the need for consistent processes for planning and operations and a consistent security management framework for coordinating, managing, and overseeing fusion center access to and protection of classified systems. As a follow-up, the PM-ISE is working with Chief Information Officers from federal agencies operating Secret-level networks to develop a proposed way-ahead for the federal Secret-domain enterprise.

### *State, Local, and Tribal Information Needs*

#### *Creating a single vehicle for reporting information needs*

Incorporating SLT needs for terrorism-related information is a key step in the NSI process. In July 2009, the NCTC produced the first consolidated national set of enduring, terrorism-related information needs that included inputs from state, local, and tribal partners. In a complementary effort, DHS has put in place an integrated process for documenting Standing Information Needs for the Homeland Security Community of Interest that will feed into the NCTC process.

### *Improved Handling and Sharing of Controlled Unclassified Information (CUI)*

#### *Launched major effort—the Sensitive but Unclassified (SBU)/CUI Interoperability Initiative—to create a federated, interoperable environment of multiple SBU/CUI networks*

A longtime objective of the ISE has been to encourage sharing of terrorism-related information at the lowest possible security level, unclassified if possible. On December 15, 2009, Secretary Napolitano and Attorney General Holder jointly released the Report and Recommendations of a Presidential CUI Task Force that had reviewed current practices and made 40 recommendations on implementing a comprehensive CUI policy that will have important implications for many ISE mission processes and core capabilities.

Responding to a White House priority, the PM-ISE, DOJ, DHS, and the Office of the Director of National Intelligence (ODNI) joined with state, local, and tribal partners on a major endeavor—the SBU/CUI Interoperability Initiative—to develop a strategy, architecture, implementation plans, and security and privacy guidelines for a federated, interoperable environment of multiple SBU/CUI networks. This effort has already achieved a number of important "quick wins."

## ISE Enablers

### *Architecture and Standards for Information Sharing*

#### *ISE Shared Spaces concept applied to a number of applications in the Federal Government's IT management framework*

During this past year, the ISE Architecture program and its concepts became part of the Federal Government's IT management framework. The PM-ISE and mission partners collaborated on a number of important initiatives, partnering with DOJ to broaden law enforcement community presence in the NSI; assisting the Department of Transportation and the Nuclear Regulatory Commission with ISE Shared Space implementation planning; and working with the Global Justice Information Sharing Initiative (GLOBAL) to develop a systems architecture reference guide.

The positive results achieved through use of the *ISE-SAR Functional Standard* demonstrated the lasting value of SAR as an institutional information sharing process and ultimately led to the establishment of the NSI PMO. Work continued on refinements

to the *ISE-SAR Functional Standard* implementation, including an analysis of the data exchange and business processes between FBI's eGuardian system and other operating ISE Shared Spaces.

The National Information Exchange Model (NIEM) is a federal, state, local, and tribal interagency initiative providing a foundation for the seamless exchange of information. The NIEM development process—the basis for ISE functional standards—is designed to develop, disseminate, and support enterprise-wide information exchanges, standards, and processes that can enable organizations in broad communities of interest to effectively share critical information. As a testimonial to its accomplishments, NIEM is being used as the standard for reporting on progress on achieving the goals of the American Recovery and Reinvestment Act of 2009. In addition, the Office of Management and Budget conducted an evaluation that highlighted the maturity and capability of federal agencies in making standards a cornerstone of their enterprise architectures.

## *Privacy, Civil Rights, and Civil Liberties*

### *More than 80% of designated fusion centers have submitted draft privacy policies*

Significant progress was made in strengthening the protection of privacy, civil rights, and civil liberties across all sectors of the ISE. Eight ISE departments and agencies have submitted ISE privacy policies (covering nine ISE members), and the remaining six ISE members have policies under development. In addition, more than 80% of the 72 designated fusion centers have submitted draft privacy policies for review and technical assistance and more than a dozen fusion centers have been notified by DHS that their policies have been determined to be "at least as comprehensive as" the ISE Privacy Guidelines.

DHS conducted Privacy, Civil Rights, and Civil Liberties "Train the Trainer" sessions for designated fusion center privacy officers and will provide ongoing support and assistance to fusion center privacy officers in developing training curriculums. Some fusion centers have already developed privacy training courses incorporating national policies and procedures, but tailored to local conditions.

## *Improving Protection While Expanding Access*

### *Harmonized information systems security controls and standards—a critical step towards establishing a single national baseline of security standards*

The Federal Government is working to put in place a policy foundation to govern access and protection of classified national security information shared by agencies with SLT partners. The proposed policy would standardize the processes for SLT and private sector access to classified information, ensure that the classified information is properly shared, and reduce the current security barriers inhibiting the sharing of classified information with these partners.

The Joint Task Force Transformation Initiative—a partnership between the National Institute of Standards and Technology, the IC, and the Department of Defense (DoD)—produced harmonized security controls and standards—a critical step towards

establishing a single national baseline of security standards. This key work will enable the reciprocal acceptance of IT security testing which in turn will allow for more system interconnections and speed the free flow of information among federal agencies and non-federal partners alike.

The Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance was developed by the Identity, Credential, and Access Management Subcommittee (co-chaired by the General Services Administration and DoD) of the Federal Chief Information Officer Council in November 2009. This document provides a common segment architecture and associated implementation guidance for use by federal agencies as they continue to invest in programs to improve identity access and management.

Through the implementation of Intelligence Community Directive 501, the IC has made considerable progress on improving information sharing by enabling discovery of disseminated analytic products. Using a combination of attribute-based access, tagged data, and auditing to promote secure information sharing, over three million intelligence products are now discoverable and that number continues to grow daily. The IC has made considerable progress on improving information sharing by enabling discovery of disseminated analytic products through the creation of the Library of National Intelligence (LNI). LNI uses a combination of attribute-based access, tagged data, and auditing to promote secure information sharing of more than three million intelligence products. Using the library, authorized IC users are able to conduct a single search of the IC's disseminated analytic products, covering 99% of the included product lines, compared to the past where users had to visit over 50 different websites to discover the same information.

## *Open Government*

### *Building Communities of Trust Initiative aims to build relationships between police departments and fusion centers and the communities they serve*

A number of activities over the last year directly supported the President's goal of creating and institutionalizing a culture of open government based on the cornerstone principles of transparency, participation, and collaboration. One example is the Building Communities of Trust initiative which focused on developing relationships of trust between police departments, fusion centers, and the communities they serve. The lessons learned from this initiative were then synthesized to develop formal Guidance, for local police agencies and fusion centers and the local communities they serve, to emphasize the value of outreach and transparency and the importance of working with local police in becoming more sensitive to local community issues. In turn, local communities will be more willing to provide information on suspicious behaviors that could potentially help law enforcement agencies detect and prevent terrorist attacks.

### *Personal and Organizational Accountability and Governance*

#### *Memorandum to Chief Human Capital Officers supporting accountability for information sharing*

Part of creating a culture of information sharing involves changing the way people value information sharing and collaboration by encouraging behaviors that foster sharing and discouraging those that do not. In October 2009, the Director, Office of Personnel Management issued a memorandum to federal Chief Human Capital Officers, which stated "information sharing and collaboration should be a common, core behavior across all Departments and agencies."

The Information Sharing and Access Interagency Policy Committee (ISA IPC) was established by the White House in 2009 and subsumed the role of the Information Sharing Council established by IRTPA. In June 2010, the PM-ISE was designated by the White House as a co-chair of the ISA IPC. This dual-role is an acknowledgment that policies, business practices, architectures, standards, and systems developed for the ISE can be applicable to other types of information beyond terrorism and *vice versa*.

Governance and decision-making across the ISE are supported by an integrated performance and investment process. This year, progress across the ISE was captured through the 2010 ISE Annual Performance Assessment Questionnaire and the collection and analysis of financial data to determine the extent to which ISE priorities are being incorporated into agency budgets. Using this information, the PM-ISE, working with Office of Management and Budget and the White House National Security Staff, established future ISE priorities as outlined in the Fiscal Year 2012 ISE Programmatic Guidance.

SECTION 1

# INTRODUCTION

> There has been a recognized need in recent years to enhance national security by establishing an information sharing environment that facilitates the sharing of terrorism-related information … across agencies and levels of government. The global nature of the threats facing the United States requires that our Nation's entire network of defenders be able rapidly to share … information so that those who must act have the information they need.
>
> — President Barack H. Obama[3]

## 1.1 Purpose and Scope

This Fourth Annual Report to the Congress on the Information Sharing Environment (ISE) responds to the requirement in the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, (IRTPA) for "a progress report on the extent to which the ISE has been implemented."[4] The report reflects the collective accomplishments and opportunities of the terrorism and homeland security[5] information sharing and access community, and highlights successful strategic partnerships between the Office of the Program Manager for the Information Sharing Environment (PM-ISE) and a host of federal and non-federal mission partners committed to the continuous improvement of sharing and collaboration in terrorism relevant information in order to make America safer while still ensuring privacy, civil rights, and civil liberties.

The term "information sharing" in the context of the ISE means that the necessary information, properly controlled, gets to the right people in time to counter terrorist threats to our people and institutions. The enactment of the Intelligence Reform Act in December 2004 signaled the start of a major effort to ensure that barriers to information sharing were removed and that best practices were employed across all levels of government.

---

3 White House Memorandum for the Heads of Executive Departments and Agencies, subject: "Classified Information and Controlled Unclassified Information" (May 27, 2009), available at http://www.whitehouse.gov/the_press_office/Presidential-Memorandum-Classified-Information-and-Controlled-Unclassified-Information/.

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

5 Section 1016 of IRTPA, as amended, directs the ISE to improve the sharing of Terrorism and Homeland Security Information. The IRTPA definition of Terrorism Information encompasses all terrorism-related information "whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities," and was explicitly amended in 2007 to include Weapons of Mass Destruction Information. For brevity, these types of information are collectively referred to as "terrorism-related" information.

The ISE is an interrelated set of harmonized policies, mission processes, and systems—leveraging common core capabilities, and relying on supporting ISE enablers—allowing the men and women on the frontline to access and share the information they need to keep the country safe. It is not, nor was it ever intended to be, a traditional, dedicated information system. IRTPA deliberately uses the word "environment" rather than "system" or "network" to suggest a decentralized, multi-faceted approach that brings together existing policies, processes, and systems developed and implemented by agencies and organizations at all levels of government that collectively support the national and homeland security missions.

## 1.2 Structure of this Report

This introductory section first cites a real-world event that occurred in the last year to illustrate the current state of information sharing and collaboration, pointing out tangible progress and acknowledging areas where more work is necessary. It goes on to describe the ISE business model, emphasizing the central role mission partners play in implementing the ISE and highlighting important programs that have now transitioned from PM-ISE sponsorship to mission partner management. Lastly, the Introduction discusses the recently issued National Security Strategy, its "whole of government" approach, and its implications for the ISE.

The remainder of the report describes information sharing progress from June 2009 through June 2010, including information on both major ISE projects and those activities launched by mission partners that have contributed significantly to inter-governmental information sharing. Although the focus of this report remains on ISE initiatives that address the specific requirements set forth in IRTPA, the report also describes mission partner accomplishments, some of which may not have been developed explicitly to support counterterrorism, but which do end up supporting the counterterrorism mission in some cases or that may ultimately become "best practices" with applicability to information sharing and collaboration government-wide, including the ISE.

The fact that the ISE can leverage these achievements is consistent with one of its key attributes identified in IRTPA—to build upon existing systems capabilities currently in use across the government.[6] The breadth of the information sharing activities described point out the need for a coherent strategy to drive these activities, minimize unnecessary duplication, and provide the management and oversight needed to leverage individual accomplishments across the entire ISE.

## 1.3 Spotlight on Information Sharing

Information sharing has been featured prominently in the media since the previous ISE report in June 2009. One major event, in particular, helped reinforce the important role that a robust Information Sharing Environment plays in keeping America safe. The failed attempt to bomb Northwest Airlines Flight 253 on Christmas day 2009 highlights the fact that merely making information accessible to those who need it is not enough and shows the importance of presenting this information in ways that make the key facts

[6] IRTPA (b)(2)(D).

## The Attempted Bombing of Flight 253

On December 25, 2009 a Nigerian national, Umar Farouk Abdulmutallab, attempted to detonate an explosive device on board Northwest Airlines Flight 253 en route from Amsterdam to Detroit. Although quick and courageous action by passengers and the flight crew prevented any serious damage and the aircraft landed safely, questions naturally arose as to whether or not the information needed to prevent the attack was available to the people who needed it. To address these questions, President Obama directed his Assistant for Homeland Security and Counterterrorism, John Brennan, to conduct a review of the incident.

The review concluded that the fundamental problems leading to the Flight 253 incident were different from those identified in the wake of the 9/11 attacks concluding that the inability to detect and prevent the attempt in advance was more a problem with "connecting the dots" than due to any breakdown of information sharing. This has also been characterized as a "signals to noise" issue where the key facts (the signals) are available to analysts but are not fully synthesized because their relationships are lost in a mass of unrelated and unprocessed data (the noise).

As President Obama noted in presenting the results of the review, "In sum, the U.S. government had the information—scattered throughout the system—to potentially uncover this plot and disrupt the attack. Rather than a failure to collect or share intelligence, this was a failure to connect and understand the intelligence that we already had."

Although the review focused most of its attention on the analytic process, it did highlight the importance of ensuring that information is accessible in a form and structure that gives analysts at all levels of government the highest likelihood of detecting and preventing future attacks.

Agencies across the Federal Government responded to the White House recommendations and actions called for by the White House review. The Director of National Intelligence (DNI), for example, conducted a 30 Day Counterterrorism Review that identified a number of findings and recommendations which are now being carried out by the Office of the DNI (ODNI) and the 16 agencies in the Intelligence Community (IC). One recommendation called for integration of disparate information systems to ensure that critical data is discoverable and accessible by analysts IC-wide.

Subsequent Executive Branch reviews of this incident and a separate review by the Senate Select Committee on Intelligence (SSCI) reached similar conclusions. The SSCI report cited instances where intelligence was either disseminated too late or not broadly enough to reach everyone with a need for the information. All these reviews agree that merely providing access, while necessary, is not sufficient. The information must also be in a form and structure where it can be readily used by counterterrorism analysts. This will require close collaboration between gatherers of information and the analysts who use it, backed up by improved training programs and tools to help the analysts distinguish between the signals and the noise, better correlate and integrate fragmentary data, and synthesize the results in an actionable way, i.e., to connect the dots.

stand out, i.e., that the signals are discernable through the noise. In this way, analysts will be better able to identify, correlate, fuse, and synthesize fragmentary information —"connect the dots"—into a coherent, actionable story that can be used to detect and prevent terrorist attacks.

### 1.3.1 Promoting an ISE Learning Culture – Continuous Improvement and Innovation

Cases like this, and the Fort Hood and Times Square incidents, show that the ISE cannot be a static environment, but must continually adapt to the challenges posed by violent extremists. To succeed, the PM-ISE and other ISE stakeholders and mission partners must promote a culture of continuous improvement and innovation, routinely challenging our assumptions and implementing measurable improvement by:

- Studying other government and private sector efforts to improve information sharing and collaboration;
- Identifying and promoting innovative solutions to information sharing challenges;
- Benchmarking best practices from all sources and encouraging their adoption; and
- Using performance goals and measures to ensure that results meet expectations.

## 1.4 The Scope of the ISE

Figure 1 portrays the ISE as a partnership of five primary communities—Defense, Intelligence, Homeland Security, Foreign Affairs, and Law Enforcement—all of which support the frontline activities shown on the left of the chart. These communities, moreover, cut across all levels of government in our federal system, involving state, local, and tribal partners as well as the private sector and international partners where appropriate. While each community has multiple missions, they all rely on timely and accurate information to achieve their goals. The intersection of these five communities with the counterterrorism mission—the effort to keep our people safe from terrorist tactics of violent extremists—constitutes the domain of the ISE.

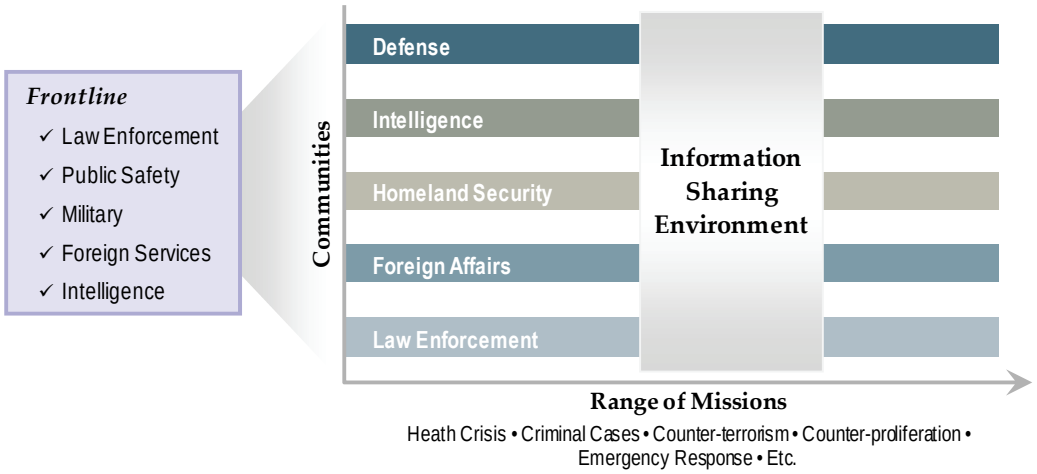



**Figure 1. The ISE as a Partnership of Five Communities**

The scope of the ISE can be described as a collection of end-to-end mission processes and supporting core capabilities, enabled by standards, architecture, security, access, policy, governance, and management. End-to-end mission processes are operated by ISE mission partners and directly support frontline law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel. They encompass a broad range of activities that are intended to have a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity.

While end-to-end mission processes—Suspicious Activity Reporting (SAR), for instance—are the central focus of the ISE, they depend on the availability of core capabilities that support individual mission processes. Fusion centers, for example, play important roles in almost all of the mission processes. Furthermore, achieving interoperability across multiple networks handling Controlled Unclassified Information (CUI) (formerly Sensitive but Unclassified (SBU) information) will contribute significantly to improving mission processes supporting SAR and Alerts, Warnings, and Notifications (AWN). Finally, ISE enablers—such as, a sound privacy, civil rights, and civil liberties (CL) policy—are essential to both ISE mission processes and the core capabilities. Figure 2 depicts this notional view of the ISE, portraying some of the major mission processes, core capabilities, and enablers.

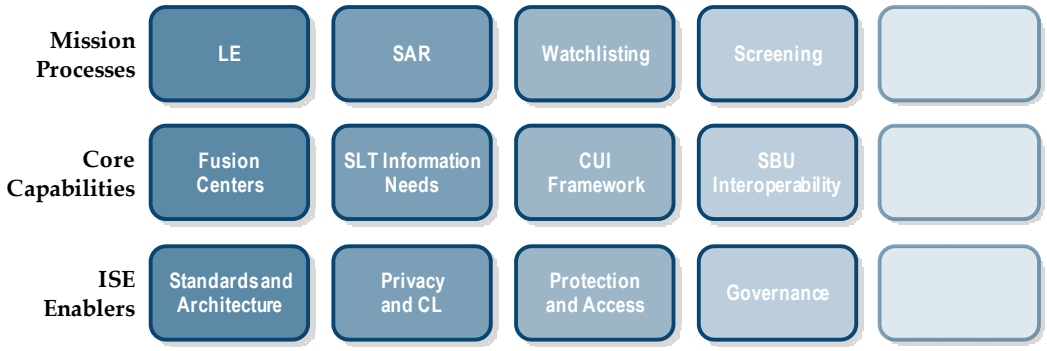



**Figure 2. Notional View of the ISE**

## 1.5 The ISE Business Model

The mission of the ISE is to improve the management, discovery, fusing, sharing, delivery of, and collaboration around terrorism-related information to enhance national security and help keep our people safe. Federal agencies and state, local, tribal, and private sector partners—the ISE mission partners—have the mission responsibility to help protect our people and our institutions. Consequently, these agencies deliver, and operate, the ISE and are accountable for sharing to enable end-to-end mission processes that support counterterrorism (CT).

### 1.5.1 Role of the PM-ISE

No single agency or department has the mandate or the tools necessary to empower and deliver the ISE in the same way as the PM-ISE. The role of the PM-ISE, therefore, is to coordinate and facilitate the development of a network-centric ISE by focusing on standards and architecture, security and access, associated privacy protections, and best

practices. The PM-ISE serves as a change agent and enabler for innovation and discovery in providing ideas, tools, resources, and management support to mission partners who then apply them to their own agencies or communities. In particular, the PM-ISE relentlessly advocates identifying, integrating, and sharing best practices. Focus on best practices raises confidence, lowers risk, and accelerates adoption, use, and reuse of key capabilities. Examples of such reuse include:

- Reuse of standards and architecture, information exchanges, capabilities, and infrastructure;
- Reuse across the terrorism information sharing mission, across complementary missions, and into new mission areas unrelated to terrorism but important to mission partners; and
- Reuse leading to time savings and cost avoidance, bringing together the power of smart management and effective governance.

