







This page intentionally left blank.

# CONTENTS

<b>INTRODUCTION</b> .....	<b>1</b>
What Is the ISE? .....	1
Purpose .....	2
Guidance and Directives .....	3
How to Use this Document .....	3
<b>1 GOVERNANCE AND POLICY</b> .....	<b>5</b>
1.1 Governance .....	5
1.1.1 Information Sharing and Access Interagency Policy Committee .....	5
1.1.2 Senior Information Sharing and Safeguarding Steering Committee .....	6
1.1.3 Convening/Liaison .....	6
1.1.4 Implementing Responsible Information Sharing and Safeguarding Governance in Your Organization .....	7
1.2 Policy .....	9
1.2.1 ISE-wide Policy .....	9
1.2.2 Implementing ISE Policy in Your Organization .....	10
<b>2 BUDGET AND PERFORMANCE</b> .....	<b>13</b>
2.1 Annual Budget Planning Cycle .....	14
2.2 The ISE Performance Framework .....	15
<b>3 INTEROPERABILITY AND STANDARDS</b> .....	<b>18</b>
3.1 ISE Interoperability Framework (I <sup>2</sup> F) .....	18
3.2 Standards Development Process and Governance .....	20
3.2.1 Standards Frameworks .....	20
3.2.2 Additional Resources .....	23
3.3 Implementing Standards in Your Organization .....	23
3.3.1 Requirements .....	23
3.3.2 Standards-Based Acquisition .....	23
<b>4 COMMUNICATIONS AND PARTNERSHIPS</b> .....	<b>25</b>
4.1 Setting Communication Goals .....	25
4.1.1 Prioritizing Your Partners and Segmenting Your Communications .....	25
4.1.2 Messaging and Communications Vehicles .....	26
4.2 Partnering with Key ISE Organizations .....	27
4.2.1 State and Local Partnerships .....	27
4.2.2 Private Sector Partnerships .....	28
4.2.3 International Partnerships .....	28
4.3 Implementing an ISE Culture in Your Organization .....	29
4.3.1 Training .....	30
4.3.2 Awards, Performance and Appraisal Incentives .....	30
4.4 Piloting .....	30
<b>5 CALL TO ACTION</b> .....	<b>32</b>
<b>APPENDIX A: CAPABILITY AREAS AND MATURITY</b> .....	<b>33</b>

This page intentionally left blank.

# INTRODUCTION

## WHAT IS THE ISE?

Our national security depends on our ability to responsibly share the right information, with the right people, at the right time.

---

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

NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING,  
DECEMBER 2012

---

The idea of the Information Sharing Environment (ISE) originated in the [9/11 Commission Report](#) and was mandated in §1016 of the [Intelligence Reform and Terrorism Prevention Act of 2004](#) (IRTPA), as amended. The Act required the President to create a distributed and decentralized Information Sharing Environment (ISE) to facilitate the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties; and to designate a Program Manager responsible for planning for, overseeing the development of, and managing the ISE. The creation of the Office of the Program Manager for the Information Sharing Environment (PM-ISE) and the history of the ISE are detailed chronologically in [PM-ISE's Facebook timeline](#), with links available to relevant documents on [ise.gov](#).

Our nation continues to face significant challenges in analyzing and disseminating terrorism, WMD, and homeland security related information. Today, ISE partners are primarily focused on implementing the [National Strategy for Information Sharing and Safeguarding](#) (National Strategy), released in December 2012. We use its three principles: 1) information is a national asset, 2) information sharing and safeguarding requires shared risk management, and 3) information informs decision-making to guide our actions. The scope of the National Strategy is not limited to terrorism, homeland security, and weapons of mass destruction information, but has grown to encompass public safety and security mission areas. ISE solutions, processes, best practices, and tools are being reused and extended to help realize the vision of the IRTPA and the National Strategy.

## ISE PRINCIPLES IN ACTION

- Lower program risk by highlighting proven processes and practices
- Increase program efficiency through use of standards and reuse of innovations and capabilities
- Accelerate mission impact through strong alignment to National Strategy, and policy frameworks
- Sustain responsible collaboration among federal, state, local, tribal, territorial, private sector, and foreign partners through streamlined policies, reduced cultural barriers, and better integrated information systems

## PURPOSE

The purpose of this ISE Management Plan (Management Plan) is to provide common business processes and tools to enable collaboration among ISE stakeholders, which include federal, state, local, tribal, territorial, private sector, and international partners. The goal is to unify efforts across government to advance the implementation of an environment that facilitates information sharing among partners, governs a complex set of stakeholders, advances standards and uniform policies and procedures, and enables interoperability across many networks and systems.

This Management Plan is a resource for ISE stakeholders at all levels of government and the private sector, from chief information officers (CIOs) to program managers. The tools serve to provide guidance, directives, processes, practices, tools, and illustrative use cases to help them:

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

## WHY ENGAGE? THE IMPORTANCE OF BEING AN ISE PARTNER

Each new ISE partner is strengthened by, and strengthens, the ISE as a whole because:

- We are driven by common requirements for responsible information sharing
- We benefit from leveraging the work of partners whose missions align with our own
- The ISE connects and builds on existing systems
- ISE solutions support analysis, investigations, and operations at and across all security levels
- ISE solutions allow us to share information across mission domains and with multiple missions partners

## GUIDANCE AND DIRECTIVES

In addition to IRTPA §1016 and the National Strategy, further Executive Branch guidance on the ISE is provided in the following documentation:

- [Executive Order 13388](#), *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, October 2005;
- The [National Strategy for Information Sharing](#), October 2007;
- [Executive Order 13587](#), *Structural Reforms to Improve Sharing and Safeguarding of Classified Information on Computer Networks*, October 2011;
- Programmatic Guidance issued by National Security Staff (NSS) and Office of Management and Budget (OMB) to federal agencies for their respective budget preparation;<sup>1</sup>
- Annual Implementation Guidance issued by PM-ISE, in collaboration with the Information Sharing and Access Interagency Policy Committee (ISA IPC) members.

A good resource to trace the evolution of the Information Sharing Environment (ISE) in the context of information sharing reforms and goals for the future of responsible information sharing is [A Brief History of the ISE](#). A comprehensive list of guidance and directives can be accessed in our [document library online](#).

## HOW TO USE THIS DOCUMENT

This document has four sections that provide details on the common processes and tools available to help you achieve your information sharing and safeguarding goals as a part of the ISE:

1. Governance and policy
2. Budget and performance
3. Standards and interoperability
4. Communications

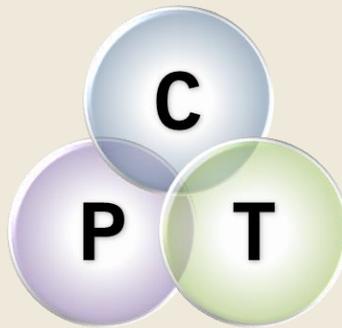
Each section describes the specific steps to take and the resources available to help reach your responsible information sharing goals. Throughout the document, examples illustrate how partners are participating in and benefiting from the ISE's processes and tools. The [ISE Building Blocks](#), a knowledge management tool available on [ise.gov](#), is an important companion to this management plan and is organized in a similar manner. It contains many important [toolkits](#), lessons learned, successes, and best practices from our partners who are building their responsible information sharing programs.

---

<sup>1</sup> Programmatic Guidance is issued only when significant program changes are expected of federal agencies.

## ASSESSING THE MATURITY OF ISE MANAGEMENT CAPABILITIES

The vision of the National Strategy will be achieved only through maturing our collective ability to use shared and common solutions, tools, and processes. PM-ISE assesses maturity using the ISE performance management framework, which aligns the goals in the National Strategy to ISE implementation guidance and measures of performance. The annual ISE performance assessment questionnaire, sent to and completed by ISE Stakeholders, provides the basis for PM-ISE to make this assessment. In addition to being aligned to the goals of the National Strategy, each question is also aligned to one or more of the following capability areas: community, process, and/or technology. Responses allow PM-ISE to measure how the ISE, as a whole, is progressing within each area. Throughout this Management Plan, you will find variations of the following illustration:



The circles represent the capability areas of community (blue circle with C), process (purple circle with P), or technology (green circle with T) used in the performance framework. The tools discussed in this Management Plan align to one or more of these categories. That alignment will be noted by the inclusion of the graphic next to each section in this Management Plan that discusses a tool, with the letters relevant to that tool displayed in the appropriate circle. For instance, if a tool can be used to help an ISE Stakeholder both improve a business process and standardize system acquisition, the letters P and T will appear in the purple and green circles; the letter C will be absent from the blue circle. These illustrations alert the reader that there is a performance-related question, with associated measures, in the ISE performance framework designed to assess the maturity of the use and efficacy of this tool.