The PM-ISE has several tools at his disposal to catalyze transformation. These include:

1. Information sharing and access subject matter expertise;
2. Interagency policy harmonization through the White House's Information Sharing and Access Interagency Policy Committee;
3. Management and budget prioritization and follow-through via partnerships with the Office of Management and Budget and the White House National Security Staff;
4. National leadership via communications and outreach activities with mission partners and the frontline;
5. Co-investment of seed capital, with mission partners, in priority early stage activities via Economy Act transactions to bridge the budgeting cycle and accelerate progress; and
6. Ability to bring together mission partners to identify and address common mission equities.

The importance of these tools and mandates becomes clear in filling the gaps in budgetary considerations which challenge the ability of any single organization to achieve the goals of sharing information. Seeding new initiatives or transformation of existing capabilities is hard; and even more so in government where funding constraints and long-lead times make budgeting for new initiatives difficult. Addressing inherent interdependencies is at the core of the office's ability to respond to and support its partners.

The PM-ISE's aim is always to develop these initiatives in full partnership with mission owners. In addition, as improved business processes, supporting policies, and technical solutions are developed and deployed, the PM-ISE helps identify, promote, and spread best practices and, where possible, influences resource allocation decisions to ensure the institutionalization and potential reuse of these mission partner capabilities.

In carrying out his responsibilities, the PM-ISE employs three engagement models:

1. For a small number of core priorities—such as SAR, SBU Networks, and fusion centers—the Program Manager engages directly to help drive progress. The goal with these efforts is transactional: to first drive transformation in conjunction with mission partners, to then help the mission partners in planning for broader implementation of the transformed effort, and ultimately to decrease involvement.
2. The PM-ISE supports a consistent set of enablers, such as privacy, information assurance, and standards and architecture. This support is ongoing, not transactional, although engagement will spike around specific challenges or opportunities.
3. Finally, the PM-ISE is committed to broadly sourcing, integrating, and sharing best practices. The PM is recognized as a champion for information sharing by agencies at all levels of government, and receives and supports requests for reuse and ramp-up of sharing best practices.

A major strength of the ISE business model has been its flexibility, a necessity for operating in uncharted waters. The expanding influence of the ISE is the result of continued success in serving our mission partners, the organizations ultimately responsible for the delivery and operation of the ISE.

### 1.5.2 Central Role of Mission Partners

The ISE is realized by the investment of mission partners and made relevant through use by frontline law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel. Ultimately, the ISE is neither more nor less than the contributions of the ISE mission partners, augmented by core capabilities and ISE enablers. Over the last several years, information sharing centers of excellence have emerged across government. These centers have developed independently and adopted different approaches to sharing information across all levels of government, but they share a common commitment to using the power of information to help keep our people safe.

### 1.5.3 Terrorism-Related Information and Beyond

The focus of the ISE is specifically on the sharing of terrorism and homeland security information. The need for collaboration and sharing of information, however, extends beyond terrorism-related issues to encompass all information relevant to the national security of the United States and the safety of the American people. Information does not typically come neatly packaged and labeled to indicate its subject matter or domain of interest. Information from one domain may prove valuable in another, often at a different time and in another form. Information that initially surfaces in the public health domain may later be determined to have implications for counterterrorism, and *vice versa*. Given that, the ISE must reach out to other information sharing activities at all levels of government to ensure effective information sharing and access, while protecting privacy and information security, across all domains that may potentially process or handle terrorism-related information.

Consequently, ISE mission partners rarely have the ability to segregate their activities to isolate terrorism information. Frontline law enforcement, for instance, is more likely to generate SARs relating to gang or narcotic crime than criminal activity with a clear terrorism nexus. The inherent adaptability of the business process developed as part of the Nationwide SAR Initiative (NSI) allows mission partners to capitalize on consistent training, privacy and civil liberty protections, oversight, and change management investments developed for the ISE and apply these capabilities more broadly to all-crimes, all-hazards operations. Such mission partner needs must be factored into ISE strategy and plans to avoid deadlock and inefficient or ineffective solutions.

### 1.5.4 Major ISE Initiative Transitions

As shown in Figure 3, four ISE initiatives have transitioned from PM-ISE sponsorship to agency management over the last four years.

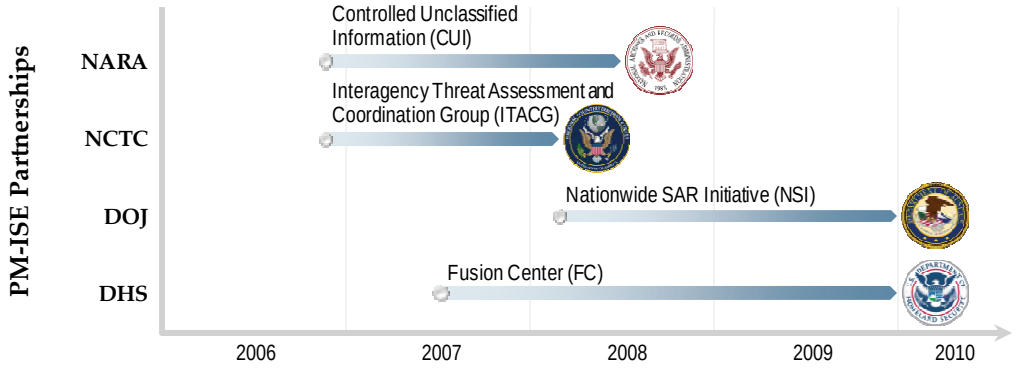



**Figure 3. Major ISE Transitions**

A May 2008 Presidential Memorandum designated National Archives and Records Administration (NARA) as the Executive Agent responsible for creating and carrying out a government-wide framework for CUI, effectively transitioning responsibility for this effort from PM-ISE to NARA.[7] Although many agencies were involved with the establishment of the Interagency Threat Assessment and Coordination Group (ITACG), the PM-ISE was a strong proponent and worked closely with other agencies to see that the ITACG was properly funded and staffed. (The PM-ISE continues to report on its progress to the Congress each year.) Subsequently, the host agency, the National Counterterrorism Center (NCTC) and lead analytic agencies (the Department of Homeland Security (DHS) and the FBI) assumed full responsibility for ITACG management in February 2008.

Since the last ISE Annual Report, two major programs graduated from the concept stage and are taking steps towards full nationwide implementation. On December 17, 2009, the President's Assistant for Homeland Security and Counterterrorism reported that Homeland Security Secretary Napolitano agreed to establish a multiagency program

[7] Presidential Memorandum for the Heads of Executive Departments and Agencies on "Designation and Sharing of Controlled Unclassified Information (CUI)," May 07, 2009 available at http://www.ise.gov/docs/guidance/May_9_2008_WH_Memorandum_CUI.pdf.

management office (PMO) "to coordinate support for a growing network of state and major urban area fusion centers," and that Attorney General Holder agreed to establish a multiagency PMO (in the Justice Department's Bureau of Justice Assistance (BJA)) "charged with developing a nationwide framework for reporting suspicious activities." The memorandum went on to say:

> *Establishing dual PMOs will institutionalize two essential national security initiatives. The fusion center concept and an overall suspicious activity reporting approach have matured under the auspices of the Program Manager, Information Sharing Environment, and through the hard work of collaborating departments and agencies and other contributors … Going forward, leadership by the Departments of Homeland Security and Justice will provide dedicated attention to speed effective implementation.*[8]

These transitions validate the assumptions underlying the overall ISE business model. As additional ISE efforts mature sufficiently, they will follow a similar path: starting out with strong PM-ISE sponsorship and support and, ultimately, assigning lead responsibility to the mission partner best postured and equipped to fully institutionalize the capability.

## 1.6 Managing the ISE

### 1.6.1 The ISE Framework

IRTPA requires the PM-ISE to "plan for and oversee the implementation of, and manage, the ISE."[9] To better define and manage ISE implementation, the PM-ISE adopted the ISE Framework in 2009. This Framework creates critical linkages between four strategic ISE goals: (1) *Create a Culture of Sharing;* (2) *Reduce Barriers to Sharing;* (3) *Improve Sharing Practices with Federal, State, Local, Tribal, and Foreign Partners; and* (4) *Institutionalize Sharing*. Associated with these four goals are fourteen sub-goals, and a corresponding set of outcomes, objectives, products, activities, and associated performance measures.

### 1.6.2 Maturity Assessment

The ISE Maturity Model (Figure 4) was a tool developed to help assess ISE progress in meeting the goals and sub-goals of the ISE Framework. Figure 5 depicts the maturity level assessments for the goals and sub-goals in the ISE Framework as of June 2010.

As Figure 5 shows, nine of the current fourteen sub-goals are in the Defined level of maturity and the remaining five are in the Managed level which gives at least a general indicator of the level of overall ISE maturity. The planned refresh of the 2007 National Strategy for Information Sharing will build on this baseline but go beyond it to describe a collaboratively-developed, concrete end state and galvanize action around well-defined goals and objectives fully vetted with our mission partners and all ISE stakeholders.

---

8 Ibid.

9 IRTPA §1016(f)(2)(a).

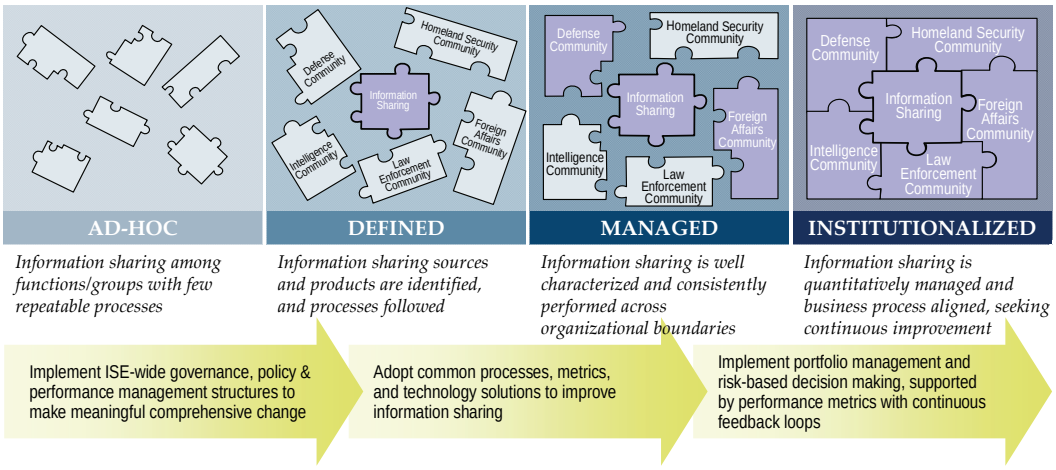



**Figure 4. ISE Maturity Model**


**Figure 5. 2010 ISE Framework Maturity Assessment**

## The National Security Strategy — Whole of Government and Information Sharing

On May 27, 2010 President Obama issued his National Security Strategy that lays out a strategic approach for advancing American interests, including the security of the American people, a growing U.S. economy, support for our values, and an international order that can address 21st century challenges. Keeping America safe is a major theme of the new strategy, and improved information sharing to counter the terrorist threats to the American people and its institutions continues to play a prominent role.

The National Strategy calls for a "Whole of Government" approach for strengthening national capacity based on applying and integrating the efforts of all agencies with a national security mission. It goes on to say:

> *To succeed, we must update, balance, and integrate all of the tools of American power and work with our allies and partners to do the same. … Our intelligence capabilities must continuously evolve to identify and characterize conventional and asymmetric threats and provide timely insight. And we must integrate our approach to homeland security with our broader national security approach.*

With respect to the counterterrorism mission, the ISE plays an essential role in this "Whole of Government" approach; without a central core for information sharing and access, we cannot succeed. Information sharing contributes, in an important way, to our efforts to achieve an advantage in the use of information to understand and counter asymmetric threats. Major ISE initiatives—including integrating and leveraging state and major urban area fusion centers; establishing a nationwide framework for reporting suspicious activity; and adopting an integrated approach to counterterrorism information systems to ensure that the analysts, agents, and officers who protect us have access to all relevant intelligence throughout the government—are explicitly cited as key elements of the President's approach to preventing attacks on our people and our institutions.

The ISE spans our federated democracy—integrating federal, state, local, and tribal governments—and in so doing, augments the "Whole of Government" concept in a critical way. Further, the ISE extends to our partners in the private sector where 85% of critical infrastructure is owned and operated and promotes sharing with international partners. This advances "Whole of Government" by leveraging and extending Open Government concepts of transparency, participation, and collaboration, with appropriate safeguards for information security, privacy, and civil liberties. Finally, the ISE spans the five critical counterterrorism communities—Intelligence, Foreign Affairs, Homeland Security, Law Enforcement, and Defense—better enabling the entire counterterrorism community to respond to the President's call for a "Whole of Government" approach.

SECTION 2

# ISE MISSION PROCESSES

> To succeed, we must update, balance, and integrate all of the tools of American power and work with our allies and partners to do the same. Our military must maintain its conventional superiority … while continuing to enhance its capacity to defeat asymmetric threats … We must invest in diplomacy and development capabilities and institutions in a way that complements and reinforces our global partners. Our intelligence capabilities must continuously evolve to identify and characterize conventional and asymmetric threats and provide timely insight. And we must integrate our approach to homeland security with our broader national security approach.
>
> — National Security Strategy, May 2010, Page 14

End-to-end mission process improvement is at the heart of building the ISE. Mission processes respond directly to external counterterrorism drivers and priorities and provide a focus for developing initiatives and measuring progress. They encompass a broad range of activities and include processes that support alerts and notifications; suspicious activity reporting; terrorist watchlist maintenance and use; and other activities and processes with direct mission impact. The distinguishing feature of ISE mission processes is that they all produce outputs that directly support those operations whose aim is to detect, prevent, disrupt, respond to, or mitigate terrorist activity.

This section is organized around a number of these mission processes. Although the list is not intended to be exhaustive and the processes are at varying levels of maturity, the discussion provides the context necessary to understand the state of implementation and ongoing challenges.

## 2.1 Law Enforcement Information Sharing

Sharing of law enforcement information is not a single integrated process. Rather it cuts across business processes in multiple communities at all levels of government. But these seemingly unrelated efforts share many features in common. A fundamental component of effective enterprise-wide information sharing, for example, is the use of information systems which regularly capture relevant data and make it broadly available to authorized users in a timely and secure manner. Although the focus of the ISE is terrorism-related information, many of the techniques used to improve sharing of terrorism information are also applicable to other types of crimes and *vice versa*. Criminal history records, law enforcement incident reports, records of judicial actions and decisions, and watch lists of known and suspected terrorists are all essential sources of vital data that provide accurate, timely, and complete information to law enforcement officers across the country.

Since 9/11 federal, state, local, and tribal (SLT) law enforcement agencies have worked collaboratively to detect and prevent terrorism-related and other types of criminal activity. FBI-sponsored Joint Terrorism Task Forces (JTTFs) and fusion centers represent a change in culture and a willingness to share information among agencies and across all levels of government. Both are partnerships that rely on new policies, business processes, architectures, standards, and systems that provide users the ability to collaborate and share information, and both resulted in the mutual agreement by trusted partners to exchange operational data reports, case files, and similar information on both open and closed investigations.

A common, although not universal, implementation approach features distributed sharing methods, which allow each organization to retain its own information and, at the same time, make it available for others to search and retrieve. Since this information may be maintained in different formats by each organization, the Law Enforcement Information Sharing Program Exchange Specification (LEXS)—a subset of the National Information Exchange Model (NIEM)—was developed to translate information shared among different law enforcement systems into a common format, enabling participants on one system to receive and use information from multiple sources.

### 2.1.1 Collaboration Across All Levels of Government

#### 2.1.1.1 Department of Justice

Over the last several years, the Department of Justice (DOJ) has launched a number of major departmental information sharing initiatives, many of which also include other federal agencies as well as SLT partners. The FBI's Criminal Justice Information Services (CJIS) Division—whose mission is to equip law enforcement, national security, and Intelligence Community partners with the criminal justice information they need to protect the United States while preserving civil liberties—has been at the forefront of many of these initiatives. (See http://www.fbi.gov/hq/cjisd/cjis.htm for more information on CJIS.)

The CJIS Division's mission is to reduce terrorist and criminal activities by sharing timely and relevant criminal justice information across the FBI and qualified law enforcement, criminal justice, and civilian agencies concerning individuals, stolen property, criminal organizations, and activities. CJIS currently serves more than one million users in 18,000 organizations. CJIS exchanges information with its partners through state-of-the-art technologies and statistical services that span the criminal justice community—from automated fingerprint systems to crime statistics; from secure communications to gun purchase background checks. CJIS services include:

- *National Crime Information Center* (NCIC), a computerized database of documented criminal justice information available to virtually every law enforcement agency nationwide, 24 hours a day and 365 days a year;
- *Integrated Automated Fingerprint Identification System* (IAFIS), the U.S. criminal fingerprint identification system;

- *National Instant Criminal Background Check System* (NICS), often known as the Brady gun check system, which determines an individual's eligibility to purchase a gun; and
- *Uniform Crime Reporting Program*, which has developed and provided statistics describing crime rates across the U.S. since 1930.

Table 1 shows performance information for a number of CJIS-provided systems.

**Table 1. Selected CJIS System Performance Statistics**

| System | Number of Records | Transactions per Day | Average Response Time | System Availability |
|---|---|---|---|---|
| **NCIC** | 15 million | 6.7 million | 0.06 seconds | 99.8 percent |
| **IAFIS** | 84 million | 288, 697 | 16.25 minutes for criminal | 99.2 percent |
| **NICS** | —[10] | 39,468 | Two minutes (92% of the time) | 99.9 percent |

At the federal level, the FBI's Law Enforcement On-line (LEO) system has provided a protected means for sharing information with regional law enforcement agency partners through a project originally known as Regional Data Exchange (R-DEx) and subsequently adopted by DOJ for all of its components and renamed OneDOJ. LEO provides access to several secure, Internet communication and transport services such as the National Alert System, Virtual Command Center, and e-Guardian. In addition, DOJ supports six Regional Information Sharing System Network (RISSNET) centers which provide tailored support for specialized law enforcement functions to meet regional needs. (See http://www.riss.net/ for more information on RISS.)

**RISSNET Performance Snapshot**

- More than 97,000 active users at more than 8,500 agencies;
- More than 600 specialized communities of interest; and
- More than 115,000 login visits and 560,000 emails processed in a typical week.

Using web-based connectivity modes, including LEO and RISSNET, DOJ is integrating the OneDOJ regional partnerships into the new Law Enforcement National Data Exchange (N-DEx) program under the CJIS Division. The N-DEx program complements current and developing sharing efforts by providing vertical and cross-jurisdictional connectivity along with robust analytical functions on a national level. It is the cornerstone of DOJ's Law Enforcement Information Sharing Program. Although the information it contains covers all types of criminal activity, N-DEx is an important tool for the CT community in their efforts to detect and prevent terrorism-related crimes.

N-DEx brings together investigative data from criminal justice agencies across the United States, including incident and case reports, booking and incarceration data, and parole/probation information. N-DEx provides advanced data exploitation tools to identify relationships and correlations between people, vehicle/property, location, and

[10] A typical NICS background check searches more than 74 million records in multiple databases.

crime characteristics. N-DEx supports law enforcement and criminal justice agencies and multi-jurisdictional task forces—enhancing national information sharing across federal, state, regional, local, and tribal investigative agencies and task forces.

The N-DEx development illustrates the value of using common standards. CJIS developed the NIEM Information Exchange Package Description (IEPD) before releasing the N-DEx Request for Procurement, allowing the standard to drive subsequent development and implementation activities. Although specific dollar savings are difficult to quantify, vendors are now packaging N-DEx-NIEM compliant applications into off-the-shelf solutions that can easily be adopted by additional jurisdictions, effectively amortizing development costs across a broader customer base.

#### 2.1.1.2 Other Federal Departments

Other departments have also undertaken efforts to improving law enforcement information sharing and collaboration. The DHS Law Enforcement Information Sharing Service (LEISS) project—a PM-ISE endorsed and sponsored effort—has directly contributed to improving the quality and quantity of information available at fusion centers. LEISS is an initiative of DHS's Immigration and Customs Enforcement (ICE) that, in collaboration with DOJ, leverages existing tools and capabilities to expand bi-directional sharing with other federal and SLT partners. LEISS has also adopted LEXS as a standard, providing a foundation for broader sharing of information. As enhancement of LEISS continues, connections will be established with additional state, local, and federal law enforcement agencies as well as with regional law enforcement groups such as fusion centers. DHS information sources will be expanded to include legally shareable enforcement data from all its law enforcement components

**Growth in LEISS**

LEISS has expanded significantly since the effort inception four years ago. There are now 489 participating agencies representing more than 26,000 user accounts and covering all major geographic regions in the U.S. The number of participating agencies is expected to more than triple over the next year.

In the Department of Defense (DoD), the Naval Criminal Investigative Service (NCIS) established the Law Enforcement Information Exchange (LInX) which offers local or regional data hosting capabilities for SLT law enforcement agencies to support their sharing efforts. The NCIS LInX PMO has partnered with N-DEx to facilitate the vertical connectivity of LInX systems to N-DEx for information sharing on a broader scale. For example, within the National Capitol Region more than 115 local, state, and federal agencies are sharing important law enforcement information through LInX. One user noted, "LInX is highly useful in providing information in an efficient format, thus allowing speed and accuracy when completing a thorough workup on a suspect." (See http://www.ncis.navy.mil/linx/steps.html for more information on LInX.)