PM-ISE will also develop new performance questions, where needed, for use in future ISE Performance Assessment Questionnaires. Appendix A describes the capability areas against a spectrum of maturity and includes notional performance assessment questions that can be used by ISE Stakeholders to self-assess their maturity level.

ISE Stakeholders' responses to the 2013 performance assessment questionnaire and PM-ISE's assessment of maturity by capability area can be found in Appendix A of the [2013 ISE Annual Report to the Congress](#).

# 1 GOVERNANCE AND POLICY

Governance and policy are used to drive the ISE toward coordinated and integrated resources and successfully implementing of the objectives of the National Strategy. Success depends upon all ISE partners participating in ISE governance processes and adopting or aligning policies that will ensure that we are working together in our implementation efforts, at all levels of government and in the private sector.

## 1.1 GOVERNANCE

Governance facilitates sharing and safeguarding of information by providing structure for the development and implementation of policy. The two primary senior governance bodies for ISE Stakeholders are the Information Sharing and Access Interagency Policy Committee (ISA IPC) and the Senior Information Sharing and Safeguarding Steering Committee (Steering Committee). These forums facilitate governance for responsible information sharing and safeguarding for all ISE partners at the level of the Executive Office of the President, in accordance with [Presidential Policy Directive \(PPD\) – 1, Organization of the National Security Council System](#) and [Executive Order 13587](#).



### 1.1.1 INFORMATION SHARING AND ACCESS INTERAGENCY POLICY COMMITTEE

The ISA IPC is co-chaired by the National Security Staff’s Senior Director for Information Sharing Policy and the Program Manager for the Information Sharing Environment. While membership of the ISA IPC is restricted by law to federal departments and agencies, the ISA IPC scope includes all levels of government. ISA IPC subcommittees and working groups include federal, state, local, tribal and territorial mission owners as well as private sector partners. To ensure the candid and timely discussion of information sharing challenges that require policy action, the ISA IPC and its subsidiary groups are exempt from the [Federal Advisory Committee Act](#).

The ISA IPC is guiding the implementation of each of the [National Strategy’s 16 priority objectives](#). Each priority objective is assigned a steward, or governance body responsible for directing, managing and monitoring implementation of the priority objective. The subcommittees of the ISA IPC are working to implement the objectives of the National Strategy, and in so doing develop goals that are approved and monitored by the ISA IPC. Representatives from ISE agencies, our ISE mission partners, chair these governance bodies and help to formulate implementation plans for their assigned objective(s). These plans are vetted with ISE stakeholders through the ISA IPC and include control milestones and performance measures that allow the ISA IPC to monitor National Strategy implementation. Subcommittees of the ISA IPC may formally charter working groups or create Tiger Teams to focus on narrower issues within a portfolio.

For more information on how to participate in National Strategy implementation, or for information on the current structure and activities of the ISA IPC, contact your agency's representative or PM-ISE's Management and Oversight Division at [DNI-PM-ISE-EXECSEC@dni.gov](mailto:DNI-PM-ISE-EXECSEC@dni.gov).

### 1.1.2 SENIOR INFORMATION SHARING AND SAFEGUARDING STEERING COMMITTEE

The President established the Steering Committee in [Executive Order 13587](#) to exercise overall responsibility and ensure senior-level accountability for interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

The Steering Committee is co-chaired by senior representatives from NSS and the OMB E-Gov office. Membership includes representatives from Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration.

The Classified Information Sharing and Safeguarding Office (CISSO), which is a component of the office of the PM-ISE, provide executive secretariat functions for the Steering Committee and collects data from agencies on the progress and performance of their safeguarding efforts. This data informs the Steering Committee's Annual Report to the President, which provides the White House an account of information sharing and safeguarding successes and challenges.

The current priorities of the Steering Committee are outlined in Priority Objective 5 of the National Strategy: *Implement removable media policies, processes and controls; provide timely audit capabilities of assets, vulnerabilities and threats; establish programs, processes and techniques to deter, detect and disrupt insider threats; and share the management of risks, to enhance unclassified and classified information safeguarding efforts.* If you would like more information, please contact the CISSO at [PM-ISE-CISSO@dni.gov](mailto:PM-ISE-CISSO@dni.gov).

### 1.1.3 CONVENING/LIAISON

Because the office of the PM-ISE is in a unique position to facilitate responsible information sharing across the whole of government, we play a neutral role when negotiating between mission interests of ISE stakeholders. The capability to convene stakeholders provides opportunities for constructive exchanges in a shared setting, as well as active listening among organizations with different missions, authorities, and resources. PM-ISE fills the role of honest broker to help non-federal players develop their requirements and inject them into national policy deliberations. When there are asymmetries between stakeholders, PM-ISE's ability to aggregate the concerns of less influential stakeholders is critical to the ultimate success of shared solutions. For example, PM-ISE's facilitation of interactions between and among individual fusion

centers and their federal partners has increased the collective voice of the network of fusion centers. Additionally, a key role for PM-ISE and governance bodies is to identify technologies, capabilities, and services that can be shared across the ISE with the intent to leverage individual agency initiatives for the greater good.

ISE Stakeholders and priorities are often discussed in the [Federal CIO Council](#), the [Committee on National Security Systems](#), the [Domestic Security Alliance Council](#), and [other interagency forums](#). The office of the PM-ISE often works on behalf of agencies to clarify governance relationships, share ideas and deconflict tasks across these forums. For information on how to appropriately interface with these bodies, contact the PM-ISE Management and Oversight Division at [DNI-PM-ISE-EXECSEC@dni.gov](mailto:DNI-PM-ISE-EXECSEC@dni.gov).

#### **FUSION CENTERS AND PRIVATE SECTOR COME TOGETHER ON CYBERSECURITY**

Agencies are undertaking new and emerging information sharing initiatives beyond traditional terrorism and homeland security missions. One example is ISE best practices and solutions supporting the cybersecurity mission and the priorities of the White House National Security Staff Cyber Directorate. PM-ISE, with the National Fusion Center Association and the International Association of Chiefs of Police, convened stakeholders from law enforcement, homeland security, emergency management, information technology, and the private sector to clarify [requirements for sharing both tactical and strategic cybersecurity](#) information and to plan pilots for demonstrating these capabilities. For more details on this and other information sharing pilots, please contact the PM-ISE Mission Programs Division at [DNI-PM-ISE-EXECSEC@dni.gov](mailto:DNI-PM-ISE-EXECSEC@dni.gov).

### **1.1.4 IMPLEMENTING RESPONSIBLE INFORMATION SHARING AND SAFEGUARDING GOVERNANCE IN YOUR ORGANIZATION**

Effective and responsible information sharing and safeguarding requires strong commitment and participation from ISE partners. Developing effective internal governance structures, designating a senior information sharing and safeguarding executive in your organization, and developing information sharing goals aligned with the National Strategy are all practical measures to ensure that information sharing and risk management goals are fully integrated in your day-to-day operations.

Mature governance structures also adhere to a performance management cycle that is results-oriented, enforces accountability, and allows data-driven decisions on technology investments and other initiatives. Agencies should have a means to apply the goals and activities of the National Strategy to support their internal efforts and establish means to track and document the benefits of those activities. Effective agency governance structures also enable agencies to offer

and reuse capabilities and services for sharing across the environment, consistent with an interoperable architecture approach.

To get started, make contact with the governance bodies that serve your community. See [ISE Building Blocks](#) or for more information please contact the PM-ISE Management and Oversight Division at [DNI-PM-ISE-EXECSEC@dni.gov](mailto:DNI-PM-ISE-EXECSEC@dni.gov).

## **BENEFITS OF PARTICIPATION IN ISE GOVERNANCE PROCESSES**

Your involvement in ISE governance bodies provides opportunities to advise the NSS and the PM-ISE and to coordinate with other departments and agencies as we develop and implement guidelines, policies, processes, practices, standards, and tools. Your involvement will help identify gaps in policies, technologies, programs and systems used by federal departments and agencies to share and safeguard information and will ensure that any initiatives developed to address these gaps include your equities. Through this involvement, the ISE’s annual planning process (described later in Figure 2) will be informed by your needs, challenges, and opportunities and you can share and reuse best practices from other ISE partners. As the ISE is implemented and expands to new missions and new categories of information, based on White House direction, your involvement will guide and support that growth, and ensure good stewardship of resources by sharing and reusing ISE solutions.

### **EXAMPLES OF EFFECTIVE GOVERNANCE**

#### **Office of the Director of National Intelligence**

The ODNI leadership is committed to information sharing across the 16 agencies of the Intelligence Community (IC). The DNI’s 2011-2015 Strategic Intent for Information Sharing provides the framework to improve responsible and secure information sharing across the IC and with external partners and customers. It supports the DNI’s strategic goal to “Drive Responsible and Secure Information Sharing,” and is consistent with both the National Intelligence Strategy and the Administration’s priorities for information sharing and safeguarding. The ODNI oversees the implementation of the strategy’s goals through the IC Information Sharing Steering Committee—the IC’s executive-level information sharing governance body. The IC Information Sharing and Safeguarding Executive is a member of both the ISA IPC and the Steering Committee, and collaborates very closely with PM-ISE to identify best practices for information sharing across the federal government. ODNI makes responsible information sharing a priority and gives weight to their information sharing initiatives—backing them with the authority of their most senior leaders. ODNI and National Counterterrorism Center (NCTC) senior leadership, such as the Civil Liberties Protection Officer, serve in key leadership roles on ISA IPC subcommittees and working groups.

### Federal CIO Council

The Federal CIO Council (Council) promotes and advances the use of interagency shared services for commodity information technology, support, and mission services. The Council has created a [Federal Shared Services Implementation Guide](#) that provides information and guidance on the provisioning and consumption of shared services in the Federal Government. The guide provides agencies with a high-level process and key considerations for defining, establishing, and implementing shared services to help achieve organizational goals, improve performance, increase return on investment, and promote innovation. The Council develops and maintains valuable tools, services, and data for CIOs and other federal IT workers—like the Federal Shared Services Implementation Guide—primarily through three core committees: 1) Innovation, 2) Portfolio Management, and 3) Information Security and Identity Management. These groups oversee short-term projects and deliverables as well as longer-term initiatives aimed at informing federal IT strategy. By working within a structure that combines formal committees, short-term agile working groups, and communities of knowledge experts, the Council is poised to help address the most relevant and pressing IT issues across the Federal CIO community.

## 1.2 POLICY

Policy provides direction on mission, budget, and strategic priorities. It serves to standardize processes and coordinate activities; to promote the use of innovative solutions and best practices; and to communicate guidance between leadership and operational components.



The ISE is built upon two levels of policy: ISE-wide policy frameworks and agency-specific policies developed to address ISE requirements.

### 1.2.1 ISE-WIDE POLICY

ISE-wide policy frameworks are important because ISE initiatives regularly span some or all of our partner communities—from federal agencies, to state and local law enforcement, to private sector owners and operators of critical infrastructures—requiring partners to develop policies that comply with the broader requirements of ISE participation within their own authorities and missions.

The ISE Policy Lifecycle, as depicted in Figure 1, outlines the steps for developing, implementing, and evaluating policies, and lays out best practices for ISE partners to use for their agency-specific policy development and implementation.

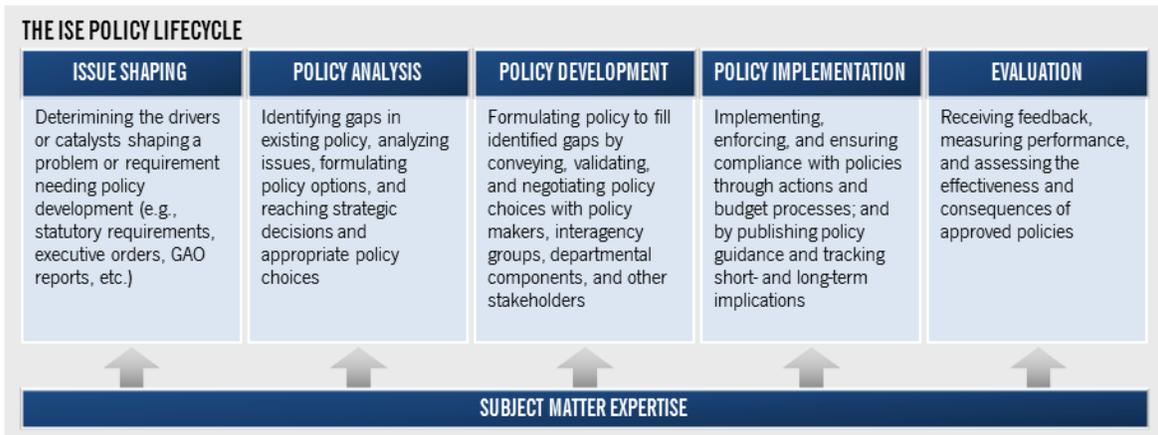


Figure 1. The ISE Policy Lifecycle

Proposals to share data across entities often encounter a familiar refrain: “There’s a legal problem – we can’t share the information.” The ISE policy framework cannot address specific scenarios, but does provide an approach for addressing information sharing legal challenges, and more importantly a forum to discuss these challenges. The ISA IPC is working on best practices and tool kits for data aggregation and related information sharing agreements to define common approaches for these challenges. The conversation begins with the mission and authorities that already exist within departments and agencies at all levels of government. The ISE relies on the expertise and advice from counsel within each department or agency to ensure that ISE policy meets the letter and intent of legal requirements. Additional detail on this [legal and policy approach for responsible information sharing](#) can be found on [ise.gov](#).

### 1.2.2 IMPLEMENTING ISE POLICY IN YOUR ORGANIZATION

The success of the ISE depends upon ISE Stakeholders implementing policies for responsible information sharing that support their missions and are compliant with ISE-wide frameworks. For example, general ISE guidance has been provided to agencies to integrate information sharing responsibilities into employee performance assessments [Performance Evaluation Element in Employee Performance Appraisals](#) (ISE-G-105) and to mandate the use of [Core Awareness Training](#) (ISE-G-104) across ISE mission partners. It is incumbent upon ISE Agency leadership to issue and implement internal policies that comply with this guidance.

Below is an example of how an ISE-wide policy requirement has been implemented by ISE mission partners through agency-specific policies.

**SHARING INFORMATION AND PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES**

As envisioned by IRTPA and stated in Homeland Security Presidential Directives 6 and 11, “the policy of the United States Government is to share terrorism information to the full extent permitted by law.” IRTPA requires information sharing activities to be conducted in a manner consistent with the provisions of the Constitution and applicable laws, including those protecting the legal rights of all Americans.

In 2006, in response to the privacy and civil liberties requirements outlined in IRTPA, the White House issued a set of policies and procedures to protect the information privacy and legal rights of Americans during information sharing activities. The ISE Privacy Guidelines establish the standards by which both Federal and non-Federal ISE partners must protect the privacy, civil rights, and civil liberties (P/CR/CL) of individuals through the development and adoption of agency-specific written P/CR/CL protection policies.

Since 2007, federal agencies and non-federal ISE mission partners made significant progress in developing agency-specific P/CR/CL protection policies consistent with the ISE Privacy Guidelines and in integrating P/CR/CL protections into ISE activities and programs. Today, nearly all federal agencies have developed and issued written P/CR/CL policies compliant with the ISE Privacy Guidelines. As of April 2011, all federally recognized state and major urban area fusion centers had completed P/CR/CL protection policies.

**BENEFITS OF PARTICIPATION IN THE ISE POLICY PROCESS**

Participation in the ISE policy process enables mission partners across communities to uniformly understand and apply ISE requirements while retaining flexibility to address their own mission requirements and authorities. A uniform approach also contributes to trusted partnerships, where one agency can be confident sharing information with another, if they are confident in that agency’s adoption of ISE requirements. This facilitates more efficient sharing of information and awareness of protected information.

The following example illustrates the benefits of ISE-wide policy frameworks.

## FEDERAL RESOURCE ALLOCATION CRITERIA (RAC)

The [Federal Resource Allocation Criteria](#) (RAC) [ISE-G-112] provides federal agencies with objective criteria and a coordinated approach to determine how to prioritize and allocate resources to the National Network of Fusion Centers, as called for in the [2007 National Strategy for Information Sharing](#) (NSIS).