### 2.1.1.3 State, Local, and Tribal Activities

SLT agencies have taken similar actions in concert with—and in some cases in advance of—federal initiatives. (See pages 17 and 18 for specific examples of SLT successes.) Numerous state and major urban areas have adopted local solutions that are now being linked together through common standards and practices. Some of these include Los Angeles, Jacksonville, Eastern Missouri, Washington State, and San Diego. As shown in Figure 6, San Diego's Automated Regional Justice Information System (ARJIS) system, which has supported the local sharing environment for many years, is now linked with national information sources. (See http://www.arjis.org/ for additional information on ARJIS.)

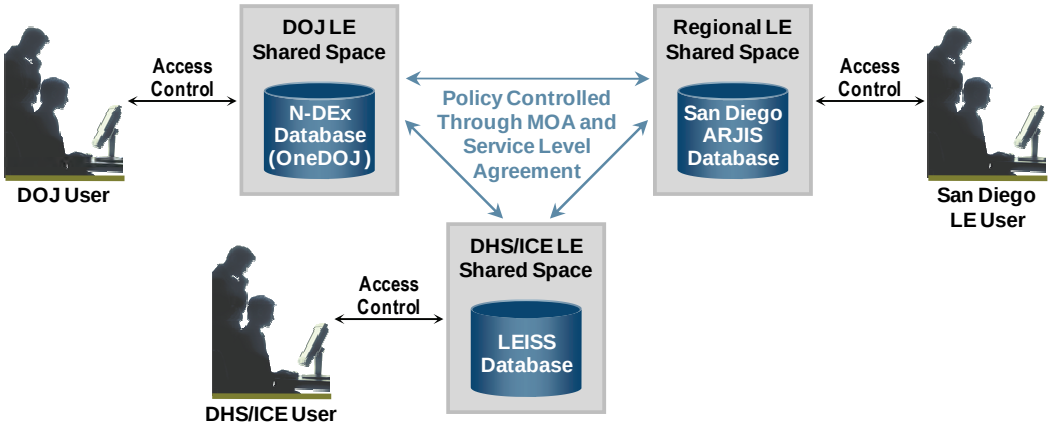



Figure 6. Example of Law Enforcement Information Sharing Flow

### 2.1.2 The Southwest Border Initiative: An Operational Example[11]

Over the past year and a half, DHS, working with its federal, state, local, tribal, and Mexican partners, has made significant progress in cracking down on border-related crime and smuggling while facilitating legitimate travel and commerce. The Administration is committed to building on these successes and addressing current challenges with our partners in order to keep our communities safe from threats of border-related violence and crime. To that end, DHS is implementing a number of initiatives to strengthen and expand upon existing, successful efforts. Many of these depend heavily on expanded information sharing and collaboration. This effort has achieved tangible results over the last 18 months attributable, at least in part, to expanded information sharing and collaboration. For example, seizures of contraband rose significantly across the board last year compared to the year before: illegal bulk cash seizures rose 14 percent; illegal weapons seizures increased by 29 percent; and illegal drugs seizures by 15 percent. Highlights include:

- Strengthening the analytic capability of fusion centers across the Southwest border to receive and share threat information, improving our ability to identify and mitigate emerging threats;

[11] Please see http://www.dhs.gov/ynews/releases/pr_1239821496723.shtm for more information.

## State, Local, and Tribal Information Sharing Successes

Analysts from the Hennepin County (Minnesota) Sheriff's Office Criminal Information Sharing and Analysis (CISA) Unit recently identified a trend of pharmacy robberies, which prompted local law enforcement to initiate an investigation. The investigation produced new information which was fed back to the analysts, allowing them to perform suspect link and timeline analysis and develop subject workups that eventually led to the apprehension of five individuals. CISA was established in 2007 to improve information sharing among federal, state, local, and tribal law enforcement agencies and to assist in the prevention and suppression of criminal activity by providing timely and accurate analysis of criminal information to county law enforcement agencies.

---

Indiana established its first web-enabled statewide intelligence sharing platform for entering, querying, and analyzing gang intelligence by authorized Indiana criminal justice authorities. The Indiana Gang Intelligence Network is a component of the Indiana Intelligence Fusion Center's Gang Intelligence Sharing Project and was created using stimulus funding for criminal justice projects. Its purpose is to improve the collection, analysis, and sharing of gang intelligence information among Indiana law enforcement and criminal justice agencies with the intent of preventing, reducing, and solving gang criminal activity consistent with protecting privacy, civil rights, and civil liberties. Indiana law enforcement and criminal justice leaders are confident that this initiative will play a key role in combating illegal criminal gang activity and violent crime in the State of Indiana.

---

In looking for ways to better use existing resources to prevent violence in and around area schools, the Southern Nevada Counterterrorism Center established a partnership with the Clark County School District Police Department which includes the assignment of a liaison officer to the Counterterrorism Center and the sharing of information, products, and resources that deal with potential or actual incidents. In addition, the School Police Department placed an executive staff member on the Center's governing board. Some of the successes from this partnership include: preventing a gang shootout; locating and returning a 6-year-old kidnap victim; and quickly determining that a bomb threat was not credible, which prevented valuable resources from being wasted. These examples illustrate that horizontal information sharing is often a result of institutionalizing relationships and is a critical component of the all-crimes and all-hazards fusion center approach to supporting law enforcement.

---

The CONNECT Consortium was created when four states with existing Web portals for accessing criminal justice information—Alabama, Kansas, Nebraska, and Wyoming,—came together to connect disparate systems so that all authorized criminal justice users, could obtain valuable information from across jurisdictional boundaries by using a single log-on to their respective portals. By combining the existing systems using the technology standards created by the U.S. Department of Justice's DOJ's Global Justice Information Sharing Initiative, they were able to implement a new approach to interstate information sharing. Central to this achievement was a policy framework that comprised a simple governance structure, standard memoranda of understanding, and individual and collective state privacy policies using the Global Justice Privacy and Civil Liberties Policy Development Guide and Implementation Templates.

---

The collaborative actions taken by the Pacific Regional Information Clearinghouse (Pac Clear) and the Missouri Information and Analysis Center (MIAC) enabled law enforcement to receive necessary information that led to the apprehension of an individual who made approximately 7 phone calls to a military facility in Hawaii, threatening to kill generals and other military personnel. The US Army and the Honolulu Police Department (HPD) identified this as a credible threat, and determined that the subject had previous connections to Missouri through information available in shared databases. Pac Clear became aware of the situation through eGuardian and identified an opportunity to provide support by offering to obtain more information about the subject's time in Missouri. Pac Clear made direct contact with the MIAC and within five minutes received a copy of the subject's Missouri driver's license photo and immediately forwarded it to the HPD. Shortly thereafter, HPD was able to post a "Be On the Look Out" alert with the subject's photo. The subject was apprehended because of the visual aid of the driver's license photo.

---

Over the last two decades separate single-agency Computer Aided Dispatch/Record Management Systems (CAD/RMS) have proliferated at law enforcement agencies across the U.S. These systems were effective in collecting and collating law enforcement records for a single agency; but their utility ended at the agency's jurisdictional boundary, since the information could not be shared with neighboring agencies. A number of states are now developing state-wide CAD/RMS systems to maximize criminal justice information sharing efforts. Delaware, Montana, South Carolina, Tennessee, and Vermont already have state-wide systems in place, and Indiana and Maryland will deploy systems soon. These state-wide systems allow officers to search hundreds of agency databases and millions of offender records in contrast to a single agency system that may provide access to only a few thousand records.

- Establishing a SAR program for the Southwest border. This will help local officers recognize and track incidents related to criminal activity by drug traffickers and utilize this information for targeted law enforcement operations on both sides of the border;
- Working with DOJ to create a new system that will link the relevant information systems of SLT law enforcement entities operating along the Southwest border with those of DHS and DOJ;
- Forging a new partnership with the Major Cities Chiefs Association (MCCA) to create the "Southwest Border Law Enforcement Compact"—designed to boost law enforcement at the border by enabling non-border state and local law enforcement agencies to detail officers to state and local law enforcement agencies along the Southwest border; and
- Increasing joint training programs with Mexican law enforcement agencies—focusing on money laundering investigations and cracking down on human trafficking and exploitation.

## 2.2 Suspicious Activity Reporting (SAR)

The Nationwide SAR Initiative builds on what law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents associated with criminal activity—and establishes a standardized process whereby SAR information can be shared among agencies to help detect and prevent terrorism-related criminal activity. (For the latest information on the NSI, please see http://nsi.ncirc.gov/.)

The NSI responds to the NSIS mandate to establish a "unified process for reporting, tracking, and accessing [SARs]."[12] The NSI process, as shown in Figure 7, involves a cycle of 12 steps that responds to the requirements articulated in the NSIS.

The intended outcome is for federal and SLT law enforcement organizations to standardize the way they gather, document, process, analyze, share, and investigate information about suspicious activities that are determined to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism), while protecting privacy and civil liberties as required by federal and SLT laws and regulations.[13]

The NSI is a collaborative effort among a number of stakeholders including DOJ and its components (in particular the Bureau of Justice Assistance and the FBI); DHS and DoD; the PM-ISE; and state and local law enforcement agencies across the nation. A number of major law enforcement organizations—the Criminal Intelligence Coordinating Council (CICC), the International Association of Chiefs of Police (IACP), the MCCA, the National Sheriffs' Association, and the Major County Sheriffs' Association (MCSA)—have also

[12] National Strategy for Information Sharing (NSIS) (October 2007), p. A1-6, 7 available at http://www.ise.gov/docs/nsis/nsis_book.pdf.

[13] *Information Sharing Environment Functional Standard: Suspicious Activity Reporting* (ISE-FS-200) (May 2009), p. 2 available at http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf.

formally endorsed the NSI and been key players in the effort to plan and carry out the ISE-SAR Evaluation Environment and the broader nationwide implementation.

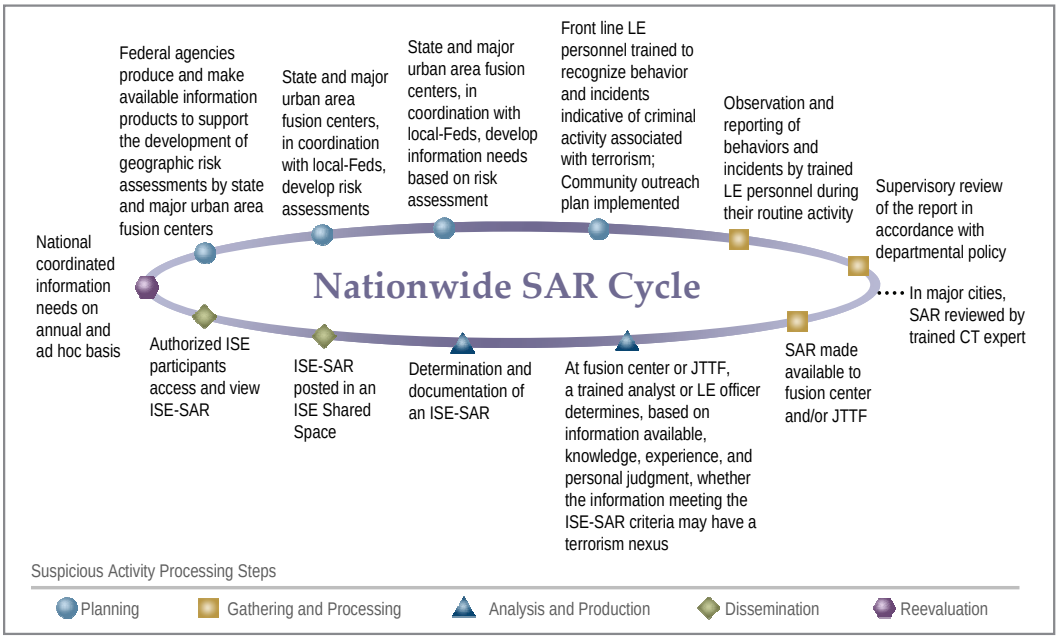



**Figure 7. Overview of Nationwide SAR Cycle**

### 2.2.1 Completion of the ISE-SAR Evaluation Environment

For the last two years, federal, state, and local organizations have developed, tested, and evaluated the policies, procedures, and technology concepts needed to implement a unified SAR process. This ISE-SAR Evaluation Environment was formally concluded in September 2009 and the results were documented in a series of publically available reports.[14] The evaluation environment successfully demonstrated the value of a unified SAR process and showed that agencies could employ different technologies and still participate smoothly in the NSI as long as they adopted common policies and business processes. In this way, the ISE-SAR evaluation environment was able to effectively leverage processes and procedures already in place at participating localities. In most

**2009-10 NSI Highlights**

- ISE-SAR evaluation environment successfully completed;
- FBI's eGuardian system fully integrated into the NSI;
- NSI privacy framework formalized;
- NSI PMO established at BJA; and
- More than 5,000 SLT executives, analysts, and frontline officers from 190 agencies trained to date.

[14] See *Nationwide Suspicious Activity Reporting Initiative: Status Report* (February 2010), available at http://www.ise.gov/docs/sar/NSI_Status_Report_FINAL_2010-02-03.pdf.

cases, participating sites were able to simply modify existing procedures to implement the standard NSI process. To date, more than 4,500 SARs have been posted to ISE Shared Space servers and more than 7,800 federated searches conducted.

The ISE-SAR evaluation environment showed that it is possible to both combat terrorism effectively and protect privacy, civil rights, and civil liberties. The NSI Privacy Framework—an outgrowth of an initial privacy analysis completed in September 2008 enhanced by lessons-learned and best practices from the evaluation environment—was adopted to serve as a foundation of the nationwide implementation.[15] Moreover, although the evaluation environment was focused on SARs that were indicative of terrorism-related crimes, both the steps in the NSI cycle and the data elements in the ISE-SAR Functional Standard are potentially adaptable to other types of criminal behavior.[16]

**Building on Existing Processes**

One large urban police department added a check-box to its existing field interview forms to specifically denote a report as a SAR. This allowed the form to be quickly and easily routed for processing and, more importantly, let the frontline officer use an already-existing, familiar form. The training of the officers—on behaviors potentially indicative of terrorism-related criminal activity and the importance of ensuring that privacy, civil rights, and civil liberties are protected—was the only new element in this process.

The major implementation approach used during the evaluation environment relied on a distributed environment consisting of multiple ISE Shared Space servers at participant locations. Information loaded into the ISE Shared Space servers can be searched, accessed, and displayed by all authorized ISE investigative and analytic personnel to support their counterterrorism missions.

Another technical solution is the FBI eGuardian system. In addition to supporting a broad user base at federal, state, local, and tribal agencies with direct access to the eGuardian system, information entered into eGuardian will be automatically replicated in a separate eGuardian ISE Shared Space server and made available to all authorized NSI participants, regardless of whether or not they have eGuardian accounts. Although eGuardian is based on different technology and provides additional analytic capabilities, its ISE Shared Space server performs are—for information sharing purposes—like all the others. Guidance provided to prospective NSI participants describes both these approaches.[17]

---

[15] Information Sharing Environment – Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis (Volume 1 – September 2008) outlined recommendations for protecting privacy, civil rights, and civil liberties during the evaluation environment. It is available at http://www.ise.gov/docs/sar/ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf.

[16] Ibid. pp. 3-5.

[17] *NSI Technical Implementation Options, Version 1* (March 2010). Available at http://www.ise.gov/docs/sar/NSI_Tech_Impl_Options_Version_1_FINAL_2010-03-09.pdf.

### eGuardian Role in the NSI

eGuardian now serves a user population of 2,226 users representing 718 law enforcement agencies, to include 91 state and 410 local agencies, many of which operate state and major urban area fusion centers; 5 tribal agencies; 109 federal agencies; 28 DoD agencies; and 75 FBI entities. Since its inception, approximately 77 FBI preliminary or full field counterterrorism investigations have been initiated as a result of information provided through eGuardian.

In addition to the ISE-SAR evaluation environment, the DHS Science and Technology Directorate conducted a 2008 SAR Capability pilot on behalf of the Federal Air Marshall Service (FAMS) that explored the use of SAR analytic capabilities tailored to the needs of investigators. A follow-on to the original effort—the Enhanced SAR Analysis Pilot, now underway—aims to develop a structured process for exploring advanced analytic capabilities and build a prototype to support FAMS operations.

### Refining SAR Databases

At the beginning of the ISE-SAR Evaluation Environment, several participants reported holding hundreds or even thousands of legacy SARs considered to be potentially terrorism-related. Sites reviewed their holdings in accordance with terrorism behaviors as described in the ISE SAR Functional Standard and reprocessed the information, significantly reducing the number of reports considered to have a potential nexus to terrorism. One site was able to filter out almost 95 percent of its legacy reports.

## 2.2.2 NSI Training

A well-developed and well-executed training program proved critical to the successful implementation of the SAR process. BJA, working with IACP and MCCA, developed a specialized training program that emphasized the need for privacy, civil rights, and civil liberties safeguards. Members of the privacy, civil rights, and civil liberties advocacy community reviewed and provided valuable input to the three-part curriculum, which included separate courses providing specialized training for three groups: executive-level personnel, frontline officers, and analysts. NSI training strengthens the vetting process so that only those SARs with analytic value are stored and shared, minimizing the amount of information to review and analyze and better protecting privacy, civil rights, and civil liberties. Table 2 summarizes NSI training results as of June 2010.

**Table 2. NSI Training Statistics**

| Course | Number of Deliveries | Number of People Trained | Number of Agencies Represented |
|---|---|---|---|
| **Line Officer** | 4 | 4,006 | 4 |
| **Executive** | 12 | 419 | 12 |
| **Analyst** | 20 | 711 | 242 |
| Total | 36 | 5,136 | 258 |

### 2.2.3 NSI Governance

In December 2009, Attorney General Holder and Homeland Security Secretary Napolitano announced the creation of an NSI PMO to be housed within DOJ and to work in partnership with a Fusion Center PMO at DHS "to enhance information sharing between federal, state, local, and tribal agencies and the private sector."[18] The NSI PMO will facilitate the implementation of the NSI across all levels of government and assist participating agencies in adopting compatible processes, policies, and standards that foster broader sharing of SARs, while ensuring that privacy, civil rights, and civil liberties are protected in accordance with local, state, and federal laws and regulations.[19] The NSI PMO is now up and operating as a part of BJA with the FBI and DHS as full partners. The PMO Director and deputies have been named and additional staff assigned. An implementation plan was completed and submitted to the White House in February 2010 and nationwide implementation is underway.

**Improving the Quality of SARs**

Based on a case that the FBI solved in 2009, a major urban area fusion center refined the list of terrorism behaviors to watch for, updated training material, and briefed airport security personnel in the fusion center's area of responsibility. The result—attributable at least in part to better informed airport security personnel—has been more consistent and higher quality reports of relevant suspicious activity.

### 2.2.4 The DHS "See Something, Say Something" Campaign

In the summer of 2010, DHS launched the first phase of its "See Something, Say Something" campaign and announced a new information-sharing partnership with Amtrak as part of the NSI, highlighting the public's role in keeping our country safe and the Obama Administration's commitment to bolstering surface transportation security.

The "See Something, Say Something" campaign—originally implemented by New York City's Metropolitan Transit Authority and funded, in part, by $13 million from the DHS Transit Security Grant Program—is a simple and effective program to raise public awareness of indicators of terrorism, crime, and other threats and emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities.[20]

## 2.3 Alerts, Warnings, and Notifications (AWNs)

Terrorist-related AWNs are produced by agencies at all levels of government—some in response to explicit statutory or regulatory requirements. They take several forms and may be disseminated through a variety of distribution channels. One of the principle

[18] See http://www.prnewswire.com/news-releases/presidential-task-force-on-controlled-unclassified-information-releases-report-and-recommendations-79312237.html for additional information.

[19] For more information on the NSI PMO, please visit http://nsi.ncirc.gov/default.aspx.

[20] See http://www.dhs.gov/ynews/releases/pr_1278023105905.shtm for additional information.

responsibilities of the Interagency Threat Assessment and Coordination Group, for example, is to facilitate the release of AWNs tailored to the special needs of SLT agencies. To cite another example, an alert capability exists within eGuardian that was successfully used to warn law enforcement agencies of a threatened "Columbine-style" attack in September 2009.

Because of its complexity and the number of agencies involved, there has been limited progress in addressing the need for a broader, better integrated system of AWN. The PM-ISE is reviewing existing processes and developing alternative approaches for addressing the AWN process. It is expected that AWN will be a major focus area for the ISE over the next year.

### 2.3.1 Interagency Threat Assessment and Coordination Group (ITACG)

The ITACG was established at the NCTC to help DHS, FBI, and other agencies produce federally-coordinated terrorism-related information products tailored to the needs of SLT and private sector partners through existing federal agency channels.

The ITACG Detail consists of fire, investigative, tribal, law enforcement, and health first responders that review federally-produced intelligence, including national intelligence threat reporting, for potential interest to state, local, tribal, and private sector partners. The Detail continues to be an effective mechanism for facilitating the dissemination of intelligence products, to which state, local, tribal, and private sector partners may not otherwise have access. The ITACG Detail identified new topics of interest and participated in the preparation of Roll Call Releases (RCRs)—a collaborative DHS, FBI, and ITACG product line, intended to provide "bottom-line" intelligence to "street-level" first responders. These products focus on indicators, tactics, techniques, procedures, and trends related to terrorism, homeland security, and weapons of mass destruction (WMD).