The goal of this policy is to enhance the effectiveness of federal support to the National Network of Fusion Centers. In the face of increasing demands and limited resources, the prioritized resource allocation established through the criteria in the RAC policy enables the federal government to concentrate resources to improve the efficiency of its support to fusion centers.

To develop and issue the RAC policy, DHS and PM-ISE worked together—via the ISA IPC’s Fusion Center Subcommittee—to create consensus among all stakeholders on how federal resources are to be prioritized and allocated, bringing transparency into the process. An analysis of current policies revealed that no policies existed to sufficiently address these issues.

PM-ISE issued the RAC as ISE guidance on behalf of the ISA IPC’s Fusion Center Subcommittee in 2011; and in our FY2014 ISE Implementation Guidance, we directed all ISE agencies to “deliver to DHS an inventory of all the steps agencies have taken to align resource decisions to the Federal RAC policy.” DHS then, through the ISA IPC’s Fusion Center Subcommittee, which they co-chair with the FBI, developed and distributed the “Federal RAC Policy Implementation Questionnaire” to ISE agencies. The responses to this questionnaire have provided a better understanding of the extent to which federal resources are deployed to fusion centers. Based on that feedback, the ISA IPC’s Fusion Center Subcommittee is in the process of developing a RAC implementation plan to better inform partners on budgetary and programmatic decisions when expending federal resources to the National Network of Fusion Centers.

For more information on how to work with PM-ISE to develop your own responsible information sharing policies, or to discuss how to ensure your policies comply with broader ISE frameworks, please contact the PM-ISE Management and Oversight Division at [DNI-PM-ISE-EXECSEC@dni.gov](mailto:DNI-PM-ISE-EXECSEC@dni.gov).

## 2 BUDGET AND PERFORMANCE

The ISE’s Annual Planning Cycle is shown below in Figure 2, focuses on implementing the 16 priority objectives of the [National Strategy](#). Driving the cycle are the implementation plans for the National Strategy’s priority objectives and the annual NSS and OMB Programmatic Guidance,<sup>2</sup> which guides federal agencies’ prioritization of ISE investments in their budget formulation process. The challenging fiscal environment necessitates the need for thoughtful choices that balance the need to meet current agency mission requirements with interoperable, standards-based solutions.

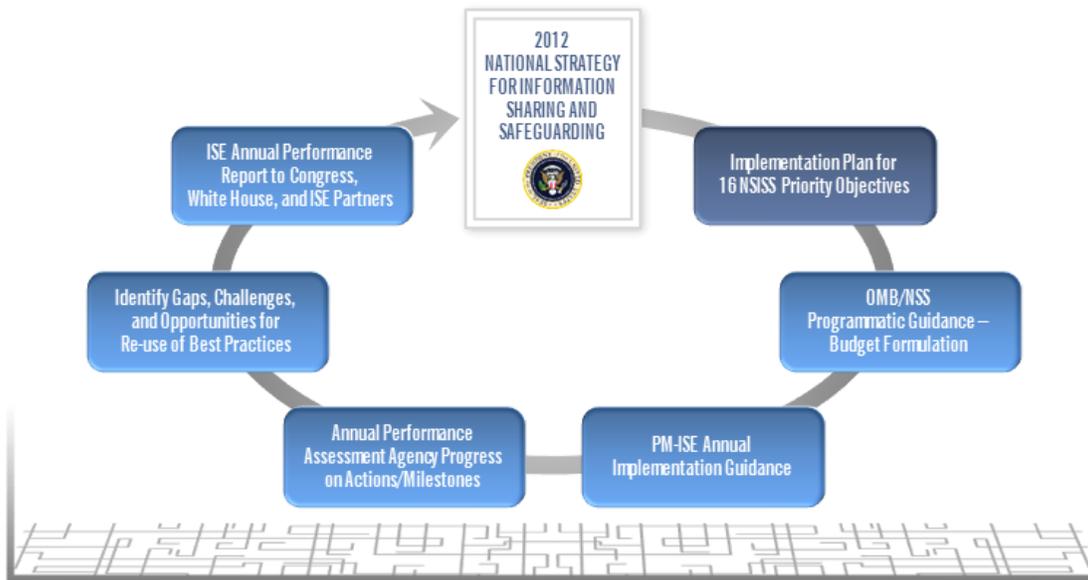


Figure 2. The ISE Annual Planning Cycle

<sup>2</sup> Programmatic Guidance is issued only when significant program changes are expected of federal agencies.

## 2.1 ANNUAL BUDGET PLANNING CYCLE



To more specifically implement White House priorities, PM-ISE publishes annual capability-focused ISE Implementation Guidance,<sup>3</sup> which is developed by PM-ISE in collaboration with federal ISE agencies via the ISA IPC and provides ISE agencies objective, system-wide performance goals for the following year as required by IRTPA §1016(h).<sup>4</sup> The ISE Implementation Guidance directly reflects the planning year actions associated with each the 16 priority objectives in the National Strategy. To measure agency performance against these goals, and in compliance with the [Government Performance and Results Modernization Act \(GPRM\) of 2010](#)<sup>5</sup> and OMB guidelines, the office of the PM-ISE conducts [ISE performance](#) assessments each year in the form of questionnaires sent to ISE agencies. Agency responses inform the [ISE's Performance Framework](#) and help PM-ISE measure progress toward realizing the National Strategy; the maturity of ISE initiatives; identifying gaps, challenges and opportunities to be addressed in the following year's planning; and comprise the basis for the annual ISE Report to the Congress.<sup>6</sup>

Responses to the annual performance assessment also help agencies examine their own programs that support the ISE, which can be helpful when:

- Communicating with OMB examiners;
- Ensuring that efforts to implement the National Strategy's priority objectives are aligned with performance measures and department or agency strategic goals; and,
- Making program and budget decisions in subsequent years.

The ISE Annual Planning Cycle demonstrates how the National Strategy, priorities, and implementation plans are linked in order to track, monitor, and provide and account for progress as transparently as possible.

<sup>3</sup> NSS and OMB Programmatic Guidance and PM-ISE Implementation Guidance are considered budget sensitive and an integral part of the budget deliberation process of the Executive Branch. Therefore, both documents are considered internal to the Executive Branch and should not be shared externally. Please contact your ISA IPC representative for a copy of these documents. Alternatively a summarized depiction of the guidance can be found in the ISE's Annual Report to the Congress.

<sup>4</sup> It is important to note that the guidance is specific to federal agencies, yet in many cases the agency actions are focused on initiatives which directly or indirectly involve non-federal ISE partners.

<sup>5</sup> The GPRM establishes the Federal Government's performance management framework and the Administration's approach to improving the effectiveness and efficiency of government.

<sup>6</sup> The ISE Annual Report to the Congress is a catalog that promotes reuse of best practices and solutions by highlighting accomplishments of ISE mission partners and showing trends in maturity through the compiled results of the ISE's performance assessment.

### OPPORTUNITY IN A CHALLENGING FISCAL ENVIRONMENT

Resource constraints, especially among state, local, tribal, and territorial (SLTT) law enforcement agencies, have necessitated the transformation of information sharing business models. Significant cost savings could be realized through consolidation, regionalization, and reuse of trusted open standards based IT platforms. One example is PM-ISE sponsorship of a [critical event deconfliction initiative](#) to identify nationwide deconfliction standards and solutions; connect deconfliction systems; and develop a nationwide deconfliction strategy.

## 2.2 THE ISE PERFORMANCE FRAMEWORK

The ISE Performance Framework, through the application of the ISE Annual Planning Cycle's tools, allows PM-ISE and ISE agencies to apply maturity-defined performance measures to monitor the performance of responsible information sharing initiatives. The framework aids PM-ISE and ISE agencies as they:



- Identify initiatives or capabilities that will help achieve strategic ISE goals
- Align initiatives with strategic objectives
- Identify gaps in these initiatives
- Fill the gaps and implement ISE best practices
- Develop measures to track information sharing progress and its impacts
- Implement a roadmap with milestones to track progress and impact

At the core of the ISE Performance Framework are the five goals of the National Strategy. PM-ISE aligns all responsible information sharing initiatives in the ISE with those goals and then identifies the technologies, processes, and community capabilities required to mature those initiatives to point where they achieve the goals as shown below in Figure 3.

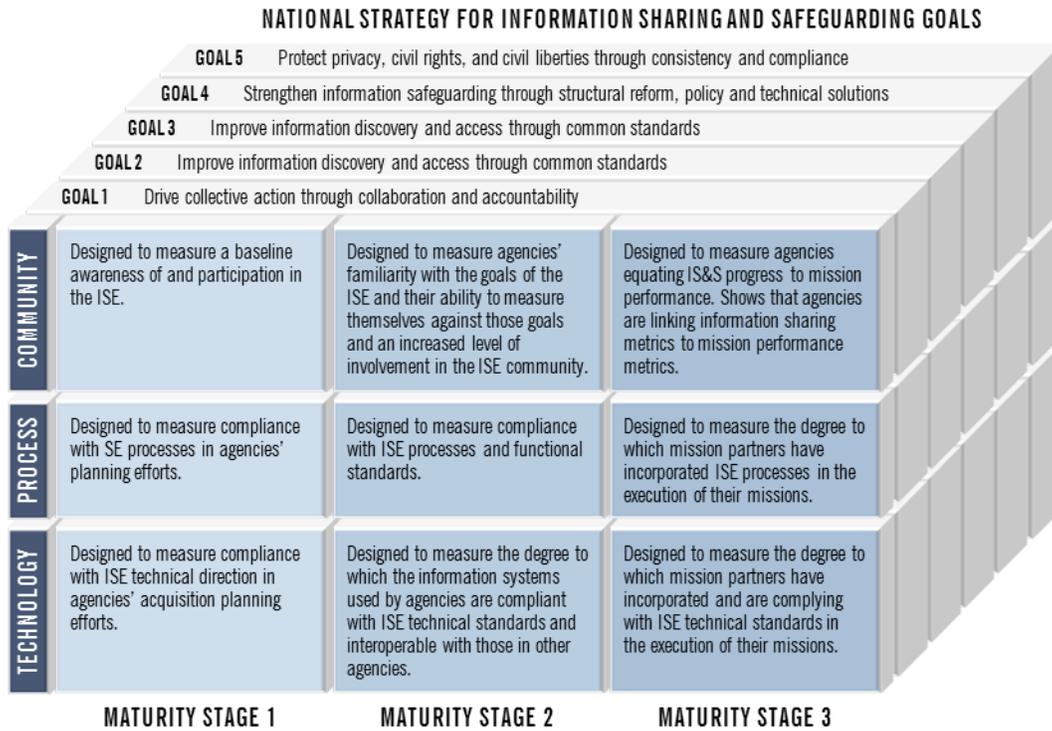


Figure 3. ISE Performance Framework

PM-ISE and mission partners continue to evolve performance measurement, including implementing outcome-based measures to help assess the national security results achieved through key initiatives. PM-ISE and ISE agencies have developed a series of performance scenarios to help agencies think about how information sharing and safeguarding efforts impact mission outcomes, and to help turn generic maturity definitions into measures that are specific to an ISE initiative. The scenarios take strategic information sharing requirements (e.g., get the right information to the right people at the right time) and apply them to real mission situations (e.g., a maritime security analyst identifies a specific threat in an eastern port). The scenarios illustrate that as responsible information sharing capabilities mature, ISE partners can see an improvement in their ability to accomplish their mission. The [Performance Scenario Guide](#) helps partner agencies develop performance case scenarios and plan and execute information sharing initiatives that are grounded in performance metrics.

This Management Plan provides common business processes and tools to enable stakeholder collaboration while executing the National Strategy, and as such will be integrated into future performance assessments and scenarios. See Appendix A for examples of how an agency can assess their maturity in using the tools described in this Management Plan.

**BENEFITS OF PARTICIPATION IN THE PERFORMANCE PROCESS**

The following example illustrates the benefits of participating in the process to develop annual guidance for the ISE; implementing that guidance within a defined governance structure; and measuring the performance of implementation to achieve information sharing capabilities.

**REQUIRING AND ENABLING THE SHARING OF INFORMATION AND PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES**

Both federal and non-federal partners are required to develop and implement written privacy, civil rights, and civil liberties (P/CR/CL) policies consistent with the ISE Privacy Guidelines. All of the abovementioned ISE management tools were used to accelerate the completion of ISE P/CR/CL protection policies by federal partners, resulting in the completion of policies by 93% of federal ISE mission partners. The 2013 ISE Performance Assessment measured the effectiveness of common P/CR/CL protections throughout ISE federal partners and found:

- ISE mission partners continue to develop and implement P/CR/CL protection policies as required by the ISE Privacy Guidelines to ensure that the information privacy and other legal rights of Americans are protected while exchanging data via the information sharing environment.
- Additional work is needed to increase the use of internal agency compliance, oversight, and accountability mechanisms for consistency in the application of P/CR/CL protections.

Beginning in 2010, DHS included special condition language in homeland security grants to state and local governments requiring that fusion centers complete ISE P/CR/CL protection policies within six months of receiving a grant award. The addition of this grant condition enabled all operational designated state and major urban area fusion centers to have completed ISE P/CR/CL protection policies as of April 2011.

If you would like more information on how to participate in the ISE budget and performance processes, please contact your agency ISA IPC representative, ISE performance point of contact, or PM-ISE Planning, Resources and Performance team at [DNI-PM-ISE-ExecSec@dni.gov](mailto:DNI-PM-ISE-ExecSec@dni.gov).

## 3 INTEROPERABILITY AND STANDARDS

The National Strategy places emphasis on improving information discovery and access through common standards; optimizing mission effectiveness through shared services and interoperability; and strengthening information safeguarding through structural reform, policy, and technical solutions.<sup>7</sup> Establishing a fully operational ISE necessitates interoperability across strategic information infrastructures of federal, state, local, tribal and territorial entities with counterterrorism and national security missions and the appropriate private sector and foreign partners.

---

Interoperability is the ability of various operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner.

U.S. CODE – TITLE 44: PUBLIC PRINTING AND DOCUMENTS

---

### 3.1 ISE INTEROPERABILITY FRAMEWORK (I<sup>2</sup>F)

[OMB Circular A-130](#) tasks executive-level agencies with developing enterprise architectures (EA), defined as “the explicit description and documentation of the current and desired relationships among business and management processes and information technology. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment.”



PM-ISE, in consultation with the Information Integration Subcommittee (IISC) of the ISA IPC, continues to develop the ISE Interoperability Framework (I<sup>2</sup>F) to enable interoperability across multiple domains and stakeholder communities. The I<sup>2</sup>F delivers a framework for *extensible, measurable, and implementable* interoperability requirements throughout the lifecycle of an investment and thus it will serve as a platform to enhance implementation of priority objectives in NSISS. The I<sup>2</sup>F will not define EA concepts that are within the scope of an organization’s internal EA Framework but will focus on guiding ISE partners in incorporating sharing and safeguarding information principles into agency-level architectures. Together with this ISE Management Plan, the I<sup>2</sup>F answers the call for an enterprise architecture program management plan that reflects relevant activities, events, and timeframes for improving ISE architecture, provides a means to address gaps, and establishes a mechanism for accountability and progress.

---

<sup>7</sup> White House, National Strategy for Information Sharing and Safeguarding, December 2012.

The I<sup>2</sup>F links three business and technical management practices and disciplines: 1) Architecture Framework Alignment, 2) the ISE Common Profile, and 3) ISE Industry Standards and Specifications Framework, all of which are designed to support interoperability requirements within the context of independent operational capabilities. The I<sup>2</sup>F describes an Integrated Landscape (I<sup>2</sup>FIL), which is realized through the application of the three linked practices and disciplines of the I<sup>2</sup>F. The standards based acquisition initiative is supported by the adoption of the I<sup>2</sup>F and its integrated management disciplines outlined in this section and depicted in Figure 4.