The ITACG Detail is fully integrated into the production processes at DHS, FBI, and NCTC and provides a valuable perspective by identifying topics of interest to state, local, and tribal agencies for consideration by production agencies, and nominating Intelligence Community products to be written or rewritten at the unclassified level or at the lowest possible classification level. The ITACG interacts directly with state, local, and tribal partners during a weekly threat teleconference and bi-weekly video teleconference hosted by DHS. In addition, the Detail also delivers its information sharing message to federal, state, local, tribal, and private sector partners during national conferences, *ad hoc* meetings, and formal training events. These presentations include analyst training at the Defense Intelligence Agency's Advanced Counterterrorist Analyst Course, the DHS Basic and Mid-level Intelligence Terrorism Analysis Course, and the FBI Basic Analyst Course.

**ITACG 2010 Contributions**

Over the last year the ITACG:

- Contributed to the publication of approximately 34 RCRs relating to terrorism, homeland security, and WMD threats;
- Reviewed, provided comments, or proposed language to 403 Intelligence Community products prior to publication by the originating agencies.; and
- Requested downgrading of 78 classified Intelligence Community products.

The ITACG Intelligence Guide for First Responders (Figure 8) was developed by state and local police and firefighters, in coordination with federal intelligence analysts, to assist state, local, and tribal first responders in accessing and understanding federal counterterrorism, homeland security, and weapons of mass destruction reporting. This unclassified guide provides a concise overview of:

- Intelligence and the Intelligence Community;
- The types of intelligence reports available to state, local, tribal, and private sector partners with instructions on how to locate them; and
- An understanding of threat information and estimative language.

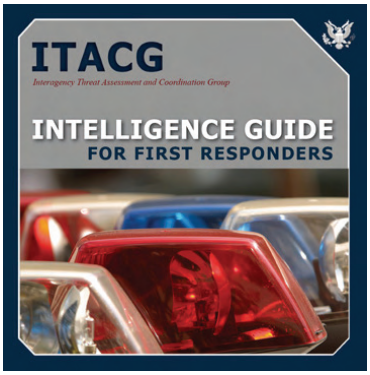



**Figure 8. ITACG Guide for First Responders**

The Intelligence Guide for First Responders has been distributed to each of the more than 48,000 state, local, and tribal police and fire departments in the country and is also available on the Internet (through the Homeland Security Information Network (HSIN), LEO, ISE.gov, and NCTC.gov) for download and reposting.

## 2.4 Cargo and Person screening

### 2.4.1 Cargo Screening

Every year almost 250 million tons of cargo crosses our Nation's land borders or arrives at our airports and seaports where it is then conveyed across our vast and complex maritime, air, rail, and roadway infrastructures. The U.S. Customs and Border Protection performs the massive tasks of administratively screening and physically scanning all cargo in-bound to the United States to detect material that could potentially be used in terrorism-related or other criminal activities. Improved information sharing and collaboration among federal, state, and local homeland security, public safety, and law

enforcement organizations that participate in the screening process can improve efficiency and help prevent potential terrorist attacks.

Accordingly, the PM-ISE is supporting mission partners in their efforts to develop cross-governmental cargo security standards and architectures—built on existing systems—to address terrorism-related secure cargo information access, data distribution, and sharing. As a result, decision makers will be better prepared to detect, prevent, or mitigate terrorist attacks or other criminal behavior.

Because of the magnitude of the task, the first step in this process was to scope the effort to better manage it. An interagency team from DHS, PM-ISE, and the Nuclear Regulatory Commission (NRC) analyzed key business processes and information flows involving nuclear and radiological threat data on inbound cargo transported over land and sea. This analysis identified three major areas where information sharing and collaboration could improve the Nation's defenses against acts of nuclear and radiological terrorism:

- Sharing information on adjudicated radiological shipments;
- Standardized information sharing on general radiological shipments and licenses; and
- Sharing post-seizure analysis and information.

Consistent with assessments and strategies developed through the Trans-border Security Interagency Policy Committee (IPC), these vetted use-cases will now be used to define the requirements and data elements necessary for developing new cargo screening functional standards for the ISE.

### 2.4.2 Improved Person Screening Using Biometrics

Historically, the person screening process has relied largely on name recognition through the use of watchlists. Given the inherent problems with spelling and duplication that inevitably occur with name-based screening, the Federal Government, the private sector, and partner nations are working to modernize and improve personal identification, authentication, and access control through the use of biometrics. Extensive biometric screening research and technology supports these mission areas, through the use of face, finger, and iris recognition modalities.

The National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management led an interagency effort to develop the *NSTC Policy for Enabling the Development, Adoption and Use of Biometric standards*, and an associated *Registry of U.S. Government Recommended Biometric Standards*.[21] This effort ensures that common biometric standards are adopted across all federal systems, that they support interoperability, and that they are potentially extensible to non-federal partners and systems. By participating in these efforts during the development stage, the PM-ISE and our partners can plan for the development of interoperable ISE standards support and improve the accuracy and reliability of person screening processes.

[21] Both documents are available at http://www.biometrics.gov/standards/.

The use of biometrics is expanding at the SLT level as well. Law Enforcement agencies in the National Capital Region can now use a handheld tool to wirelessly access biometric data and arrest history. This project integrates two regional information-sharing programs—the National Capital Region Automated Biometric Identification System project and the National Capital Region Law Enforcement Information Exchange. The Biometric Identification System project takes an unknown subject's fingerprint and compares it wirelessly against the database of biometric information. The Law Enforcement Information Exchange system provides search tools to allow local, state, and federal law enforcement agencies to access data on arrests, booking information, citations, and other important law enforcement information.

The project, which was supported by a DHS grant, allows officers to access information from both systems using the handheld tool. This gives law enforcement the ability not only to recognize suspects who lack identification or who may be attempting to mask their identities, but to also determine arrest history and other useful information.

### 2.4.3 National Targeting Center-Passenger (NTC-P)

The NTC-P is responsible for coordinating DHS Customs and Border Protection (CBP) field-level activities related to anti-terrorism efforts and plays a vital role in the identification of individuals who pose a national security concern at 327 U.S. ports of entry and over 30 Border Patrol checkpoints throughout the U.S. The NTC-P is the CBP focal point for all possible Terrorist Screening Data Base (TSDB) encounters with CBP field entities and is the primary contact between CBP field offices and other government agency case agents on all positive TSDB encounters.

NTC-P uses several automated enforcement data processing systems which are focused on detecting and preventing terrorist access to the United States including the Automated Targeting System-Passenger and the Intelligence Operations Framework System. These systems allow NTC-P to screen passenger manifests and related information prior to a passenger's arrival in the United States and to respond to terrorism related alerts and provide time sensitive research and support on any issues related to international passengers and travel at and between U.S. ports of entry.

The Center is a part of the CBP layered approach strategy to homeland security by pushing U.S. borders outward and attempting to interdict possible terrorists and other mala fide travelers before they can board a U.S.-bound. NTC-P has on-site liaison officers from the FAMS, ICE, TSA, the Department of State, and the Citizenship and Immigration Service Fraud Detection and National Security Division.

## 2.5 Terrorist Watchlists

In response to the Christmas Day incident on Northwest Flight 253, the National Security Staff led an effort to develop updated watchlisting guidance that includes improved business processes and rules. The Transportation Security Administration (TSA) completed the deployment of *Secure Flight*, an aviation security program that enhances the security of domestic and international commercial air travel through the use of improved watchlist matching.

The basic information flow diagram for the Consolidated Terrorist Watchlist Nomination and Export business process is shown in Figure 9. The Terrorist Screening Center (TSC) has several initiatives completed or underway to improve the way that terrorist watchlists are processed and shared. The TSC export to DHS's Secure Flight program was implemented in the NIEM-compliant Terrorist Watchlist Person Data Exchange Standard (TWPDES). Since late 2009, TWPDES has been used daily to share the list of No-Fly and selectee-designated Known or Suspected Terrorists (KSTs) for screening of airline passengers. TSA officers, not aircraft operators, vet passengers against the U.S. Government's terrorist watchlist using passenger name, date of birth, and gender as key identifiers before a boarding pass is issued—fulfilling a key recommendation of the 9/11 Commission Report and IRTPA. Under this program, more than 99 percent of passengers will be automatically cleared, thereby facilitating travel, while enhancing watchlist matching processes.

Through the leadership of PM-ISE and the ODNI, and with the support of DHS and FBI, TWPDES is now available as an unclassified XML standard with no prohibitions on dissemination. As a result, international partners and vendors can now freely access and develop software that is consistent with this NIEM-compliant XML standard for data sharing. TWPDES is also compliant with the American National Standards Institute (ANSI) and the National Institute for Standards and Technology (NIST).

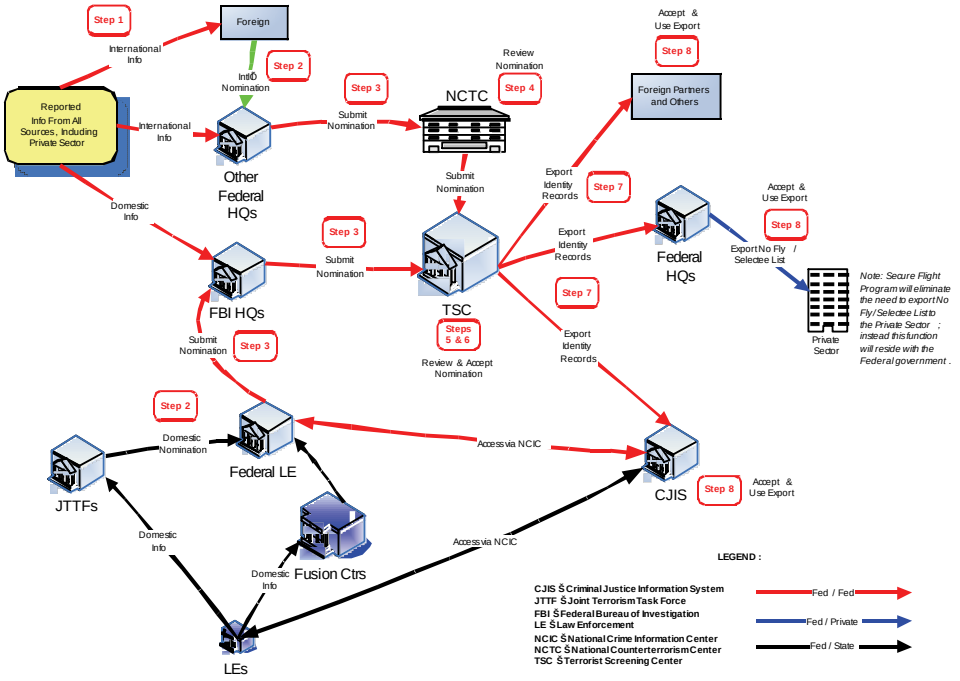



**Figure 9. Consolidated Terrorist Watchlist Nomination and Export Information Flow Diagram**[22]

[22] Please see appendix E of *ISE Enterprise Architecture Framework, Version 2.0* (October 21, 2008) available at http://www.ise.gov/docs/eaf/ISE-EAF_v2.0_20081021.pdf for more information.

In late 2009, BJA, supported by DHS and TSC, completed the development of an "encounter service" that provides 85% of the documentation, code base, and protocols to complete the installation of the service at any state or major urban area fusion center. This service allows federally recognized fusion centers to share positive KST encounter data with both TSC and other centers to support analysis and information sharing about terrorist activities. Using TWPDES makes it easier for fusion centers to provide the software products and documentation necessary to implement a robust, NIEM-compliant data exchange.

As of June 22, 2010, the Secure Flight program was fully implemented for 100 percent of flights by U.S. aircraft operators. This accounts for more than 90 percent of all travel to, from, and within the United States. All foreign air carriers are expected to implement Secure Flight by the end of 2010.

In addition to supporting the Secure Flight Program, TSC has designed two additional information sharing initiatives that will have significant impact on the way watchlists are developed and shared once they are fully implemented:

- The Department of State (DoS) will import a TWPDES 3.0 upgrade in Fall 2010. This product will provide all of the necessary data for biometric and biographic screening of KSTs in one record and within a single export. Maintaining the integrity of the record's biographic and biometric data will reduce the likelihood of errors in data integrity while providing analysts with more complete information.
- TSC has also designed and will implement an export for our international partners using NIEM and TWPDES. Once implemented, this export will allow for freer and higher quality exchanges of watchlist information with our closest partners.

These two enhancements will provide richer data feeds, higher quality information exchanges, and increased flexibility to members of the screening community in modernizing their business processes and practices to better deal with a threat such as the one posed by the Flight 253 incident.

**Improved Sharing of Watchlist with Fusion Centers**

Fusion centers are now able to use a standards-based solution for receiving information on positive hits against the TSC Watchlist thanks to the recent completion of the "TSC Encounter Information Service Specification Package (SSP)." This SSP—tested during a pilot project at five fusion centers—was complies with the Justice Reference Architecture (JRA) services model, and was presented in conjunction with three other SSPs recently completed for use by fusion centers.

## 2.6 Sharing with the Private Sector

The National Strategy for Information Sharing recognizes the importance of private sector involvement in the ISE, particularly critical infrastructure owners and operators. Consequently, the PM-ISE, working with DHS and other stakeholders, confirmed that the

Critical Infrastructure and Key Resources Information Sharing Environment (CIKR ISE) would be fully integrated into the national ISE. The CIKR ISE provides a unifying, integrated framework for stakeholders from all levels of government and critical infrastructure owners and operators to communicate, coordinate, and collaborate through the efficient exchange of timely and useful information pertinent to their shared mission of protection and resiliency. Recent accomplishments in private-sector sharing include:

- The Transportation Sector Information Sharing and Analysis Center content portal was established to provide tactical and planning functionality for sharing suspicious activity reports, situational awareness, and terrorism analysis affecting the Transportation Sector;
- The Healthcare and Public Health Sector adopted the CIKR ISE as the centralized information sharing capability for all its critical infrastructure initiatives and programs;
- The Food and Agriculture Sector integrated Food Shield and the Homeland Security Information Network-Critical Sectors (HSIN-CS), the technical platform supporting the CIKR ISE, into a unified information sharing environment for the Sector; and
- The collaboration tool within the CIKR ISE on HSIN-CS was used over the past year to host over 25 educational events for approximately 17,000 critical infrastructure stakeholders. Valuable information was provided to participants on topics such as CIKR resilience and threat detection.[23]

## 2.7 Sharing with International Partners

Combating violent extremism is not only a U.S. concern. Our allies and partners have also suffered the devastating effects of terrorist attacks and, as the events of the last year show, the plans for future attacks may originate far from the ultimate target. Accordingly, robust and regular two-way information sharing and collaboration with international partners continue to be cornerstones of our effort to thwart terrorist attacks. Last year, agencies continued to use the *Checklist of Issues for Negotiating Terrorism Information Sharing Agreements and Arrangements,* a tool that includes a list of issues for agencies to consider when negotiating terrorism-related information sharing agreements with foreign partners.

Dealing with non-U.S. counterparts is largely done on a community, rather than an ISE-wide basis. Typically communities or agencies work directly with their foreign counterparts to put effective agreements in place and maintain those though regular contacts and information exchanges. The Intelligence Community, for example, has long had close bilateral or multilateral arrangements with partners around the globe while the FBI's Legal Attachés (LEGATs) have forged close ties with law enforcement counterparts abroad.

[23] See http://www.dhs.gov/files/programs/gc_1189168948944.shtm for additional information.

As of July 2010 the Department of State and the TSC have concluded non-binding arrangements or formal agreements with 18 foreign partners encompassing commitments for the reciprocal exchange of terrorism screening information pursuant to Homeland Security Presidential Directive-6. TSC provides our foreign partner with access to a subset of the Terrorist Screening Database in exchange for a list of known or suspected terrorists from our foreign partner. The State Department leads the diplomatic outreach for the HSPD-6 initiative and conducts negotiations jointly with the TSC, the implementing agency.

**Need for Strong International Partnerships**

We're working closely with our international partners to make sure that we address any weak links—so that a terrorist can't exploit a security gap in one country to gain access to the entire global aviation network … We're also working to secure strong international agreements so that all of our allies and international partners can benefit from one another's intelligence about known terror suspects. This goes beyond aviation security as well. We're using the logic of information-sharing and threat-based protocols to implement a smart, strategic approach to passenger and cargo screening at our sea and land ports as well.

— Secretary Janet Napolitano

### 2.7.1 U.S.-E.U. Declaration on Counterterrorism

A hallmark achievement in international collaboration was the adoption by the U.S. and the European Union (E.U.) of the *2010 Declaration on Counterterrorism*, in which the U.S. and the E.U. seek to forge a durable framework to combat terrorism within the rule of law.[24] The Declaration stresses that an effective and comprehensive approach to diminishing the long term threat of violent extremism is a vital component of U.S. and E.U. efforts to combat terrorism. It highlights efforts of both parties to foster information sharing and cooperation in the prevention, investigation, and prosecution of terrorism-related offenses, emphasizing cooperation in border security, countering terrorist financing, enhancing the global non-proliferation regime, and promoting the counterterrorism work of the United Nations.

"The Council's adoption of this [U.S.-E.U.] Declaration is a crucial step forward in our mutual fight against terrorism. … [It] demonstrates our joint commitment to protect our citizens from terrorism consistent with our laws, our values, and our commitment to individual privacy. Our work with our E.U. partners to protect the security of our citizens is critical to the success of our counterterrorism efforts."

— Attorney General Eric Holder

[24] A copy of the declaration is available at http://www.europa-eu-un.org/articles/en/article_9814_en.htm.

### 2.7.2 The Global Enrollment System (GES)

The Global Enrollment System, which provides expedited travel for pre-approved, low risk travelers through dedicated lanes and kiosks, is the system of record for U.S. Trusted Traveler Programs. GES interacts with similar systems from several foreign countries, including Canada and the Netherlands. Sharing with these external systems had previously been done using custom services that were built using message formats unique to each bilateral relationship.

Use of NIEM is critical to the deployment of GES for a variety of reasons, including its unambiguous specification of all elements in any interchange. Future interfaces with international systems will also use this interface, and the intent is that, over time, legacy interfaces will also be made NIEM-conformant. This will ensure that all data exchanges will have the same, well-defined meaning and that development and maintenance costs will be reduced.

The U.S. is currently working with Mexico to allow Mexican citizens to enroll in the Global Entry Trusted Traveler Program. Automated kiosks are designed to process pre-approved, low-risk international travelers who qualify. GES is leveraging and extending its existing NIEM-conformant schema to create a generic, reusable web services interface with Mexico. Mexican citizens who apply to Global Entry will be required to be vetted by Mexico as well as by the U.S. GES will provide enrollment information to Mexico via the NIEM-conformant web interface; and Mexico will, in turn, provide the vetting status using the same interface.

### 2.7.3 Aviation Security and the Air Domain Awareness (ADA) Initiative

The 2010 National Security Strategy places a high priority on aviation security calling for, "increased information collection and sharing, stronger passenger vetting and screening measures, the development of advanced screening technologies, and cooperation with the international community to strengthen aviation security standards and efforts around the world."[25] The PM-ISE is supporting the National Strategy for Aviation Security and the Air Domain Awareness Initiative in building a multi-layer aviation security network intended to secure the people and interests of the United States. Interagency integration will lead to shared situational awareness to help mitigate threats associated with the air domain, both nationally and internationally. The PM-ISE will specifically support the Air Domain Awareness Board, under the Trans-border IPC, by working with the ADA Governance, Capabilities and Resources, and Information Sharing Working Groups to implement proven ISE mission processes to integrate aviation security initiatives into a unified national effort.

### 2.7.4 National Law Enforcement Telecommunications System (NLETS) and INTERPOL-Washington

Effective collaboration depends heavily on efficient communications. The National Law Enforcement Telecommunications System provides two basic capabilities to its users. First, it is an international, computer-based message-switching system that links

[25] *National Security Strategy* (May 2010), p. 20.

together state, local, and federal law enforcement and justice agencies for the purpose of information exchange. Second, it provides information services support for a growing number of justice-related applications. NLETS not only has a national impact but an international one as well since it supports the efficient, secure, and accurate exchange of intelligence across jurisdictional and technological boundaries.

### Information Sharing Through INTERPOL

INTERPOL Red Notices are international wanted notices that provide information on the identification of fugitives who are the subjects of arrest warrants and are wanted for prosecution or to serve a sentence for serious offenses. They are issued by INTERPOL, the International Criminal Police Organization, at the request of member countries in order to seek the location of fugitives for the purpose of extradition. The country issuing a Red Notice commits to seeking the provisional arrest and extradition of the fugitive in question should he or she be located. Red Notices typically produce fast responses. In one example, a Red Notice issued by the U.S. on November 17, 2009 resulted in an arrest 10 days later in Bulgaria.