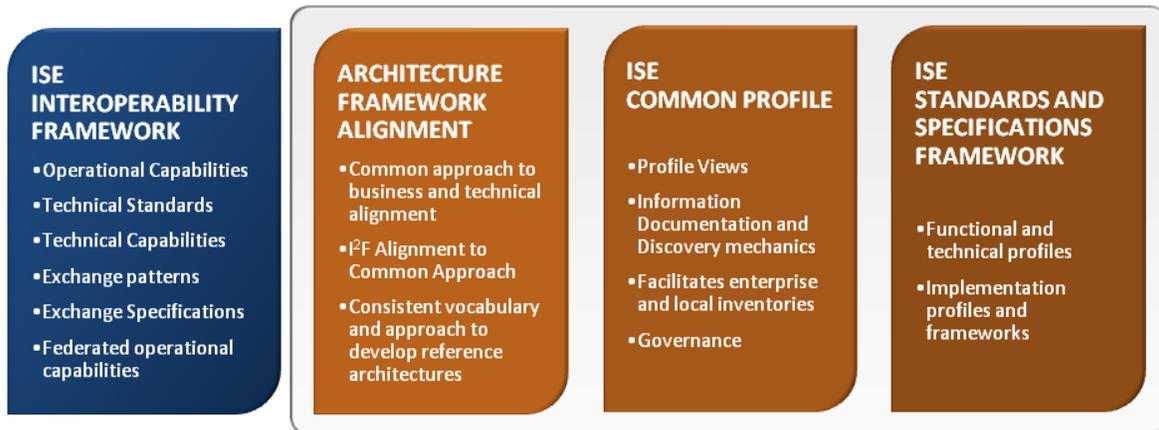


Figure 4. I<sup>2</sup>F Integrated Landscape

## BENEFITS OF USING THE I<sup>2</sup>F

The I<sup>2</sup>F provides a flexible, common method to implementing information exchange across a broad spectrum of information systems and distributed IT architectures. Reference architectures, or template solutions, currently included in the I<sup>2</sup>F are data aggregation, geospatial information, and identity management.

The I<sup>2</sup>F enables the discovery, reuse, and development of capabilities. When implemented through governance structures such as outlined in Section 1, it provides a means to identify technologies, capabilities, and services that can be shared across the ISE.

## ADDITIONAL RESOURCES

- [Executive Order 13642: Making Open and Machine Readable the New Default for Government Information](#), May, 2013
- [OMB Memorandum M-13-13: Open Data Policy – Managing Information as an Asset](#), May 2013
- [The Common Approach to Federal Enterprise Architecture](#), May 2012
- [ISE-G-108: Identity and Access Management Framework for the ISE](#), December 2008

- [ISE-G-109: ISE Enterprise Architecture Framework \(EAF\)](#), September 2008
- [ISE-G-110: ISE Profile and Architecture Implementation Strategy \(PAIS\)](#), May 2009

For more information, contact PM-ISE's Standards and Architecture Division at [DNI-PM-ISE-ExecSec@dni.gov](mailto:DNI-PM-ISE-ExecSec@dni.gov).

## 3.2 STANDARDS DEVELOPMENT PROCESS AND GOVERNANCE



[OMB Circular A-130](#) directs agencies to develop and maintain an EA Framework and to adopt and consistently enforce standards that support the entire EA.<sup>8</sup>

Common standards can define and normalize processes, all of which support the planning, integration, and implementation activities that impact an organization's internal and external information resources. Generally, information sharing standards are a combination of the data that needs to be shared and a technology or architectural environment that enables this sharing.

### 3.2.1 STANDARDS FRAMEWORKS

The ISE Standards and Specifications Framework, part of the I<sup>2</sup>F, is a more finely grained categorization taxonomy that defines a framework for understanding standards, the function they serve, involved stakeholders, and relationships between standards. An appendix of the I<sup>2</sup>F, the Common Profile Framework<sup>9</sup> provides the characteristics of a "profile" that enables interoperability. A profile characterizes a base set of standards with options necessary to facilitate the accomplishment of the organization's mission and provide a common methodology for referencing standards across multiple solutions. The Standards Working Group (SWG) and Standards Coordinating Council (SCC), both part of the ISA-IPC, are standing bodies of the IISC that evaluate existing standards and standards frameworks for reuse and also aid in the development of new standards. The process for identifying standards for reuse, and interaction between mission partners, governing bodies, industry, and standards development organizations is described in Figure 5.

<sup>8</sup> OMB Circular No. A-130 Revised: Management of Federal Information Resources (8)(b)(2)(c)(ii).

<sup>9</sup> The ISE Common Profile is a construct based on the ISO/IEC Technical Recommendation 10000-1.

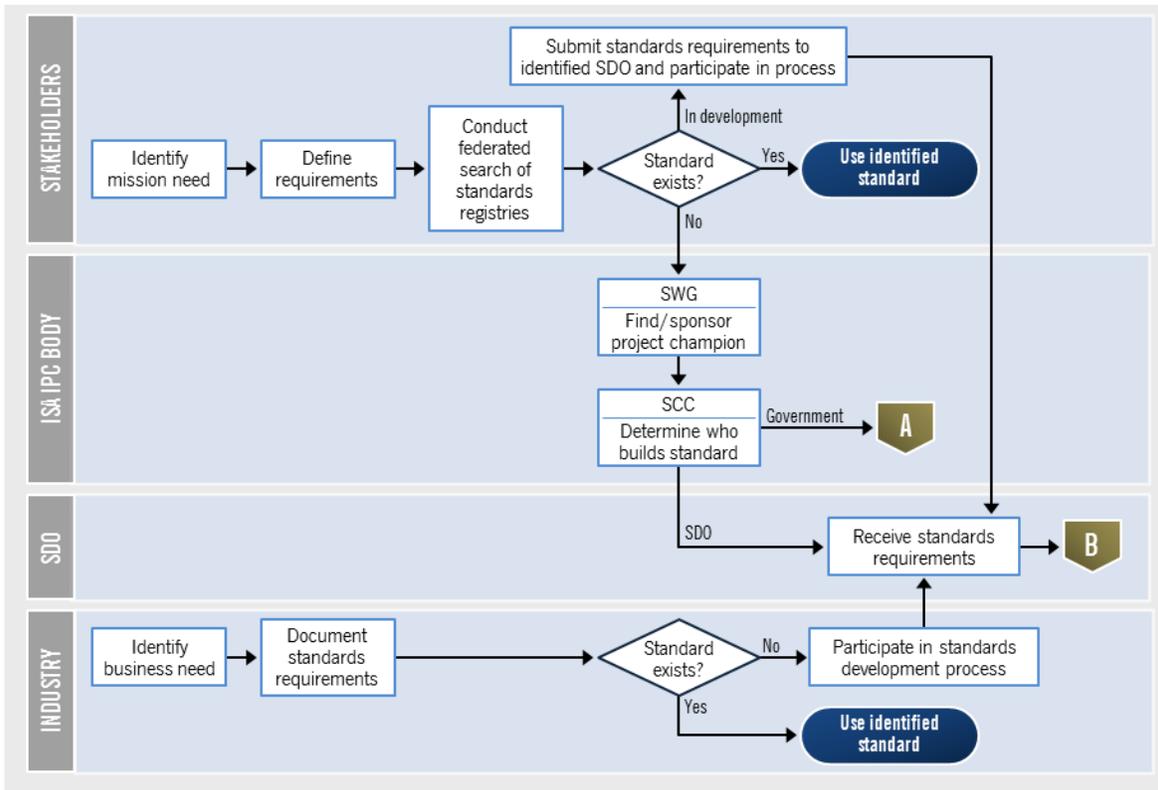


Figure 5. Standards Engagement Process

ISE implementation requires effective partnering between government and industry so that government’s interoperability requirements are transparent to industry, resulting in vendor solutions that meet these requirements with the appropriate standards “built in”. Industry and government standards and certification programs exist to provide an environment for:

- evaluating standards through a consensus process
- testing standards, and
- certifying projects through a conformance management process

## STANDARDS CONFORMANCE AND CERTIFICATION

In December 2012, the IJIS Institute Springboard<sup>10</sup> program conducted its first standards conformance test on the new Prescription Drug Monitoring Program (PDMP) Information Exchange (PMIX), to determine whether it met the required interoperability standards. PDMP is a web-based program that collects, analyzes, and reports information on the prescription, dispensation, and use of prescription drugs. Many states currently report problems with “pill mills”—doctors who prescribe large quantities of painkillers to people who do not need them medically—the sharing of information about prescription drugs is a crucial way to reduce prescription drug abuse.

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

### 3.2.1.1 NATIONAL INFORMATION EXCHANGE MODEL (NIEM)

One of the most widely adopted information sharing standards framework used by ISE partners is the National Information Exchange Model (NIEM). NIEM is a community driven, government-wide, standards-based approach that can support a community that requires interoperable information exchanges to advance their respective missions. For more information on the NIEM engagement process, contact the [National Information Sharing Standards \(NISS\) help desk](#) or visit the [NIEM website](#).

### 3.2.1.2 OPEN DATA STANDARDS

Presidential Executive Order 13642, [Making Open and Machine Readable the New Default for Government Information](#), and OMB’s Memorandum M-13-13 on [Managing Information as an Asset](#) establish a framework to help institutionalize the principles of effective information management at each stage of the information's life cycle to promote interoperability and openness. Whether or not particular information can be made public, agencies can apply this framework to all information resources to promote efficiency and produce value.

OMB M-13-13 requires agencies to collect or create information in a way that supports downstream information processing and dissemination activities. This includes:

<sup>10</sup> <http://ijis.org/programs/springboard.html>

- Using machine readable and open formats, data standards, and common core and extensible metadata for all new information creation and collection efforts,
- Information stewardship through the use of open licenses and review of information for privacy, confidentiality, security, or other restrictions to release, and
- Building or modernizing information systems in a way that maximizes interoperability and information accessibility, maintains internal and external data asset inventories, enhances information safeguards, and clarifies information management responsibilities.

### 3.2.2 ADDITIONAL RESOURCES

- [ISE-AM 300: Common Terrorism Information Sharing Standards \(CTISS\) Program](#), 2007
- [Common Terrorism Information Sharing Standards \(CTISS\) Program Manual](#), 2007
- [ISE-G-106: Technical Standards – Information Assurance October](#), 2008
- [ISE-G-107: Technical Standards – Core Transport October](#), 2008
- Links to existing standards: <http://ise.gov/building-blocks/standards-and-interoperability><sup>11</sup>

## 3.3 IMPLEMENTING STANDARDS IN YOUR ORGANIZATION

### 3.3.1 REQUIREMENTS

The elicitation and articulation of requirements is a core PM-ISE capability that helps ensure the success of solutions adopted across the community. This capability is necessary because organizational culture and mission requirements vary between organizations that should be sharing information. This can create friction that prevents information transactions or reduces the efficiency of transactions (e.g., because data formatted or modeled for one mission type may need to be transformed before it's useful or legally permissible in another mission type). PM-ISE is in the position to facilitate the development of cross-organization technical and policy requirements that minimize organizational bias.



### 3.3.2 STANDARDS-BASED ACQUISITION

Responsible information sharing is dependent upon effective partnering between government and industry so that government's requirements for interoperable exchange standards are transparent to industry. Vendors need these requirements in advance to build them into commercial products prior to responding to an acquisition. Consistent language throughout this evolving process will help ISE partners work with vendors and other agencies to promote interoperable products and services that enable information sharing and safeguarding.

<sup>11</sup> Click on "apply standards" and then "what standards exist."

Award vehicles—including acquisitions and grants—for ISE products and services must include appropriate and clear standards language identified as requirements prior to making investment decisions. This will provide solutions conformant to the appropriate, available, and approved interoperability standards, enabling easier information sharing across agencies.

The I<sup>2</sup>F's Common Profile provides a tool that requirements and systems professionals can use to search for solutions to the business problem and to determine what technical solutions are immediately available and which consensus-based standards to incorporate into acquisitions and grants. Therefore program managers can use preapproved and specific language provided through the Common Profile to reuse in their requirements documents. This will significantly reduce time spent searching for interoperability standards, eliminate time spent writing standards language, and potentially reduce cost by reusing an interoperable IT solution.

### GLOBAL STANDARDS USED IN GRANTS

The Bureau of Justice Assistance (BJA) has a Global Standards Council (GSC) to ensure that technical products developed in the national justice community evolve in a cohesive manner so that consumers find a single set of products that are known to work well together and reinforce one another. To achieve interoperability and cost savings, the GSC initiated a structured approach to leveraging standards which can be located at the “[BJA](#)” website. In addition, BJA recently released a Pre-RFP Toolkit that was created to assist program managers on how to incorporate DOJ's [Global Standards Package \(GSP\)](#) in to justice acquisitions.<sup>12</sup> The GSP is a collection of normative, independently versioned standards that are assembled into a package of composable, interoperable solutions specifically supporting the exchange of justice information. The [GSC Grant Condition](#) requires that grantee comply with GSP components ([NIEM](#), [GRA](#), and [GFIPM](#)) “Compliance to the GSP requires conformance to all components of the GSP whenever applicable”<sup>13</sup>. By requiring this language, it ensures that vendors develop systems in a consistent manner across the Justice Information Sharing spectrum.

<sup>12</sup> [IJIS Institute Releases Justice Information Sharing Pre-Request for Proposals Toolkit](#)

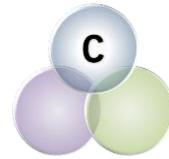
<sup>13</sup> [Global Standards Package Grant Condition](#)

## 4 COMMUNICATIONS AND PARTNERSHIPS

When Congress established the PM-ISE and mandated the creation of an information sharing environment, it was clear that the ISE would require partnerships across government to make the vision a reality. Each new ISE partner is strengthened by, and strengthens, the ISE as a whole by ensuring that those who protect our nation have the information they need. While the original congressional requirement was specific to terrorism information, the mission of ISE partners has broadened, making strategic partnerships and communications are imperative.

### 4.1 SETTING COMMUNICATION GOALS

Within the framework of the National Strategy, it's important to establish your organization's goals for your communications with the ISE as a whole and with the ISE partners with which you most often share information. This helps keep your activities focused and provides a shared understanding within your organization as to what you hope to accomplish.



#### 4.1.1 PRIORITIZING YOUR PARTNERS AND SEGMENTING YOUR COMMUNICATIONS

Because the ISE is so broad and covers large mission areas, ISE mission partners are extremely diverse. At the broadest level, your communications strategy needs to address all of these stakeholders. For example, the [FBI Information Sharing and Safeguarding Report 2012](#) communicates to both its federal and non-federal partners by highlighting significant activities of the Bureau, in a format intended to mirror strategic issues and initiatives across the entire US Government's diverse information sharing environment. When targeting narrower audiences, it is important to remember that stakeholder priorities will vary among the different types of organizations and individuals based on mission, community, and level of investment in ISE processes. For example, while all ISE mission partners will be interested in cutting red tape and hastening responsible information sharing, border states and towns may be particularly concerned about initiatives focused on exchanging terrorism screening information and securing the borders, while local municipalities are interested in finding better ways to improve information sharing with their state and federal partners. Communication elements to keep in mind:

- Understand your ISE stakeholders to effectively target your communications
- Identify your stakeholders' needs and requirements—be sure to shape your communications to acknowledge their priorities.
- Differentiate between internal and external audiences. While we typically think about developing effective communications with external ISE mission partners, effective internal

communication mechanisms can positively impact mission success. It's important that your team understands and supports your agency's participation in ISE initiatives.

- State your requests clearly. When communicating, be very clear about what your desired outcomes are and what you need and want other ISE stakeholders to do.

Once you have established your organization's goals for ISE communications and identified those stakeholders most important for your organization's success, you can create an ISE communications strategy that addresses these goals and stakeholders specifically.

[Contact PM-ISE's Stakeholder Engagement Team](#) to learn more.

## 4.1.2 MESSAGING AND COMMUNICATIONS VEHICLES

As a starting point, it is best to craft key messages, using [plain language](#). Key messages will serve as the foundation for your ISE communications. You should use these core messages repeatedly, and will just need to tweak them to address each audience's specific needs and concerns. Your core messages may address:

- Your organization's relationship to the ISE
- Your organization's needs vis-à-vis the ISE
- The overall importance of the ISE to your organization's mission
- ISE success stories from your organization and other relevant ISE partners

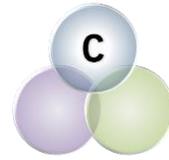
The action(s) your employees should take to further your organizational goals in the ISE

- Your organization's role in specific ISE areas, such as cyber security, standards, interoperability, etc.

Once your key messages have been established, you can use variations of them in any number of communications vehicles or channels, to include online communications and social media, press kits and releases, [conferences and events](#), and involvement in associations and industry.

Inbound communications techniques that involve a dialogue and feedback are the hallmark of today's communications strategies. Many of the communications techniques described earlier provide mechanisms for feedback loops. Setting up processes and methods for gathering feedback and engaging in a dialogue is not difficult, but they do require an ongoing commitment to monitor the various mechanisms, analyze the comments, and reply.

## 4.2 PARTNERING WITH KEY ISE ORGANIZATIONS



ISE partners represent a wide variety of mission categories, and each has a critical role in helping to build our collective capabilities. IN this section, we have provided a few examples of ISE partners who are creating the culture of responsible information sharing. As you will see, these actions include mission partners from many disparate ISE communities.