Through a direct partnership with INTERPOL-Washington, a component of DOJ's U.S. National Central Bureau, the NLETS network allows U.S. law enforcement agencies to query INTERPOL information provided by its 188-member countries. This access allows federal, state, local, and tribal law enforcement agencies to obtain and share international investigative information related to persons, travel documents, and vehicles. INTERPOL-Washington also facilitates the exchange of criminal investigative information with the foreign law enforcement agencies of INTERPOL member countries through INTERPOL's secure network, referred to as I-247. For additional information on NLETS, please see http://www.nlets.org/.

## The NSI — The ISE in Action

Last year an employee at a self-storage facility noticed something unusual. A group of men had begun to meet frequently around a storage unit—as many as 20 or 30 times in the span of a few days—and were very careful to conceal their property by backing their SUV right up to the storage unit door. The self-storage facility had recently received information on indicators of suspicious activity as part of the NSI. The employee contacted local police. Local police ran checks and found that the FBI had an active investigation and the individuals were under surveillance. Two weeks after the employee's report, the FBI arrested four men on a number of terrorism charges, including charges arising from a plot to detonate explosives near a synagogue and to shoot military planes with Stinger surface-to-air guided missiles.

---

Shortly after attending training on the agency SAR process, a Los Angeles motorcycle officer observed a traffic violation, issued a citation, and impounded the vehicle. The officer then contacted the agency's Major Crimes Division and inquired about completing a SAR based on an expired international driver's license and the unusual level of anxiety expressed by the driver. After receiving the information, detectives conducted a follow-up investigation and discovered the information was of interest to the FBI, resulting in a further investigation.

---

A contract background Investigator for the DoD, telephoned the FBI's Threat Investigation Division office to report a suspicious vehicle. According to the investigator, the vehicle was moving so slowly that she almost had to come to a complete stop behind the car before she could safely pass. The investigator described the vehicle and reported that the driver appeared to be taking video footage of a military base using a telephoto lens. This information was received by a JTTF—through eGuardian—from Pentagon Force Protection. A trace of the license plate revealed that the subject of the incident had been involved in a pre-existing investigation.

---

In February 2010, the FBI's Internet Tip website received information that an identified soldier had made threatening comments about his National Guard Unit over a social network. This incident was uploaded into eGuardian and shared with the appropriate FBI Field Office and the U.S. Army Criminal Investigation Command. The matter is now the subject of a joint Army-FBI investigation.

---

In January 2010, a line officer at the Los Angeles Police Department, an ISE-SAR Evaluation Environment site, discovered a store owner who was selling illegal cigarettes, brass knuckles, counterfeit name-brand purses and wallets, and drug paraphernalia. While conducting a search at the store, LAPD officers observed a bomb-making recipe taped to the wall. Subsequently, the store owner was arrested, the recipe was determined to be a viable bomb-making formula, and an investigation into possible terrorism financing is ongoing.

SECTION 3

# ISE CORE CAPABILITIES

> "We are improving information sharing and cooperation by linking networks to facilitate federal, state, and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate. We are coordinating better with foreign partners to identify, track, limit access to funding, and prevent terrorist travel."
>
> — National Security Strategy, May 2010, Page 20

Although end-to-end mission processes form the heart of the ISE, they depend on the availability of core ISE capabilities that cut across multiple missions. Fusion centers, for example, play important roles in almost all of the mission processes. Furthermore, achieving interoperability across multiple SBU/CUI networks will contribute significantly to improving processes supporting suspicious activity reporting and alerts, warnings, and notifications.

## 3.1 National, Integrated Network of State and Major Urban Area Fusion Centers

The ability to analyze and quickly draw appropriate inferences from multiple and sometimes disparate information sources lies at the heart of the challenge the ISE was established to address—to provide the right information to the right people in time to prevent terrorist attacks and to protect our people and our institutions.

In the aftermath of 9/11, states and localities acted independently to create and invest in fusion centers, developing local and regional capabilities that previously existed only at the federal level. The 72 designated fusion centers include one fusion center designated by each state, for a total of 50 state-designated fusion centers (primary designated centers). The Governor of each state designated his or her primary state fusion center, ensuring each state had the most appropriately located center for the unique needs of the state. The 22 additional centers were chosen for their support of major urban areas, as well as in order to cover a broad geographic area, including the border regions.

The list of 72 centers was agreed upon collectively by the former National Fusion Center Coordination Group, which included participation from the ODNI, DHS, the FBI, DOJ/BJA, and SLT partners. The Federal Government did not dictate where centers should be built and maintained, nor will it discourage the creation of new centers, although federal support beyond the 72 designated centers is not programmed in the coming years.

The primary state-designated center serves as the hub of information sharing within states that have multiple centers. That primary state-designated center is responsible

for ensuring that information is passed from the Federal Government to those entities within the state that require that information. This geographic dispersal and system of primary and additional centers in states is aimed at eliminating redundancy and ensuring consistent coverage and support.

Fusion centers serve as the primary focal points within the state and local environment for the receipt, analysis, and sharing of all-crimes/all-hazards information and, in turn, provide federal agencies with critical state and local information and subject-matter expertise—enabling the effective communication of locally generated terrorism-related information. Consequently, the Federal Government has actively supported state and local efforts to establish and maintain fusion centers. In particular, development of a *National Integrated Network of State and Major Urban Area Fusion Centers* has been a vital part of the effort to build the ISE since its inception.

### 3.1.1 Fusion Center Governance

Considerable progress has been made over the last year not only in better supporting fusion center operations, but also in institutionalizing the Federal Government's role by taking steps that will eventually lead to a more sustainable model for fusion center support. In a December 17, 2009 memorandum, the Assistant to the President for Homeland Security and Counterterrorism directed DHS "to coordinate support for a growing network of state and major urban area fusion centers." Secretary Napolitano agreed to establish a multiagency program management office, and the Department is bringing together multiple federal agencies and representatives of state, local, tribal, and territorial governments to provide effective, efficient, and coordinated support to designated fusion centers. Working with stakeholders, DHS developed an implementation plan for the PMO and is in the final stages of establishing the office. The FBI has designated a senior FBI employee with significant fusion center experience to serve full time as Deputy Director once the multiagency PMO is fully established.

**2009-10 Highlights**

- DHS developed implementation plan for multiagency PMO;
- Critical Operational Capabilities Strategy developed;
- Progress made in integrating tribal governments into fusion centers;
- Baseline Capabilities Assessment pilot completed and nationwide assessment begun; and
- Fourteen fusion centers have approved ISE privacy policies, with another 47 in the draft stages.

### 3.1.2 Baseline Capability Assessment

As a result of discussions among key federal partners and fusion center directors at the 2010 National Fusion Center Conference, it was agreed to move forward with the implementation of a Critical Operational Capabilities Strategy for fusion centers. This strategy is focused on identifying and addressing the capabilities essential to ensuring

effective information sharing between the Federal Government and SLT partners during crises or emergencies. The implementation of this strategy consists of four distinct steps:

- Assessing fusion center capabilities;
- Prioritizing the actions needed to sustain critical operational capabilities;
- Leveraging and focusing resources on those priorities; and
- Identifying the additional resources necessary to achieve baseline capabilities and sustain operations over the long term.

In the summer of 2009, DHS and PM-ISE jointly conducted a Baseline Capabilities Assessment pilot in three states to help finalize the methodology and tools for the Nationwide Baseline Capabilities Assessment now underway. The full nationwide assessment began in April with the issuance of an on-line questionnaire to guide self-assessments by fusion center directors. The second phase, on-site validation by joint PM-ISE, DHS and FBI teams, began in June and will conclude in September 2010.

DHS, in coordination with the FBI and other federal partners, will leverage the baseline capability assessment data to establish strategic priorities and help identify any gaps in capabilities at individual fusion centers and across the national network. Moreover, partners at all levels of government will gain valuable information for planning investments and allocating resources that will help achieve and sustain baseline capabilities at individual fusion centers and across the network.

### 3.1.3 Access to Classified Systems

Providing SLT access to Secret-level classified systems is an essential ISE capability. A number of fusion centers already have access to the FBI Secret-level network (FBINet) or the Homeland Secure Data Network (HSDN). In addition, a joint DoD-DHS initiative allows cleared, authorized state and major urban area fusion center personnel access via HSDN to specific classified terrorism-related information stored on DoD's Secret Internet Protocol Router Network (SIPRNet).

Responding to a task from the National Security Staff in October 2009, PM-ISE completed a study of the current state of fusion center connectivity to federal Secret networks.[26] The study found that, while there are no technical barriers to Secret connectivity for fusion centers, there are a number of issues that must be addressed to achieve sustainable connectivity and access. One key recommendation identified the need for consistent processes for planning and operations and a consistent security management framework for coordinating, managing, and overseeing fusion center access to and protection of classified systems. As a follow-up to the analysis, PM-ISE is working with Chief Information Officers (CIOs) from federal agencies operating Secret-level networks to develop a proposed way-ahead for the federal Secret enterprise.

Later this summer the NCTC will deploy a new version of its NCTC-Current capability. NCTC-Current serves as a one-stop shop for the counterterrorism community at the Secret-level with the look and feel of an online newspaper. It provides finished

[26] The study has been completed and will be briefed to the NSS and other stakeholders in August 2010.

intelligence on CT topics and situational awareness reports from multiple sources. The primary audience includes DoD, DHS, FBI, and state and major urban area fusion centers.

### 3.1.4 Tribal Participation in Fusion Centers

Two ongoing collaborative efforts—one involving the East Valley Gang and Criminal Information Fusion Center and the Salt River Pima-Maricopa Indian Community and the other between the Arizona Counterterrorism Information Center (ACTIC) and the Tohono O'odham Nation—have demonstrated the potential value of establishing close working relationships between tribal agencies and fusion centers.

The Tribal Working Group of the Senior Level Interagency Advisory Group (SLIAG) is developing a Fusion Center Tribal Implementation Guide consistent with national policy on consultation and coordination with tribal governments. The Guide will include success stories and best practices and will provide guidance on integrating tribal agencies into fusion centers along with criteria for assessing progress.

**Tribal-Fusion Center Collaboration – A Success Story**

In May 2010 a task force led by the Tohono O'odham Tribal Police broke up a major Southwest U.S. cocaine ring. The operation—conducted in conjunction with agents from the U.S. Border Patrol, U.S. Immigration and Customs Enforcement, the Bureau of Indian Affairs, the FBI, the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the ACTIC, the Pinal County Sheriff's Office, and the Tempe Police Department—resulted in the arrest of 10 individuals and the seizure of weapons, cash, vehicles, cocaine, and other drugs.

### 3.1.5 Critical Infrastructure Protection

The DHS Office of Infrastructure Protection (IP) is working with fusion centers to identify their information sharing needs and requirements and to provide them with Federal critical infrastructure protection and resilience resources. Over the past year, two portals were deployed: one in the Northern California Regional Intelligence Center and the other in the Northern Nevada Counterterrorism Center, which provides critical infrastructure owners and operators the capability to obtain locally-significant information. Thirteen additional fusion centers are in the process of incorporating this capability as well. To accomplish this, DHS IP coordinated with the DHS Office of Intelligence and Analysis to develop a consolidated suite of relevant resources, tools, and products—referred to as "IP-in-a-Box"—with fusion center stakeholders. This toolkit, which was piloted in five fusion centers, included a number of analytic and geospatial tools and support as well as critical infrastructure training courses.

### 3.1.6 Other Fusion Center Accomplishments

There has been significant progress made in assessing fusion center capabilities and in making fusion center operations more sustainable. For example,

- DHS is in the process of establishing an internal joint fusion center office to coordinate and integrate all DHS activities supporting state and major urban area fusion centers, and work closely with the multiagency PMO to ensure a seamless Federal Government support effort;
- The DHS Federal Emergency Management Agency (FEMA) revised State Homeland Security Grant Guidance to tie the use of DHS grant funds to fusion center progress in achieving baseline capabilities;
- Over the last year, the number of DHS analysts deployed to fusion centers increased by more than 50% from 36 to 62, and the FBI now has 74 personnel assigned to 38 fusion centers;

**FBI Fusion Center Engagement Strategy**

The FBI developed and began implementation of a Fusion Center Engagement Strategy based on shared common mission alignment and mutual benefits of enhanced relationships between field offices and fusion centers. Closely coordinated with PM-ISE and DHS, this Strategy was designed to help FBI standardize language and the engagement definition process. By the end of Fiscal Year 2010 all 56 field offices will have conducted a self-assessment of their relationship with the 72 approved fusion centers, providing a comprehensive understanding of how the FBI is currently engaged with fusion centers and joint field office-fusion center visions as to how their relationships can be enhanced.

- The FBI negotiated Joint Duty Credit for personnel assigned to fusion centers and is modifying the career path for FBI intelligence analysts to include assignment to fusion centers; and
- DHS conducted Privacy, Civil Rights, and Civil Liberties "Train the Trainer" sessions for designated fusion center privacy officials at 2010 regional fusion center conferences. DHS will provide ongoing support and assistance to the fusion center Privacy Officers in developing privacy, civil rights, and civil liberties training curriculums for fusion center personnel.

## 3.2 State, Local, and Tribal Information Needs

The NSIS directed the U.S. Government to "facilitate the exchange of coordinated sets of requirements and information needs across the federal and non-federal domains to help guide the targeting, selection, and reporting of terrorism-related information."[27] In July 2009, the NCTC—in coordination with the ODNI, DHS, FBI, and state, local, and tribal partners—produced the first consolidated national set of enduring, terrorism-related information needs that included inputs from SLT partners.

[27] NSIS, p. 11.

These terrorism-related information needs broadly define the types of information needed by federal, state, local, tribal, and private-sector partners for counterterrorism efforts and inform the production and dissemination of both time-sensitive and strategic information and intelligence products to SLT and private-sector partners. The involvement of fusion centers ensures that SLT inputs are represented in the authoritative list of information needs used by the counterterrorism community. The identification and sharing of terrorism information needs (TINs) also supports the NSI by providing "… a mechanism for state, local, and tribal agencies to input terrorism information needs and provide for annual review, revision, and sharing of CT information needs across all levels of government."[28]

In a separate but related effort, DHS has put in place an integrated process for documenting Standing Information Needs for the Homeland Security Community of Interest. This process has been under development for several years and uses a standard methodology which includes a questionnaire and template to assist in capturing SLT needs as well as those of DHS components and other agencies. The methodology—adjusted to accommodate the additions of SLT members—allows states to follow a common template that will also align SLT needs with those of other community members. The 2010 update to the baseline, currently in the review process, will contain the essential elements of information submitted by as many as 20 states. This version also incorporates the NCTC TINs, providing states with a single vehicle for reporting and information needs.

## 3.3 Improved Handling and Sharing of Controlled Unclassified Information (CUI)

Although a certain amount of terrorism-related information will always have to be classified, as much as possible should be handled as CUI (previously known as SBU). Because of this, improving the way that CUI information is marked, handled, and shared is an important priority for the ISE. This subsection discusses two independent but related activities. One is the effort—under the leadership of the National Archives and Records Administration (NARA)—that is focused on the marking and handling of CUI information; the other is an initiative to promote interoperability of information systems and networks that process, store, and share SBU/CUI.

### 3.3.1 Implementing the CUI Framework

Rules and practices for marking, handling, and sharing SBU information were formerly administered through *ad hoc* policies and procedures that varied widely from one federal agency to another. Stakeholders were governed by different agency-specific rules that often caused confusion and inconsistent handling and protection of important information. A May 2008 Presidential Memorandum designated NARA as the Executive

[28] *Nationwide SAR Initiative Concept of Operations*, Version 1 (December 2008) available at http://www.ise.gov/docs/sar/NSI_CONOPS_Version_1_FINAL_2008-12-11_r5.pdf.

Agent responsible for implementing a government-wide framework for CUI. In turn, the Archivist of the United States established the CUI Office to accomplish this task.[29]

Over the following year, the CUI Office consulted with federal agencies through a CUI Council to draft implementing directives on the appropriate designation, marking, safeguarding, and dissemination of CUI. The CUI Office also established and convened an *ad hoc* committee to address the specific information sharing needs of SLT partners and conducted extensive outreach efforts to keep public advocacy groups informed.

**2009-10 CUI/SBU Highlights**

- CUI Task Force report approved and released;
- Basic CUI training being developed;
- SBU/CUI Interoperability requirements developed with inputs from publically accessible website; and
- Quick win initiatives to promote SBU/CUI interoperability developed and launched.

On December 15, 2009, Homeland Security Secretary Napolitano and Attorney General Holder jointly released the Report and Recommendations of a Presidential CUI Task Force that had reviewed current SBU practices and made 40 recommendations on implementing a comprehensive CUI policy.[30] This report was a resounding endorsement of the ongoing CUI effort and included a specific recommendation for expansion of the CUI policies beyond the original terrorism-related information scope.[31] Currently, the report's recommendations are being reviewed and work is underway to further develop the policies and procedures necessary for moving forward on CUI implementation. The CUI Office has also hosted inter-agency and open government meetings to solicit a variety of perspectives on CUI policy efforts.

To provide information-sharing partners with a clear, consistent introduction to CUI, the CUI Office is developing a basic CUI awareness training module and additional, more specific training for the CUI audience.

### 3.3.2 The SBU/CUI Interoperability Initiative

Much of the information critical to counterterrorism and homeland security professionals is protected on multiple SBU/CUI networks such as LEO, RISS (or RISSNET), HSIN, and the unclassified domain of the IC's Intelink system (Intelink-U). Responding to a White House priority, PM-ISE, DOJ, DHS, and the ODNI joined with state, local, and tribal partners on a major new endeavor—the SBU/CUI Interoperability Initiative. This

[29] Presidential Memorandum for the Heads of Executive Departments and Agencies on "Designation and Sharing of Controlled Unclassified Information (CUI)," May 07, 2009 available at http://www.ise.gov/docs/guidance/May_9_2008_WH_Memorandum_CUI.pdf.

[30] Presidential Memorandum for the Heads of Executive Departments and Agencies on "Classified Information and Controlled Unclassified Information," May 27, 2009.

[31] The joint press release and full report can be found at http://www.dhs.gov/ynews/releases/pr_1260887995817.shtm.

effort is developing strategy, architecture, implementation plans, and security and privacy guidelines to establish and maintain a federated, interoperable environment of multiple SBU/CUI networks. Some of the highlights of this Initiative included:

- Developing an SBU/CUI Interoperability Initiative Segment Architecture, consistent with the federal Segment Architecture Methodology that provides a compilation of business processes and functions, services, data, and technology drivers necessary for aligning and harmonizing SBU/CUI networks in the ISE Core;
- Developing implementation plans for near-term efforts to improve the interoperability of the four networks that include cross-network data sharing, protected electronic mail, shared user and service directories, shared services, and cooperative help desk support; and
- Partnering with the Federal CIO Council to standardize user access approaches through common identity credentials.

## Integrating the Front Line —SBU Interoperability

Beginning with the passage of the Computer Security Act of 1987 and continuing today, there has been a recognized need to both protect and share sensitive, unclassified information stored on and disseminated electronically from U.S. Government information systems. The dilemma posed by Sensitive But Unclassified (SBU) information—now renamed Controlled Unclassified Information (CUI)—is how to enforce the controls necessary to protect sensitive information and the privacy, civil rights, and civil liberties, of individuals, while also providing efficient access to the information that the Nation's law enforcement, homeland security, and national security officials need to do their jobs.

Multiple SBU/CUI networks, portals, and systems currently exist with overlapping customers and content. The overarching requirement is for a federal, state, local, and tribal law enforcement officer/analyst to log-in once and be granted access to an interoperable and protected SBU/CUI environment, regardless of who owns the underlying systems.

Although this effort is also setting the foundation for a more robust, longer-term implementation based on common architecture and standards, the current focus is to address short-term needs through a series of "quick win" initiatives using LEO, RISS, HSIN, and Intelink-U as the platforms. An initial set of activities, scheduled for completion through summer 2010, include:

- *Gathering User Requirements.* By analyzing input gathered from a publically accessible website, this effort has identified almost 125 unique requirements that will form the basis for longer-term progress.
- *Improving Network Usability for Frontline Personnel.* The four participants will ensure that key capabilities (Search, Quick Links, White Pages, and e-mail) are visible on the network home page of each system.
- *Sharing User and Service Directories*. The four networks are working to provide each other with their user directories providing the foundation for an integrated, cross-network set of directories to help users more easily locate individuals or capabilities.
- *Expanding Access to FBI Virtual Command Center*. Intelink-U, RISS, and HSIN have announced the availability of this service to their user base and LEO has demonstrated the ability to establish a virtual command center in near-real time.
- *Broadening Use of Protected e-mail*. The four systems have already exchanged e-mail routing information and will adopt an email awareness package that warns users of the potential for email to be sent in the clear over the open Internet.
- *Improve Access to Help Desks*. The networks are taking steps to simplify the way that users obtain assistance on the four systems. RISS has developed a procedural guide and Intelink is assembling a single presentation to be shared among all help desks.

Together, these initial joint deliverables provide meaningful interoperability and end user capability to the frontline.

SECTION 4

# ISE ENABLERS

> The United States Government has an obligation to make the best use of taxpayer money, and our ability to achieve long-term goals depends upon our fiscal responsibility. A responsible budget involves making tough choices to live within our means; holding departments and agencies accountable for their spending and their performance; harnessing technology to improve government performance; and being open and honest with the American people.
>
> — *National Security Strategy*, May 2010, Page 34

ISE mission processes and core capabilities depend heavily on supporting ISE enablers. All mission processes, for example, must be designed and implemented in a way that protects privacy, civil rights, and civil liberties. Moreover, although specific implementations will be tailored to mission needs, ISE systems must all be based on the ISE Enterprise Architecture Framework (ISE EAF) and must conform to ISE common standards. Lastly, ISE governance and management provides a framework for focusing agency attention on information sharing priorities and in seeing that appropriate resources are budgeted to fully institutionalize process improvements and new capabilities.

## 4.1 Architectures for Trusted Interconnection and Sharing

Through the ISE Architecture Program, partner agencies jointly identify the necessary institutional elements to guide information technology (IT) systems planning and implementation supporting nationwide sharing of controlled unclassified and classified information. Approaches used for the ISE Architecture Program, moreover, have also proven applicable to information sharing in other mission areas including maritime, cargo, aviation, cyber security, and healthcare.

IRTPA and other governing statutes and regulations require the implementation of an ISE Architecture-driven methodology to connect distributed and diverse ISE participant systems. The ISE Architecture Program describes the rules and practices needed for the planning and operation of these systems consistent with enterprise architecture best practices. The concept of ISE Shared Spaces—a fundamental element of the ISE EAF—describes a functional and technical systems view supporting information processing and usage requirements from IRTPA that explicitly cite the need for a distributed, trusted, and standards-based implementation (see Figure 11).[32]

[32] See IRTPA §1016(b)(2) for a discussion of the required attributes of the ISE. For additional details on the concept of ISE Shared Spaces, please see *ISE Enterprise Architecture Framework, Version 2.0* (October 21, 2008)

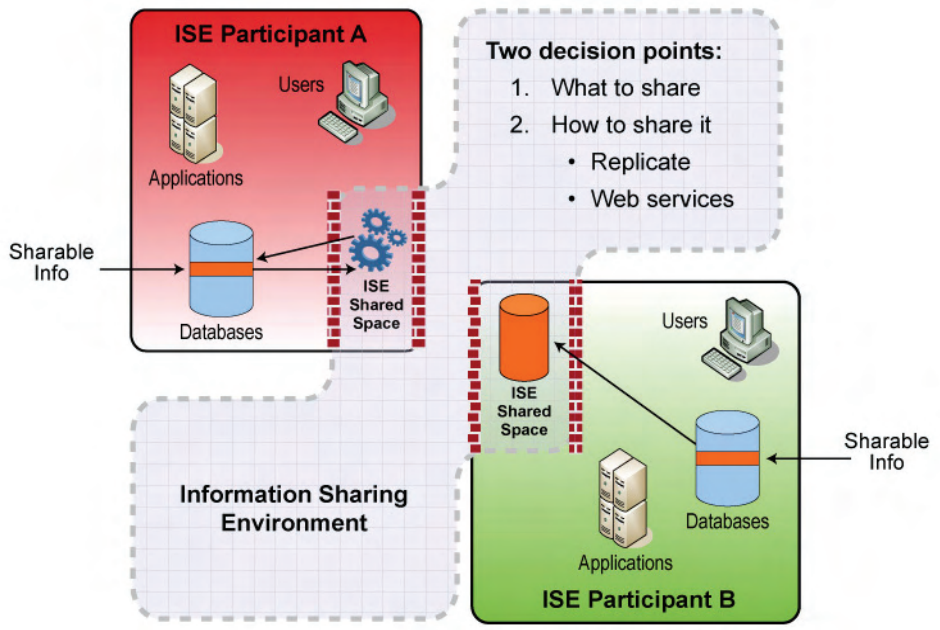



**Figure 11. ISE Shared Spaces and ISE Core Concepts**

ISE participants may require multiple ISE Shared Spaces to support their information sharing requirements. Nevertheless, they all operate under the general management and operational oversight of that ISE participant, even in those cases where the supporting infrastructure for the Shared Spaces (i.e., servers, and associated software) is provided by another agency or organization. The "ISE Core" (also shown in Figure 11) consists of networked infrastructure and services provided by designated organizations (or implementation agents) that enable transport, discovery, and other services necessary for interconnection.

During this past year, the ISE Architecture Program and its concepts became part of the Federal Government's IT management framework as a result of work to expand the implementation, and use of ISE Shared Spaces. Specifically, the PM-ISE:

- Partnered with DOJ to broaden law enforcement community presence in the NSI by reconciling data exchanges and business process flows between the FBI's eGuardian system and other operating ISE Shared Spaces;
- Identified potential improvements to be incorporated in the next version of the ISE-SAR Functional Standard that fully encompass eGuardian as part of the NSI;
- Assisted sites participating in the ISE-SAR Evaluation Environment in properly implementing ISE Shared Spaces;
- Assisted DOT and the NRC, a new partner in the ISE, with ISE Shared Space implementation planning;

available at http://www.ise.gov/docs/eaf/ISE-EAF_v2.0_20081021.pdf and the ISE Profile and Architecture Implementation Strategy, Version 2.0 (June 2009) available at http://www.ise.gov/docs/eaf/ISE-PAIS_V2.0.pdf.

- Coordinated technological enhancements with state and major urban area fusion centers deploying operational ISE Shared Space systems that support the NSI and other ISE applications;
- Partnered with DOJ's Global Justice Information Sharing Initiative (GLOBAL) to develop a systems architecture reference guide to help define common business processes, services, and technology implementation approaches to aid partners in technically interfacing in the ISE; and
- Compiled a prioritized list of tools useful for planning and configuring fusion center systems connecting to the ISE.

## 4.2 Common Standards for Sharing Information

Structured, standards-driven approaches to technology and enterprise data management provide the foundation for community-wide sharing that also protects privacy, civil rights, and civil liberties. The need for common standards is cited in no fewer than thirteen separate places in the NSIS—an explicit recognition that common standards are the fundamental building blocks enabling effective and efficient information sharing. Without a common lexicon—a *lingua franca* that all participants can understand—meaningful information exchange is impossible. Moreover, such standards need to be closely tied to and driven by the end-to-end mission processes they support so that the standards enable, rather than hinder, the information exchanges that the mission process demands.

The International Organization for Standardization and the International Electrotechnical Commission employ a general construct, called a Standards Profile, as a way of grouping a set of one or more base standards that, taken together, help accomplish a particular function or capability. The profile structure promotes interoperability, identifies repeatable IT services, and accelerates delivery of common mission capabilities and standards. In addition, the reuse of commonly accepted and approved engineering practices, techniques, and rules to develop new or similar capabilities can reduce cost and accelerate the schedule in many cases. The use of standards profiles is planned to be incorporated as part of the CISS.

There are a number of Federal Government standards initiatives that affect the ISE. This section first describes the Common Information Sharing Standards (CISS)—the standards program of the ISE. It then goes on to talk about two broader standards programs: NIEM and Universal Core (UCORE). The NIEM and UCORE PMOs, with support by PM-ISE and Office of Management and Budget (OMB), have initiated a strategic process for institutionalizing NIEM and UCORE across the ISE.

**The Power of Standards**

A series of government-wide "success stories" were developed to describe the value of NIEM and UCORE in increasing information sharing to benefit mission processes. These stories are designed to help promote the adoption of enterprise data management through approaches such as the NIEM development process for cross-governmental information sharing environments. They provide insight for non-technical decision-makers about how both these standards approaches can be applied to real-world mission challenges in different user environments.[33]

### 4.2.1 ISE Common Standards

The Common Information Sharing Standards (CISS) Program provides standards, or rules, for technology implementation and information sharing processes and products. This program was initially known as the Common Terrorism Information Sharing Standards Program. But over time it became clear that it is not possible to draw arbitrary boundaries around types of information. Consequently, the CISS Program now factors in the need to exchange information with other relevant domains—such as the critical infrastructure, maritime, and biohazard domains—which in turn can contribute to counterterrorism investigative and response missions. The CISS Program produces two types of standards (see Figure 12):

- *Functional Standards* set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business processes (categorized as "government-unique standards"); and
- *Technical Standards* document methodologies and practices to design and implement information sharing technology capability into ISE systems in order to enable interoperability and interconnectivity (derived from voluntary consensus standards).

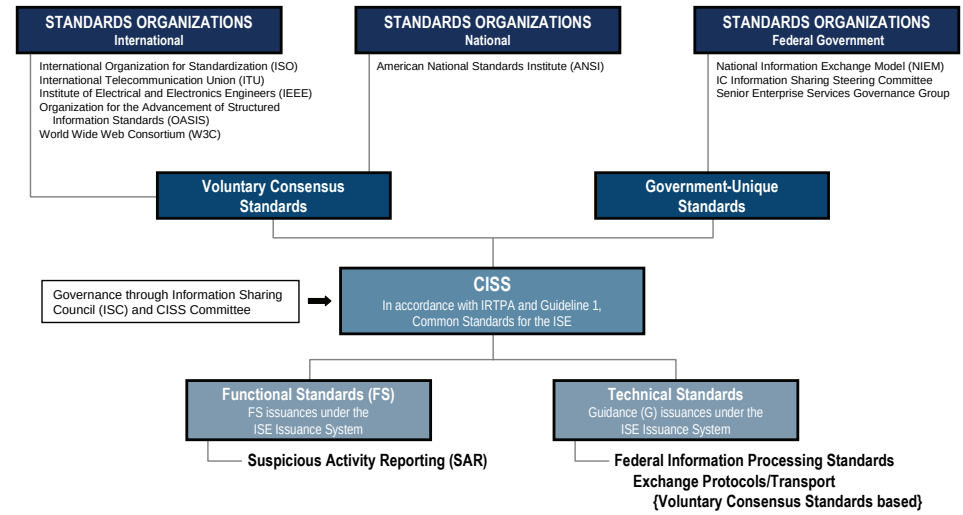
Functional Standards codify business processes, information exchanges, and data fields for use by all ISE participants, and include provisions to control distribution of and access to operationally sensitive or privacy-related information when stored in ISE Shared Spaces.

For example, the *ISE-SAR Functional Standard (ISE-FS-200)*—first issued in January 2008 and updated in May 2009—includes the business rules and formats for exchanging SARs that were agreed to both by operating organizations and privacy and civil liberties advocacy groups. The standard supports broad, standardized dissemination of ISE-SARs while protecting the privacy, civil rights, and civil liberties of Americans.

The positive results achieved through use of the *ISE-SAR Functional Standard* in the ISE-SAR Evaluation Environment and the NSI have demonstrated the lasting value of SAR as an institutional information sharing process and led, ultimately, to the establishment of

[33] These stories are available on the PM-ISE website at http://www.ise.gov/.

the NSI PMO. Work to refine the *ISE-SAR Functional Standard* implementation such as, for example, conducting an analysis of the data exchange and business processes between FBI's eGuardian system and other operating ISE Shared Spaces, is ongoing. These refinements will provide important process and data updates leading to completion of a single integrated version of the *ISE-SAR Functional Standard* for the NSI.




Note: Figure does not reflect all standards organizations in existence – this is CISS focused

**Figure 12: CISS Orientation in the International Standards Community**

### 4.2.2 The National Information Exchange Model (NIEM)

The National Information Exchange Model is a federal, state, local, and tribal interagency initiative providing a foundation for seamless information exchange. The NIEM development process—the basis for CISS functional standards—is designed to develop, disseminate, and support enterprise-wide information exchanges, standards, and processes that can enable organizations in broad communities of interest to effectively share critical information.

**What Is NIEM?**

NIEM was launched on February 28, 2005, through a partnership agreement between the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) and signed by their Chief Information Officers. It leverages the data exchange standards efforts successfully implemented by GLOBAL and extends the Global Justice XML Data Model (GJXDM) to facilitate timely, secure information sharing across the entire law enforcement, public safety, emergency and disaster management, intelligence, and homeland security enterprise.

Providing immediate access to timely, accurate, and complete information, and sharing critical data at key decision points throughout the whole of the justice and public safety enterprises are key objectives of the NIEM program. Fundamentally though, NIEM is not

just about technology or making systems perform better. It is about making major improvements in the way information is shared throughout the Nation.

As an incentive to encourage use of standards, NIEM has inaugurated a special set of awards known as the "Best of NIEM." Additional details plus information on the five award winners for 2009 can be found at http://www.niem.gov/Awards2009.php.

**2009-2010 Highlights in Use of Standards**

- Continued Public Sector adoption of NIEM;
- NIEM used as standard process and framework for recipient transparency reporting against American Recovery and Reinvestment Act of 2009; and
- NIEM adoption as the basis for functional specifications of meaningful use of Electronic Health Records by Department of Health and Human Services.

### 4.2.3 Universal Core (UCORE)

UCORE is a federal information sharing initiative that supports the NSIS and associated agency strategies. UCORE enables information sharing by defining an implementable specification, known as an XML schema, containing agreed-upon representations for the most commonly shared and universally understood concepts of who, what, when, and where in the context of national security.

Begun initially as a DoD-ODNI partnership effort in 2007, the release of UCORE 2.0 in 2008 represented a collaboration of four major agencies—DoD, ODNI, DOJ, and DHS. UCORE improves information exchange by providing standard XML-based definitions for the critical, universally understood concepts described above and implementing them across a broad government stakeholder base, regardless of the IT system being used. It also provides a mechanism to mark information with security classification markings through a standard used within the Intelligence Community, known as the Information Security Markings (ISM) standard.

### 4.2.4 NIEM and UCORE – A Real World Example

In 2008, the Seahawk project in Charleston, South Carolina, operating under the umbrella of the Maritime Domain Awareness initiative, generated a Vessel Activity Report (VAR) for each vessel inbound to the Port of Charleston. Using the Maritime Information Exchange Model (MIEM)—which would soon become NIEM-Maritime—the Department of Transportation, the Coast Guard, the Navy, and 30 other participating federal, state, and local agencies could all exchange information about cargos, crews, and vessels. The Seahawk platform generated a VAR for each vessel, adding value with a risk assessment, vessel analyses, and related data.

The Seahawk pilot demonstrated that UCORE could take the who/what/when/where data in each MIEM-conformant VAR, digest it, and make it understandable to any UCORE-conformant information exchange beyond the maritime community—even if that user group was not itself MIEM-conformant. When the MDA community converted

from MIEM to NIEM, in order to conform to DHS enterprise standards, the MDA community brought its UCORE-compatibility with it to the NIEM world, demonstrating the power of standards to bridge network boundaries.

Today, the MDA initiative is one of the most significant cross-domain information-sharing enterprises in the Federal Government, linking industry, the Navy, the Coast Guard, and the Department of Transportation around the world. It comprises a striking example of success, built on a foundation of UCORE and NIEM.[34]

## 4.3 Privacy, Civil Rights, and Civil Liberties

This Administration has an unwavering commitment to safeguarding the privacy, civil rights, and civil liberties of individuals within the activities of the ISE. The issuance of the ISE Privacy Guidelines established a robust protection framework for privacy, civil rights, and civil liberties.[35] Federal and non-federal agencies implement these guidelines by:

- Developing and adopting written privacy policies;
- Designating Privacy Officers responsible for ensuring compliance with privacy laws and regulations;
- Providing annual training on privacy, civil rights, and civil liberties protections;
- Ensuring that privacy protections are integrated into business processes, systems, and information sharing agreements; and
- Engaging in local outreach and collaboration with community and privacy and civil liberties groups to foster transparency and trust.

Significant progress was made over the last year in strengthening the protection of privacy, civil rights, and civil liberties across all sectors of the ISE. ISE member agencies and SLT partners continued to develop and implement privacy, civil rights, and civil liberties policies. Eight ISE departments and agencies (covering nine ISE members) have submitted ISE Privacy Policies to the ISE Privacy Guidelines Committee (PGC).[36] The remaining ISE member agencies have policies under development.

ISE initiatives, including the Nationwide SAR Initiative and related efforts with designated state and major urban area fusion centers, contributed to the further enhancement of the privacy, civil rights, and civil liberties protection framework and demonstrated the value of this framework to protecting information during operational activities. Privacy and civil liberties advocacy groups played an essential role in refining privacy protections across ISE initiatives by contributing to the development and review

[34] For more on the NIEM-UCORE story, see UCORE and NIEM: Creating Potent New Cross-Boundary Networks available at http://www.ise.gov/docs/sar/UCORE_NIEM_Success_Story_20100421.pdf.

[35] 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://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf.

[36] While there are sixteen ISE member agencies, some members are components of larger Departments. These Departments have chosen to develop Departmental ISE Privacy Policies which cover these component members. This does not preclude each Department's ISE components from issuing additional mission-specific privacy policies.

of products and reports, and by participating in initiatives, such as Building Communities of Trust (see below).

### 4.3.1 Privacy and Fusion Centers

Designated state and major urban area fusion centers were a primary area of focus in 2009-10. Highlights include:

- More than 80% of the 72 designated state and major urban area fusion centers have submitted draft privacy policies for review and technical assistance;
- More than a dozen fusion centers have been notified by DHS that their policies have been determined to be "at least as comprehensive as" the ISE Privacy Guidelines;[37]
- DHS instituted a new requirement in the 2010 Homeland Security Grant Program limiting the use of grant funds by fusion centers that do not have privacy, civil rights, and civil liberties protections in place within six months of receiving their grant award;
- GLOBAL, in conjunction with the PGC, released an updated Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template in April 2010;
- Ongoing technical assistance from federal partners to fusion centers included assistance with developing privacy policies, conducting policy reviews, and providing training to fusion centers on privacy policy development;
- DHS conducted Privacy, Civil Rights, and Civil Liberties "Train the Trainer" sessions for designated fusion center privacy officers at 2010 regional fusion center conferences (DHS will provide ongoing support and assistance to fusion center privacy officers in developing privacy, civil rights, and civil liberties training curriculums for fusion center personnel); and
- Some fusion centers have already developed privacy training courses incorporating national policies and procedures, but tailored to local conditions. The Indiana Intelligence Fusion Center (IIFC), for example, has developed an online course that provides training to all personnel on the IIFC privacy policy. (See http://www.in.gov/isp/files/iifc_privacy_policy_training/aPLiteFlash/.)

### 4.3.2 Privacy and the NSI

The conclusion of the Evaluation Environment phase of the NSI resulted in a major update to the 2008 ISE-SAR *Initial Privacy Analysis*. This update—the *Nationwide Suspicious Activity Reporting Initiative: Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations*—evaluates the experiences of the twelve participating sites and examines the implementation of the privacy, civil rights, and civil liberties protection framework by participating sites. It also makes recommendations for the ongoing protection of privacy, civil rights, and civil liberties to be followed during the nationwide implementation of the NSI by the NSI PMO. The report was published in July 2010.

[37] DHS is the Executive Agent for the management of Fusion Center activities. The DHS Chief Privacy Officer conducts the review of fusion center privacy policies in her capacity as a Co-Chair of the PGC.

### 4.3.3 Privacy Guidelines Committee

In the summer of 2010, the PGC—co-chaired by privacy and civil liberties officials of the Office of the DNI, DHS, and DOJ—will be established as a subcommittee under the Information Sharing and Access Interagency Policy Committee (ISA IPC), a body established by the White House to oversee federal information sharing activities. The PGC continues to ensure consistency and standardization in the implementation of the ISE Privacy Guidelines across ISE member agencies and non-federal SLT partners and serves as a support resource for ISE partners. The PGC Co-Chairs have continued to meet with representatives of privacy and civil liberties advocacy groups to obtain their inputs and incorporate their suggestions into ISE initiatives such as the NSI.

## 4.4 Improving Protection While Expanding Access

*Trust*—confidence that all parties will adequately protect the information they receive and effectively manage risks arising from interconnecting systems—is an indispensible element of effective information sharing and collaboration. The ISE is envisioned as a trusted partnership of agencies at all levels of government and the private sector. There is no inherent conflict between sharing information and protecting it. Figure 10 depicts protection and sharing as two sides of a single, indivisible coin. Without protection, sharing is not possible; and without sharing, protection loses its relevance.


**Figure 10. Protection and Information Sharing are Two Sides of a Single Coin**

Ensuring trust requires adoption of practices that assure that information is protected from unauthorized disclosure (confidentiality), that it is accurate and dependable (integrity), and that it is accessible when needed (availability). These practices cut across all sub-disciplines of the security field encompassing personnel, physical, and information systems security.

To engender this trust, the ISE has attempted to normalize federal security practices and risk management methodologies to foster acceptance government-wide. That acceptance then leads to "reciprocity" between agencies, i.e., recognition that each

organization's protection processes and systems are trusted to perform securely and predictably. Given that the ISE includes state, local, and tribal agencies and, in certain cases, private sector and foreign partners as well, it is important to ensure that federal security policies and practices are designed up front with extensibility to SLT and other partners in mind.

### 4.4.1 State, Local, Tribal, and Private Sector Partners Security Framework

IRTPA requires that the ISE provide and facilitate "the sharing of terrorism information among all appropriate federal, state, local, and tribal entities … at and across all levels of security."[38] Disparate policies and practices for physical, personnel, and information systems security have been specifically identified as key impediments to sharing this information. In response, various ISE communities have begun to promote the mutual acceptance of security policies and practices across the Federal Government. Even when they are well-coordinated, however, federal policies for accessing and managing classified information have not consistently addressed state, local, tribal, and private sector partners operational needs nor have they been uniformly extended to include state, local, tribal, and private sector partners. This lack of uniformity has resulted in inconsistent application, confusion, and negative mission impacts.

An interagency policy committee worked over the last year to develop a policy that will establish a federal-wide security program to govern access to classified national security information shared by agencies with state, local, tribal, and private sector partners, and to ensure the proper safeguarding of such information. The proposed policy will standardize the processes for state, local, tribal, and private sector partners' access to classified information, ensure that the classified information is properly shared, and reduce the current security barriers inhibiting the sharing of classified information with these partners. The committee will designate an Executive Agent for the program and establish a Policy Advisory Committee to recommend policy and procedural changes as the program develops.

### 4.4.2 Information Systems Security

Reciprocity of IT system security certification and the acceptance and recognition among participating ISE agencies of each other's accreditation decisions is another important factor in ensuring efficient and effective information sharing. Several initiatives—led jointly by NIST, the Committee on National Security Systems (CNSS), and the ODNI—have made considerable progress in updating and harmonizing federal security standards and processes, setting the stage for future extensibility to state, local, tribal, and private sector partners.

With the issuance of NIST Special Publication 800-53 in August 2009 and CNSS Instruction 1253 in October 2009, the IC, DoD, and civilian federal agencies, for the first time, have adopted a common set of security controls that forms a *de facto* national

[38] IRTPA, §1016(b)(2).

baseline for all federal information systems.[39] Although agency certifiers and accreditors will tailor requirements to their own environments, alignment of these controls, and issuance of subsequent publications relating to risk management and security assessment, will eventually enable all federal agencies to reciprocally accept other agencies' security testing results when interconnecting systems.

The alignment and harmonization of federal information systems security standards on a common baseline will, in turn, present state, local, tribal, and private sector partners with a single, predictable security goal. Harmonized standards will also enable implementation of reciprocity policies, not only among federal agencies and systems, but with state, local, tribal, and private sector partners as well, thereby reducing the time—and cost—required to interconnect systems.

### 4.4.3 Identity and Access Management

Properly identifying and authenticating users of IT systems is a necessary condition for trusted operations. The Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Part A, was developed by the Identity, Credential, and Access Management Subcommittee (co-chaired by the General Services Administration and DoD) of the Federal CIO Council in November 2009. This document provides a common segment architecture and associated implementation guidance for use by federal agencies as they continue to invest in FICAM programs. The FICAM segment architecture will serve as an important tool for providing awareness to external mission partners and will drive the development and implementation of interoperable solutions. The Global Federated Identity and Privilege Management and the Trusted Broker systems are two approaches in use today that work toward interoperating under the FICAM umbrella.

When fully implemented, FICAM will close identified security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. Leveraging the digital infrastructure in a secure manner will enable the transformation of business processes, many of which are vital to the security of the United States.

In addition to important progress in aligning access management procedures, PM-ISE sponsored ground-breaking work with NIST and DHS to develop an automated means to evaluate access management policies. Using new algorithms to electronically translate policies and regulations in natural language into automated instructions, NIST developed a pilot system that evaluates multiple policies, identifies gaps and contradictions, and reveals the actual access that results from overlaying more than one policy. As more and more information passes through many mission partners and

[39] "Recommended Security Controls for Federal Information Systems and Organizations" available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf and "Security Categorization and Control Selection for National Security Systems" available at http://www.cnss.gov/Assets/pdf/CNSSI-1253.pdf.

systems, each with different access policies, the significance of automating access polices will be increasingly necessary to ensure efficient and appropriate access.

### 4.4.4 Updated Policy for Handling Classified Information

Improving protection and expanding access are complementary, not conflicting, goals. The policy governing the handling of classified national security information has undergone significant revision over the past year designed to ensure that classification is not a barrier to providing information to those who need it in a timely way. On December 29, 2009—following a Presidentially-mandated 90-day review—the Administration released Executive Order (EO) 13526, which governs the handling, marking, and eventual declassification of Classified National Security Information. The new order replaces EO 12958, and provides more "accurate and accountable application of classification standards and routine, secure, and effective declassification" through:

- Establishment of a National Declassification Center;
- Measures to ensure proper classification of information;
- Greater emphasis on sharing classified information among those who need it, including a redefinition of the "need to know" principle and less restrictive rules for sharing classified information between agencies; and
- Provisions that ensure greater openness and transparency in the government's Classification and Declassification programs.[40]

Agencies are formulating plans to implement these changes.

### 4.4.5 Expanding Discovery and Access in the Intelligence Community

The Intelligence Community has continued the transformation of information sharing by implementing IC Directive (ICD) 501, "Discovery and Dissemination or Retrieval of Information." This policy promotes responsible information sharing by distinguishing between discovery (obtaining knowledge that information exists) and dissemination or retrieval (obtaining the contents of the information). The policy directs all IC elements to fulfill their "responsibility to provide" by making intelligence discoverable by automated means by authorized IC personnel. It also establishes procedures for gaining access to information that has been discovered and for resolving disputes if access is denied.

Through the implementation of ICD 501, the IC has made considerable progress on improving information sharing by enabling discovery of disseminated analytic products through the creation of the Library of National Intelligence (LNI). LNI uses a combination of attribute-based access, tagged data, and auditing to promote secure information sharing of more than three million intelligence products.

Metadata tagging—information about other data—is crucial to ICD 501 implementation and is the linchpin to the effective management of data throughout the intelligence cycle. It facilitates discovery, retrieval, and protection. The IC is using XML as the

[40] Executive Order 13526 is available at http://www.archives.gov/federal-register/executive-orders/2009-obama.html.

standard for metadata implementation, and most IC elements are meeting IC metadata standards required to submit products to the LNI.

**The Value of the LNI**

People with a mission need are increasingly able to conduct a single search of the IC's disseminated analytic products, covering 99% of the included product lines, compared to the past where users had to visit over 50 different websites to discover the same information.

The next steps include making the LNI more complete and timely while improving the quality of the metadata in the LNI, which will further improve the ability of users to search for disseminated analytic products as well as developing a secure repository for discovery of sensitive intelligence products by authorized IC personnel.

The ODNI has convened an information sharing planning and assessment team to review the IC's information sharing challenges and to assess information sharing reactions within the IC and with a wide range of external customers and partners. The ODNI continues to work with the PM-ISE to improve counterterrorism and homeland security sharing across the Federal Government and with SLT agencies and private sector organizations.

The Analytic Transformation Roadmap is also informing IC information sharing efforts and the IT investments that enable improved sharing. The Roadmap establishes a unified vision and high level schedule showing how the IC's flagship information sharing programs interact to support intelligence analysis. Specifically, it maps out the incremental integration of the A-Space collaboration environment, a key component of the ODNI's Analytic Transformation Program, with powerful search and retrieval capabilities. The resulting unified analytic environment will dramatically improve the ability of analysts to harness their content and make it available for collaborative analysis.

## 4.5 Open Government

Most of the work of building the ISE to date has been aimed at expanding information sharing across all areas of government in the U.S. and, to a lesser extent, with private sector organizations and foreign partners. As the ISE continues to evolve, however, we recognize that to support the Administration's commitment to openness and transparency, we must extend those efforts to include the American public as well.

My Administration is committed to creating an unprecedented level of openness in Government. We will work together to ensure the public trust and establish a system of transparency, public participation, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government.

— President Barack H. Obama

A number of separate but related activities over the last year directly supported the President's goal of creating and institutionalizing a culture of open government based on the cornerstone principles of transparency, participation, and collaboration.[41] This section highlights several of these activities that respond directly to the four major improvement areas cited in the Open Government Directive: publishing government information online; improving the quality of government information; creating and institutionalizing a culture of open government; and enabling a policy framework for open government.

### 4.5.1 Building Communities of Trust (BCOT)

The Building Communities of Trust (BCOT) initiative is a joint effort of BJA, the Community Oriented Policing Services (COPS) office and PM-ISE. The control and prevention of terrorism-related and other criminal activity requires meaningful sharing of information between police agencies, and especially between the community and the police. BCOT focuses on developing relationships of trust between police departments, fusion centers, and the communities they serve—particularly immigrant and minority communities—to prevent terrorist-related crime and to help keep our communities safe. The knowledge of communities and the mutual understanding that comes from trust-based relationships between law enforcement and the local community not only enable law enforcement officers and analysts to more readily distinguish between innocent culturally-based behaviors and behavior indicative of criminal activity, but also make the community more likely to report suspicious, potentially criminal activity.

To define and evaluate the concepts underlying the BCOT initiative, four locations were chosen (three cities and one state). At each of these locations (see Table 3), a diverse group of representatives from the local community, the police, and fusion center leadership conducted roundtable discussions to explore how these groups could effectively engage in meaningful and ongoing dialogue to build relationships of trust. Primary attention was placed on minority and immigrant communities—i.e., residents of neighborhoods with cultures that often do not have strong histories of collaborative relationships with the police.

**Table 3. BCOT Pilot Sites**

| Pilot Site | Participating Organizations |
|---|---|
| Miami | 18 |
| Boston | 20 |
| Seattle | 20 |
| Texas | 12 |

Specific types of information gathered during these pilot sessions included:

- Views of community leaders regarding effective strategies for developing trust;

[41] Memorandum for the heads of Executive Departments and Agencies from OMB Director Peter R. Orszag entitled "Open Government Directive" (December 8, 2009) available at http://www.whitehouse.gov/open/documents/open-government-directive.

- Suggestions as to the types of training and guidance that will be most useful to police executives and their employees;
- Stories about successful experiences communities have had in developing relationships of trust, which can serve as models for adoption; and
- Best practices that assist fusion center analysts in becoming more knowledgeable, and more sensitive to local communities and cultures.

The lessons learned from these roundtable dialogues were then synthesized to develop formal guidance for local police agencies, fusion centers, and communities to use in developing their own locally-based approaches. This guidance, planned for release in the summer of 2010, emphasizes the value of outreach and transparency, and the importance of collaboration between local police and communities to ensure that the police factor local community concerns into their crime-fighting strategies.

### 4.5.2 Interacting with the Public

In the spirit of transparency in government, and following the lead of other government initiatives such as Data.gov, the PM-ISE engaged users of four major Sensitive But Unclassified (SBU) systems—LEO, RISSNET, the HSIN, and the IC unclassified system, Intelink-U—to gather ideas and feedback to help formulate requirements as part of an initiative to improve interoperability of SBU/CUI systems and networks. This was a three-week project that allowed users to post questions and suggestions through a publically accessible website—www.sbuconnectivity.ideascale.com (see Figure 13).


**Figure 13. Screen Shot of Requirements-Gathering via ideascale.com**

The process resulted in 357 comments, 48 new ideas, and more than 5,000 votes on those ideas by participants. The approximately 98 unique requirements identified through this process have been binned into nine categories for further analysis and prioritization. Table 4 provides additional details.

**Table 4. Detailed results of Requirements-Gathering Effort**

| Period | Ideas | Comments | Votes |
|---|---|---|---|
| **Week 1** | 18 | 123 | 4,042 |
| **Week 2** | 12 | 115 | 650 |
| **Week 3** | 4 | 97 | 273 |
| **Follow-up** | 3 | 22 | 52 |
| **Total** | 37 | 357 | 5,017 |

Most federal, state, local, and tribal ISE participants maintain public websites that provide the public with useful information and include directions about where the public can send comments and suggestions. The PM-ISE website is currently being redesigned to provide more information to ISE participants and the public and present it in a better-structured and more accessible way.

### 4.5.3 Tribal Consultation

In order to broaden the scope and depth of consultation available to tribal governments on information sharing issues, the SLIAG is formulating a tribal consultation policy. Executive Order 13175 of November 6, 2000 and an accompanying Presidential Memorandum directed federal agencies to consult with federally-recognized tribes before issuing federal regulations or standards that could affect tribal equities.[42] This Tribal Consultation Policy will provide additional clarification of the EO as it relates to information sharing and collaboration. A tribal representative has also been included as a member of the ITACG detail.

## 4.6 Personal and Organizational Accountability

A major factor in creating a culture of information sharing and collaboration involves encouraging behaviors that foster information sharing and discouraging those that don't. Rewarding behaviors that foster information sharing and adoption of collaborative cross-agency work teams will improve performance throughout the government and enhance efforts conducted with non-governmental partners. People who are properly trained, held accountable, and rewarded for sharing and collaborating with their counterparts from other agencies not only provide short-term improvements in information sharing and collaboration, but, by serving as role models for others, effect lasting longer-term culture change. Their behaviors become "best practices," the ones that all employees strive to emulate.

[42] Executive Order 13175, "Consultation and Coordination with Indian Tribal Governments" is part of the federal Register and is available at http://www.naihc.net/NAIHC/files/ccLibraryFiles/Filename/000000002535/02-19-2010-Executive-Order.pdf. The Presidential Memorandum, "Tribal Consultation," is available at http://www.whitehouse.gov/the-press-office/memorandum-tribal-consultation-signed-president.

In October 2009, the Director, Office of Personnel Management issued a memorandum to federal Chief Human Capital Officers in which he stated "information sharing and collaboration should be a common, core behavior across all Departments and agencies." Now that this principle has been endorsed by the Federal Government's Human Capital Authority, the ISE will close the books on additional work on appraisals and incentives, and going forward, will concentrate instead on developing a culture of learning based on continuous, measurable improvements to information sharing and collaboration across the ISE.

**Appraisals and Incentives**

- As of June 2010, almost all federal agency employees that were identified as supporting ISE priorities, included "information sharing and collaboration" as an explicit evaluation factor component in their performance appraisals;
- In 2009, the ODNI presented 24 awards recognizing distinguished service and/or exceptional contributions to information sharing and collaboration; and
- The DoD introduced a special award—the "Secure Information Sharing Award"—that recognizes the contributions made by employees who find new ways to view security and sharing as interdependent rather than conflicting concepts.

## 4.7 ISE Governance

### 4.7.1 The PM-ISE

To "plan for and oversee the implementation of, and manage the ISE," IRTPA established the position of Program Manager to be "responsible for information sharing across the Federal Government."[43] Consistent with the direction and policies issued by the President, the DNI, and the Director of the Office of Management and Budget (OMB), the PM-ISE issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE.[44] The PM-ISE acts as the catalytic agent for improving terrorism-related information sharing among ISE participants by working in collaboration with them to remove barriers, facilitate change, and ensure that ISE implementation proceeds efficiently and effectively. To better assist in and oversee ISE implementation activities, the Office of the PM-ISE has staff with experience in counterterrorism, information sharing, technology, and policy at all levels of government. The PM-ISE:

[43] IRTPA §1016(f). Amendments to IRTPA included in the Implementing Recommendations of the 9/11 Commission Act of 2007 identified additional attributes and gave additional authorities, including the authority to issue guidelines and standards, to the PM-ISE.

[44] IRTPA §1016(f)(2)(A)(iii).

- Coordinates the sharing of terrorism-related information among federal, non-federal entities, and the private sector;
- Issues common ISE standards governing sharing of terrorism-related information by federal agencies; and most importantly
- Acts as an "honest broker" collaborating with mission partners and all ISE stakeholders to achieve progress in information sharing and collaboration.

### 4.7.2 The Information Sharing and Access Interagency Policy Committee (ISA IPC)

The ISA IPC was established by the White House in 2009 and subsumed the role of a predecessor interagency body (the Information Sharing Council) established by IRTPA. It was chaired initially by the Senior Director for Information Sharing Policy on the White House National Security Staff. In a July 2009 memorandum, the Assistant to the President for Homeland Security and Counterterrorism made clear that the Administration regarded information sharing as extending beyond-terrorism related issues to encompass "the sharing of information more broadly to enhance the national security of the United States and the safety of the American people."

In June 2010, the PM-ISE was designated by the White House as a co-chair of the ISA IPC. This dual role for the Program Manager is an acknowledgment that policies, business practices, architectures, standards, and systems developed for the ISE can be applicable to other types of information beyond terrorism and *vice versa*. In his dual role, the PM-ISE will help ensure that there will be the closest possible alignment between the ISE and broader national security information sharing activities.

### 4.7.3 ISE Performance Management

Governance and decision-making across the ISE are supported by the integrated performance and investment process, shown in Figure 14. The PM-ISE actively monitors progress toward information sharing performance objectives and goals. This year, progress across the ISE was captured through:

- ISE agencies providing ongoing awareness of progress being made, including responses to the 2010 ISE Annual Performance Assessment Questionnaire (See Appendix A for detailed results); and
- PM-ISE collection and analysis of financial data to determine the extent to which ISE priorities are being incorporated into agency budgets.

Based on the analysis of the current level of progress and performance, ISE leadership, working with OMB and the White House National Security Staff, has established future ISE priorities. These priorities, outlined in the Fiscal Year (FY) 2012 ISE Programmatic Guidance, align resources and investments necessary to meet ISE priorities. The FY 2012 ISE-specific programmatic guidance identifies the following priorities:

1. Building a national integrated network of fusion centers;
2. Continuing implementation of the NSI;
3. Establishing SBU/CUI network interoperability;

4. Improving governance of the classified National Security Information program; and
5. Advancing implementation of CUI policy.

The PM-ISE issued separate guidance that identifies specific actions to be taken to address these ISE priorities.

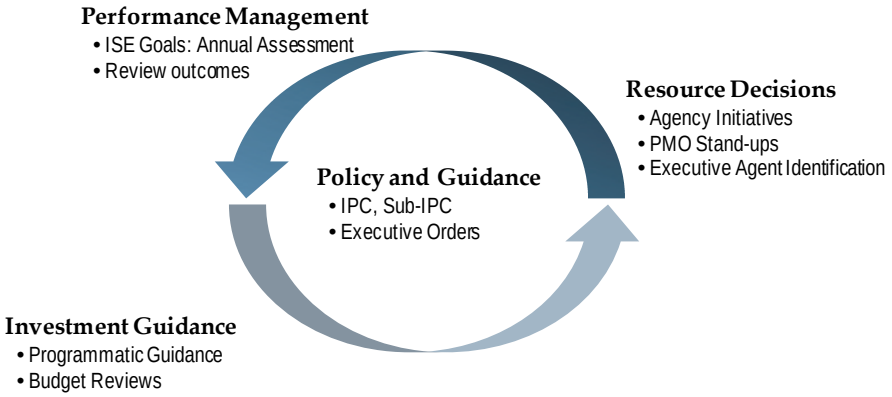



**Figure 14. The Performance-Investment Cycle**

The 2011 performance and investment process will focus on ensuring that the ISE is making further progress in these priority areas. The process for measuring the progress of the ISE continues to evolve. The PM-ISE works closely with key points of contact at each ISE agency to obtain feedback and gather insights on improving the process and measures. The intent of this is two-fold: to improve the overall ISE process and to influence the performance management processes at each of these agencies.

The inclusion of ISE stakeholders in the development of the assessment process will serve to increase interagency buy-in and support; refine and enhance performance questions; and improve the overall assessment results.

## Standards-Based Innovation: Crossing Organizational and Domain Boundaries

The ISE cannot be built nor will it deliver required capabilities without standards-based innovation. Innovation will result in faster delivery of more cost effective solutions; greater agility in the face of evolving threats through reuse and the ability to identify new requirements and form dynamic networks across mission partners; and the ability to reduce redundancy and unnecessary complexity that drives costs, slows progress, and only aids those that would do us harm. Standards-based innovation includes the development of business processes or functional standards with a particular focus on standardizing the information exchanges at the outer edge of organizations. The Nationwide SAR Initiative, highlighted earlier in this report, is a primary example of this dynamic.

The National Information Exchange Model (NIEM)—a voluntary consensus standard developed in partnership with federal, state, local, and tribal governments, the private sector, and academia—is a key focal point for standards-based innovation. NIEM was launched in 2005 through a partnership agreement between the departments of Justice and Homeland Security and signed by the agencies' Chief Information Officers. NIEM is not a software program, a computer system, nor a data repository but is a common vocabulary and mature framework surrounding information exchanges among and between governmental entities as well as with private sector and international partners that allows disparate systems to share, exchange, accept, and translate information.

NIEM-based standards innovation is already yielding results, both for mission partners (the buy side) and industry partners (the sell side). In each federal agency's FY 2011 Passback, a provision asked all to evaluate the adoption and use of the NIEM as the basis for developing reference information exchanges to support specification and implementation of reusable cross-boundary information exchanges. Agency responses indicate that two agencies are currently implementing NIEM on an enterprise level; thirteen agencies or Lines of Business have committed to use NIEM; and seven are pursuing further evaluation. Of the others, several opportunities exist for possible future use.

One example of buy-side results is DHS cost avoidance through use of standards-based innovation. In the President's FY 2011 Budget, DHS reports $26 million in cost avoidance and 30% cost and time savings in FY 2009 from planning to design through use of NIEM.[45] With enactment of the President's FY 2011 Budget, DHS is committed to delivering $470 million in cost avoidance through FY 2013. All of these savings come through reductions in complexity through coordinated evolution and reuse of best practices, specifications, and actual information exchanges across DHS operational units.

[45] DHS FY 2011 Congressional Budget Justification, p. 229.

Another buy-side result can be found in DHS's and DOJ's integration of NIEM into existing IT processes to achieve internal efficiency and interoperability, and to extend these gains to the outer edge. DHS and DOJ now use NIEM as part of their IT strategic plans, Request for Proposals (RFPs) to vendors, and grant language to state, local, and tribal governments. DOJ, working through the Bureau for Justice Assistance and with DHS, has developed grant language for state, local, and tribal partners that supports use of NIEM at all levels of government. This guidance "… requires all grantees to use the latest NIEM specifications and guidelines regarding the use of XML for all grant awards."

On the sell-side, industry is beginning to integrate NIEM and support for specific information exchanges into standard product and service offerings. Leading-edge technology vendors are beginning to market NIEM integration and compatibility. Several commercial products support the NIEM-based SAR functional standard described earlier in this report, and vendors are differentiating themselves in the marketplace by innovating on top of the SAR standard.

The use of common standards, through efforts like NIEM, offers an unprecedented opportunity for substantial gains for cross domain information exchange, particularly at organizational boundaries. Standards-based innovation and adoption challenges the *status quo* and presents a way forward to significant improvements in mission effectiveness and efficiency.

# APPENDIX A – DETAILED ISE PERFORMANCE RESULTS

The tables in this appendix contain selected results from the 2010 ISE Performance Assessment, as of June 30, 2010, as self-reported by the ISE Departments and Agencies. These results have been organized according to the ISE Framework Goals and Sub-Goals. Performance data of some sections (i.e. sections 5, 8, 9, and 10) was gathered outside the annual performance assessment, and thus is not included as part of this. Where possible, the "Highlight" box is used to describe successes relative to 2009 to help show the progress that continues to be made by the ISE. Where new measures were introduced for 2010, the "Highlight" box describes the importance of the measure for 2010 only. Please note that there are two DoD members of the ISE, and so a "Yes" response for DoD/JCS counts as two yeses.

## GOAL 1: CREATE A CULTURE OF SHARING



### *1. Personnel Appraisals*

| | | | | |
|---|---|---|---|---|
| **Measurement Objective** | Add information sharing elements to employee performance appraisals. | | | |
| **2010 Metric** | 13 out of 15 ISE departments and agencies have included (or plan to include) "information sharing and collaboration" as a component in performance appraisals of employees supporting ISE-related priorities. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | Yes | | DOJ | Yes |
| DHS | Yes | | DoS | Yes |
| ODNI | Yes | | DOT | Yes |
| DOC | Yes | | FBI | Yes |
| DoD/JCS | Under Development | | HHS | Yes |
| DOE | No Response | | NCTC | Yes |
| DOI | Yes | | Treasury | NA |
| **2010 Highlight** | **All responding ISE departments and agencies with information sharing and collaboration requirements are aware of and actively making attempts to include this requirement in employee performance appraisals.** | | | |

GOAL 1

## 2. ISE Awareness Training

| Measurement Objective | Ensure all ISE departments and agencies are developing information sharing and collaboration related mission-specific training. | | | |
|---|---|---|---|---|
| 2010 Metric | 9 out of 15 ISE departments and agencies implemented mission-specific training that supports information sharing and collaboration. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | Yes | | DOJ | Yes |
| DHS | Yes | | DoS | No |
| ODNI | Yes | | DOT | Yes |
| DOC | No | | FBI | Yes |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | No | | Treasury | No |
| 2010 Highlight | **86% of responding ISE departments and agencies offer some sort of information sharing and collaboration training for their employees.** | | | |

| Measurement Objective | Ensure all ISE departments and agencies are recognizing the potential to share training practices with other agencies/partners. | | | |
|---|---|---|---|---|
| 2010 Metric | 8 out of 15 ISE departments and agencies have training on information sharing and collaboration that could be shared with other agencies/partners. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | Yes | | DOJ | Yes |
| DHS | Yes | | DoS | Yes |
| ODNI | Yes | | DOT | No |
| DOC | No | | FBI | No |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | No | | Treasury | No |
| 2010 Highlight | **The majority of ISE departments and agencies are collaborating with each other to ensure sharing of information sharing and collaboration training.** | | | |

## 3. Incentives for Information Sharing

| Measurement Objective | Make information sharing a factor in awards and incentives programs. | | | |
|---|---|---|---|---|
| 2010 Metric | 12 out of 15 ISE departments and agencies offer (or intend to offer) an award that includes information sharing and collaboration directly or indirectly as criteria. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | Yes | | DOJ | Yes |
| DHS | Yes | | DoS | Under Development |
| ODNI | Yes | | DOT | Yes |
| DOC | No | | FBI | Yes |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | Yes | | Treasury | Yes |
| 2010 Highlight | **86% of responding ISE departments and agencies have adopted or intend to adopt incentives such as personnel recognition, cash awards, and other rewards.** | | | |

# GOAL 2: REDUCE BARRIERS TO SHARING

2 GOAL

## 4. *Systems Security Practices*

| Measurement Objective | Work toward systems security reciprocity among federal/state/local and private sector entities. | | | |
|---|---|---|---|---|
| 2010 Metric | 9 out of 15 ISE departments and agencies have documented policies and/or implementation guidelines on IT security reciprocity stating the conditions under which they will accept the security certification and/or accreditation of another organization. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | Yes | | DOJ | Under Development |
| DHS | Yes | | DoS | No |
| ODNI | Yes | | DOT | Yes |
| DOC | No | | FBI | No |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | Yes | | Treasury | Yes |
| 2010 Highlight | **The majority of ISE departments and agencies are now working to document IT security reciprocity practices and procedures.** | | | |

## 5. *CUI Framework – See the discussion in the body of this report for information on progress*

## 6. *ISE Shared Spaces*

| Measurement Objective | Implement ISE Shared Spaces. | | | |
|---|---|---|---|---|
| 2010 Metric | 8 out of 15 ISE departments and agencies have incorporated CISS Technical Standards into their architectures. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | Yes | | DOJ | Yes |
| DHS | Yes | | DoS | No |
| ODNI | Yes | | DOT | No |
| DOC | No | | FBI | Yes |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | Under Development | | Treasury | No |
| 2010 Highlight | **The majority of ISE departments and agencies are now factoring the CISS Technical Standards into their architectures.** | | | |

2 GOAL

| Measurement Objective | Implement ISE Shared Spaces. | | | |
|---|---|---|---|---|
| 2010 Metric | 11 out of 15 ISE departments and agencies are able to share terrorism and homeland security information following the ISE Shared Spaces concept. | | | |
| Agency | 2010 Response | | Agency | 2010 Response |
| CIA | Yes | | DOJ | Yes |
| DHS | Yes | | DoS | Yes |
| ODNI | Yes | | DOT | Yes |
| DOC | No | | FBI | Yes |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | Yes | | Treasury | No |
| 2010 Highlight | **79% of responding ISE departments and agencies now have the capability to share terrorism and homeland security information through ISE Shared Spaces.** | | | |

## *7. Privacy Policies*

| Measurement Objective | Ensure privacy protection across the ISE. | | | |
|---|---|---|---|---|
| 2010 Metric | 9 out of 15 ISE departments and agencies have developed and implemented an ISE Privacy Policy and submitted it to the Privacy Guidelines Committee. | | | |
| Agency | 2010 Response | | Agency | 2010 Response |
| CIA | Yes | | DOJ | Yes |
| DHS | Yes | | DoS | Under Development |
| ODNI | Yes | | DOT | Under Development |
| DOC | Under Development | | FBI | Yes |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | Yes | | Treasury | Under Development |
| 2010 Highlight | **There has been a four-fold increase in the past year in the number of responding ISE departments and agencies who have developed and implemented ISE privacy policies.** | | | |

# GOAL 3: IMPROVE SHARING PRACTICES WITH FEDERAL, STATE, LOCAL, TRIBAL AND FOREIGN PARTNERS

3 GOAL

***8. Nationwide SAR Initiative – See the discussion in the body of this report for information on progress***

***9. ITACG – See the discussion in the body of this report for information on progress***

***10. State and Major Urban Area Fusion Centers – See the discussion in the body of this report for information on progress***

***11. Information Sharing with Foreign Partners***

| Measurement Objective | Make available to the appropriate personnel tools and mechanisms for the negotiation of terrorism-related agreements and arrangements. | | | |
|---|---|---|---|---|
| 2010 Metric | 9 out of 15 ISE departments and agencies have or will use the Checklist of Issues for Negotiating Terrorism Information Sharing Agreements and Arrangements. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | NA | | DOJ | Yes |
| DHS | Yes | | DoS | Yes |
| ODNI | Yes | | DOT | Yes |
| DOC | NA | | FBI | Yes |
| DoD/JCS | Yes | | HHS | NA |
| DOE | Yes | | NCTC | NA |
| DOI | NA | | Treasury | NA |
| 2010 Highlight | **Compared to 2009, three times as many ISE departments and agencies are currently using or plan to use the Checklist.** | | | |

# GOAL 4: INSTITUTIONALIZE SHARING

## 12. *Enterprise Architecture – Investments*

| Measurement Objective | Further integrate their IT management structures with ISE Enterprise Architecture principles. |
|---|---|
| 2010 Metric | 10 out of 15 ISE departments and agencies have mapped at least one IT investment to their information sharing segment architectures. |

| Agency | 2010 Response | Agency | 2010 Response |
|---|---|---|---|
| CIA | Yes | DOJ | Yes |
| DHS | Yes | DoS | Yes |
| ODNI | Yes | DOT | Yes |
| DOC | No | FBI | Yes |
| DoD/JCS | Yes | HHS | No |
| DOE | No Response | NCTC | Yes |
| DOI | Under Development | Treasury | No |

| Measurement Objective | Further integrate their IT management structures with ISE Enterprise Architecture principles. |
|---|---|
| 2010 Metric | 7 out of 15 ISE departments and agencies have represented all their major ISE IT investments in their enterprise transition plans. |

| Agency | 2010 Response | Agency | 2010 Response |
|---|---|---|---|
| CIA | No | DOJ | Yes |
| DHS | No | DoS | No |
| ODNI | No | DOT | Yes |
| DOC | Not Applicable | FBI | Yes |
| DoD/JCS | Yes | HHS | No |
| DOE | No Response | NCTC | Yes |
| DOI | Yes | Treasury | Yes |

| Measurement Objective | Further integrate their IT management structures with ISE Enterprise Architecture principles. |
|---|---|
| 2010 Metric | 6 out of 15 ISE departments and agencies have included at least one information sharing measurement indicator in the Section D Performance Information table of their Exhibit 300s for ISE investments. |

| Agency | 2010 Response | Agency | 2010 Response |
|---|---|---|---|
| CIA | No | DOJ | Yes |
| DHS | Yes | DoS | No |
| ODNI | No | DOT | Yes |
| DOC | Not Applicable | FBI | Yes |
| DoD/JCS | Yes | HHS | No |
| DOE | No Response | NCTC | Yes |
| DOI | Under Development | Treasury | No |

| 2010 Highlight | **In the past year, there has been a significant increase in the number of ISE departments and agencies taking the steps to integrate investment best practices into their architecture frameworks.** |
|---|---|

GOAL 4

## 13. Common Information Sharing Standards (CISS)

### 13a. Information Sharing Segment Architecture:

| Measurement Objective | Adopt ISE standards. | | | |
|---|---|---|---|---|
| 2010 Metric | 5 out of 15 ISE departments and agencies have completed approved information sharing segment architectures. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | No | | DOJ | Yes |
| DHS | Yes | | DoS | No |
| ODNI | No | | DOT | Yes |
| DOC | Not Applicable | | FBI | Under Development |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | No | | Treasury | Not Applicable |

### 13b. Information Sharing Segment Architecture:

| Measurement Objective | Adopt ISE standards. | | | |
|---|---|---|---|---|
| 2010 Metric | 8 out of 15 ISE departments and agencies reference the Information Sharing Environment section of the federal Transition Framework Catalog in building their segment architectures. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | Yes | | DOJ | Yes |
| DHS | Yes | | DoS | No |
| ODNI | Yes | | DOT | Yes |
| DOC | Not Applicable | | FBI | Under Development |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | No | | Treasury | Not Applicable |

### 13c. CISS Functional Standards:

| Measurement Objective | Adopt ISE standards. | | | |
|---|---|---|---|---|
| 2010 Metric | 5 out of 15 ISE departments and agencies have incorporated CISS Functional Standards into the management and implementation of their ISE-related mission business processes. | | | |
| **Agency** | **2010 Response** | | **Agency** | **2010 Response** |
| CIA | No | | DOJ | Yes |
| DHS | Yes | | DoS | No |
| ODNI | No | | DOT | No Response |
| DOC | Not Applicable | | FBI | Yes |
| DoD/JCS | Yes | | HHS | No |
| DOE | No Response | | NCTC | Yes |
| DOI | No | | Treasury | Not Applicable |

GOAL 4

## *13d. CISS Technical Standards:*

| Measurement Objective | Adopt ISE standards. | | |
|---|---|---|---|
| **2010 Metric** | 6 out of 15 ISE departments and agencies have incorporated CISS Technical Standards into enterprise architectures and IT capability. | | |
| **Agency** | **2010 Response** | **Agency** | **2010 Response** |
| CIA | No | DOJ | Yes |
| DHS | Yes | DoS | No |
| ODNI | No | DOT | No Response |
| DOC | Not Applicable | FBI | Yes |
| DoD/JCS | Yes | HHS | No |
| DOE | No response | NCTC | Yes |
| DOI | Yes | Treasury | Not Applicable |

| 2010 Highlight | **Adoption of ISE standards by ISE departments and agencies has been limited to this point.** |
|---|---|

## *14. Investment and Performance Integration*

| Measurement Objective | Further integrate ISE investment and performance management initiatives into department and agency management structures throughout-year planning and increased involvement of Performance Improvement Officers. | | |
|---|---|---|---|
| **2010 Metric** | 12 out of 15 ISE departments and agencies apply transition plans and relevant Segment Architecture transition plans at key decision points in the IT capital planning and investment cycle. | | |
| **Agency** | **2010 Response** | **Agency** | **2010 Response** |
| CIA | Yes | DOJ | Yes |
| DHS | Yes | DoS | Yes |
| ODNI | Yes | DOT | Yes |
| DOC | Not Applicable | FBI | Yes |
| DoD/JCS | Yes | HHS | No |
| DOE | No Response | NCTC | Yes |
| DOI | Yes | Treasury | Yes |
| **2010 Highlight** | **One approach to measuring how well an agency is linking performance and investment is to identify points in the investment cycle where the enterprise architecture is factored into investment decisions. As of Spring 2010, 12 out of 15 ISE departments and agencies had demonstrated that they have applied enterprise architecture transition plans at key decision points in their IT investment cycle.** | | |

# APPENDIX B – ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ACTIC | Arizona Counterterrorism Information Center |
| ADA | Aviation Security and the Air Domain Awareness |
| AICP | Authorized Intelligence Community Personnel |
| AIS | Automatic Identification System |
| ARJIS | Automated Regional Justice Information System |
| ATF | Bureau of Alcohol, Tobacco, Firearms, and Explosives |
| AWN | Alerts, Warnings, and Notifications |
| BCOT | Building Communities of Trust |
| BJA | Bureau of Justice Assistance |
| BLC | Baseline Capabilities |
| CAD/RMS | Computer Aided Dispatch/Record Management System |
| CBP | Customs and Border Protection (DHS) |
| CIA | Central Intelligence Agency |
| CICC | Criminal Intelligence Coordinating Council |
| CIKR | Critical Infrastructure and Key Resources |
| CIO | Chief Information Officer |
| CISA | Criminal Information Sharing and Analysis Unit (Hennepin County, MN) |
| CISO | Chief Information Sharing Officer (FBI) |
| CISS | Common Information Sharing Standards |
| CJIS | Criminal Justice Information Services |
| CL | Civil Liberties |
| CNSS | Committee on National Security Systems |
| CONOPS | Concept of Operations |
| COPS | Community Oriented Policing Services |
| CPIC | Capital Planning and Investment Control |
| CT | Counterterrorism |
| CUI | Controlled Unclassified Information |
| DHS | Department of Homeland Security |
| DNI | Director of National Intelligence |
| DOC | Department of Commerce |
| DoD | Department of Defense |
| DOE | Department of Energy |
| DOI | Department of the Interior |
| DOJ | Department of Justice |

| | |
|---|---|
| DoS | Department of State |
| DOT | Department of Transportation |
| EA | Enterprise Architecture |
| EAF | Enterprise Architecture Framework |
| EO | Executive Order |
| E.U. | European Union |
| FAMS | Federal Air Marshall Service |
| FBI | Federal Bureau of Investigation |
| FBINet | Federal Bureau of Investigation Secret Domain Network |
| FCMG | Fusion Center Management Group |
| FEA | Federal Enterprise Architecture |
| FEMA | Federal Emergency Management Agency |
| FICAM | Federal Identity, Credential, and Access Management |
| FIRES | Foreign Intelligence Relationship Enterprise System |
| FS | Functional Standards |
| FSAM | Federal Segment Architecture Methodology |
| FY | Fiscal Year |
| GES | Global Enrollment System |
| GJXDM | Global Justice Extensible Markup Language Data Model |
| GLOBAL | Global Justice Information Sharing Initiative |
| HHS | Department of Health and Human Services |
| HPD | Honolulu Police department |
| HQ | Headquarters |
| HSDN | Homeland Security Data Network |
| HSIN | Homeland Security Information Network |
| IACP | International Association of Chiefs of Police |
| IAFIS | Integrated Automated Fingerprint System |
| IC | Intelligence Community |
| ICD | Intelligence Community Directive |
| ICE | Immigration and Customs Enforcement (DHS) |
| ICAM | Identity, Credential, and Access Management |
| IdAM | Identity and Access Management |
| IEPD | Information Exchange Package Description |
| IIFC | Indiana Intelligence Fusion Center |
| IMO | International Maritime Organization |
| Intelink-U | IC Information System for the Unclassified Domain |
| IPC | Interagency Policy Committee |
| IRTPA | Intelligence Reform and Terrorism Prevention Act of 2004 |
| ISA | Information Sharing and Access |
| ISE | Information Sharing Environment |

| | |
|---|---|
| ISE EAF | Information Sharing Environment Enterprise Architecture Framework |
| ISM | Information Security Markings Standard |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITACG | Interagency Threat Assessment and Coordination Group |
| JCS | Joint Chiefs of Staff |
| JRA | Justice Reference Architecture |
| JTTF | Joint Terrorism Task Force |
| KST | Known or Suspected Terrorist |
| LEGAT | Legal Attaché (FBI) |
| LEISP | Law Enforcement Information Sharing Program |
| LEISS | Law Enforcement Information Sharing Service |
| LEO | Law Enforcement Online |
| LEXS | Law Enforcement Information Sharing Program Exchange Specification |
| LInX | Law Enforcement Information Exchange |
| LNI | Library of National Intelligence |
| MCCA | Major City Chiefs Association |
| MCSA | Major County Sheriffs Association |
| MDA | Maritime Domain Awareness |
| MIAC | Missouri Information Analysis Center |
| MIEM | Maritime Information Exchange Model (now known as NIEM Maritime) |
| MOA | Memorandum of Agreement |
| NARA | National Archives and Records Administration |
| NCIC | National Crime Information Center |
| NCIS | Naval Criminal Investigative Service |
| NCTC | National Counterterrorism Center |
| N-DEx | Law Enforcement National Data Exchange |
| NICS | National Instant Criminal Background Check System |
| NIEM | National Information Exchange Model |
| NIST | National Institute for Standards and Technology |
| NLETS | National Law Enforcement Telecommunications System |
| NRC | Nuclear Regulatory Commission |
| NSI | Nationwide SAR Initiative |
| NSIS | National Strategy for Information Sharing |
| NSS | National Security Systems |
| NTC-P | National Targeting Center-Passenger (DHS CBP) |
| NSTC | National Science and Technology Council |
| ODNI | Office of the Director of National Intelligence |
| OMB | Office of Management and Budget |
| OneDOJ | Unified DOJ Information Sharing Support (formerly R-DEx) |

| | |
|---|---|
| P&II | Performance and Investment Integration |
| Pac Clear | Pacific Regional Information Clearinghouse |
| PAIS | Profile and Architecture Implementation Strategy |
| PGC | Privacy Guidelines Committee (ISE) |
| PIN | Priority Information Need |
| PMO | Program Management Office |
| PM-ISE | Program Manager, Information Sharing Environment |
| RCMP | Royal Canadian Mounted Police |
| RCR | Roll Call Release |
| R-DEx | Regional Data Exchange |
| RISS | Regional Information Sharing System |
| RISSNET | Regional Information Sharing System Network |
| SAR | Suspicious Activity Reporting |
| SBU | Sensitive But Unclassified |
| SIPRNet | Secret Internet Protocol Router Network |
| SISA | Secure Information Sharing Award (DoD) |
| SLIAG | Senior Level Interagency Advisory Group |
| SLT | State, Local, and Tribal |
| SSCI | Senate Select Committee on Intelligence |
| SSP | Service Specification Package |
| TIN | Terrorism Information Need |
| TSA | Transportation Security Administration (DHS) |
| TSC | Terrorist Screening Center |
| TSDB | Terrorist Screening Data Base |
| TWG | Tribal Working Group |
| TWPDES | Terrorist Watchlist Person Data Exchange Standard |
| UCORE | Universal Core |
| VAR | Vessel Activity Report |
| WMD | Weapons of Mass Destruction |
| XML | Extensible Markup Language |


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

202.331.2490

Visit us on the web at http://ise.gov