### 4.2.1 STATE AND LOCAL PARTNERSHIPS

Building efficient and effective information sharing environments at the state and local levels is helping to solve challenges related to shrinking budgets, dynamic threats, and exploding amounts of data. Each state has unique requirements, but states are seeing results by building ISEs based on best practices. The call to action for these efforts is the DOJ's Global Justice Sharing Initiative's (Global) "Strategic Solutions to Transform Our Nation's Justice and Public Safety Information Sharing." Released in November 2012, the paper challenges governors, sheriffs, chiefs of police, and other Global Advisory Committee (GAC)<sup>14</sup> members to develop single-sign-on and federated query capabilities, leverage secure cloud solutions, develop and engage in shared services and systems, ensure interoperability between law enforcement deconfliction systems, advance information sharing to support successful reentry of formerly incarcerated individuals, and to collaborate with federal partners to coordinate a consistent approach to federal funding, policy support, and universal adoption of common standards and technologies.

In line with the recommendations in the recently released report, Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities (GAO-13-471), DHS continues to emphasize the importance of and monitor the level of ongoing coordination and collaboration between a number of entities: fusion centers, FBI Field Intelligence Groups (FIGs), the High Intensity Drug Trafficking Areas (HIDTA) Program's Investigative Support Centers (ISC), the Regional Information Sharing Systems (RISS) Program's Centers, Joint Terrorism Task Forces (JTTF), and major city and county intelligence units to support implementation of the statewide fusion process.

Examples of cooperative partnerships at the state and local level include Fusion Center Partnerships, Fusion Liaison Officer Programs, P/CR/CL Protections, Field Analytic Support Task Force, and Building Communities of Trust. For a details and a more comprehensive list, go to Section 1 the [ISE Annual Report](#).

<sup>14</sup> <http://it.ojp.gov/default.aspx?area=globalJustice&page=1021>

## 4.2.2 PRIVATE SECTOR PARTNERSHIPS

Public-private partnerships, as defined by the National Council for Public-Private Partnership (NCP3P) are “a contractual agreement between a public agency (federal, state, or local) and a private sector entity.” The skills and assets of each sector (public and private) are shared through these agreements to deliver a service or facility for the use of the general public. DHS is a key ISE partner that leverages effective public-private partnerships to drive outcomes and support mission responsibilities.

A prime example of the need for public-private partnerships can be found in the critical infrastructure protection mission space, where over 85 percent of the nation’s infrastructure is owned and operated by the private sector. The structure of the existing critical infrastructure partnership is explained at length in the [National Infrastructure Protection Plan \(NIPP\)](#), which consists of government, private sector-specific and cross-sector councils that enable government and private sector partners to engage in joint discussions and participate in a broad spectrum of information sharing activities. The desired end-state of an effective partnership model is an environment in which public and private partners work in a networked manner to effectively and efficiently share timely and actionable information and allocate risk-reduction responsibilities.

As part of its responsibility to enhance critical infrastructure security and resilience under [Presidential Policy Directive 21 \(PPD-21\)](#), DHS along with other key federal and private sector partners, conducted an in-depth review of the current public-private partnership model in use across the Federal government. They found that “successful partnership models have a common set of attributes—they have a defined purpose; clearly articulated goals; participation from the appropriate membership; have buy-in from organizational leadership; clearly define governance; are built on a foundation of trust; include robust communication channels and mechanisms to share information; have measurable outcomes that move partners towards the articulated goals.”<sup>15</sup>

## 4.2.3 INTERNATIONAL PARTNERSHIPS

Canada and the U.S. are connected by critical infrastructure, from bridges and roads to energy infrastructure and cyberspace. The [Beyond the Border Action Plan](#) includes measures to enhance the resilience of our shared critical and cyber infrastructure and to enable our two countries to rapidly respond to and recover from disasters and emergencies on either side of the border.

Canada and the U.S. continued implementing the [Canada-U.S. Action Plan for Critical Infrastructure](#), including conducting a Regional Resilience Assessment Program project for the

---

<sup>15</sup> Evaluation of the Existing Public-Private Partnership Model. DHS Integrated Task Force. July 12, 2013. Pages 4-6.

Maine-New Brunswick region and a joint risk analysis, collaborative cross border analytical products and best practices to enhance critical infrastructure security and resilience.

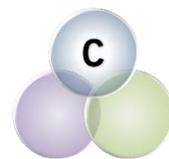
PM-ISE participates in annual North America Day (NAD) talks, a forum that brings together the Chief Information Officers of Canada, Mexico, and the United States. These talks have resulted in tangible projects that are becoming prototypes for international information sharing. For example, in 2011 the three countries signed a trilateral Memorandum of Understanding and established information-sharing pilot projects to exchange test data for public health alerts and stolen vehicle information. In 2012, the three countries agreed to collaborate on Open Government platform (OGPL) participation by Canada and Mexico that builds on the work of the U.S. and India; ideas for accelerating some U.S.-Canada Beyond the Border projects by extending them to include Mexico; and sharing best practices in the three countries' identity management and authentication programs.

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

Although not specific to international partners, building a culture of information sharing extends across borders. As such, the work that PM-ISE does with the International Division of the International Association of Chiefs of Police provides opportunities to further work on interoperability, especially as it relates to Suspicious Activity Reports (SAR) training, metrics, and policies. PM-ISE has also worked to construct and continuously update the [ISE Building Blocks](#) provides international partners with best practices and lessons learned from other mission partners in the ISE.

### 4.3 IMPLEMENTING AN ISE CULTURE IN YOUR ORGANIZATION

Anyone can achieve their responsible information sharing goals by using the tools and processes described in this Management Plan—governance and policy; performance management; interoperability standards and frameworks; communications strategies—however, to truly achieve an ISE in which all participants responsibly share the right information, with the right people, at the right time requires a management approach that institutionalizes a culture of information sharing. To achieve this change in culture, leaders and managers in the ISE must make responsible information sharing a priority for their respective organizations and educate and incentivize their workforces. Training, awards, and personnel performance and appraisal incentives are powerful tools.



### 4.3.1 TRAINING

Organizational cultures across the ISE vary widely, and information sharing is not always viewed as required behavior. To promote a shared awareness of the ISE and encourage such behavior, the PM-ISE issued the ISE Core Awareness Training Course to Federal departments and agencies and [ISE-G-104: ISE Policy Mandating Core Awareness Training](#) across ISE Mission Partners. The course is intended to give a common understanding of the ISE to all employees who support the counterterrorism mission. This training, coupled with continued efforts to include information sharing as a formal evaluation factor in personnel performance reports and agency incentive programs, is designed to help move the traditional “need to know” culture to one based on a “responsibility to provide.”

There are many examples of training resources that support the ISE. One is the US Department of Justice, Office of Justice Programs, Bureau of Justice Assistance's, Global Information Sharing Toolkit (GIST). This toolkit is a resource library of guides and training available to federal, state, local, tribal and territorial law enforcement and can be found at the DoJ Justice Information Sharing [GSIT](#) website.

### 4.3.2 AWARDS, PERFORMANCE AND APPRAISAL INCENTIVES

Many agencies offer awards for excellence in information sharing. The National Fusion Center Association offers a variety of awards for excellence, to include: Infrastructure Protection, Analysis, Outreach, outstanding performance by representatives and the federal and state and major urban area levels, Fusion Center of the Year and a Lifetime Achievement Award. DoD offers a Secure Information Sharing Award. Check with your agency to understand incentives to promote information sharing. In austere budget times, it is important for agencies to also be creative about the use of non-monetary awards to sustain and promote excellence in information sharing.

The Office of Personnel Management (OPM) and the PM-ISE have issued guidance to assist ISE agencies in the development of information sharing priority elements for inclusion in employee performance appraisals: [ISE-G-105: Guidance on Integrating Information Sharing Responsibilities into Employee Performance Assessment](#), ISE Guidance for the *Inclusion of Information Sharing Performance Evaluation Element in Employee Performance Appraisal Memorandum*, September 23, 2008; and OPM Guidance for *Inclusion of Information Sharing Performance Evaluation Element in Employee Performance Appraisal Memorandum*, September 24, 2008.

## 4.4 PILOTING

PM-ISE supports rapid-transition projects, developed in conjunction with interagency stakeholders and end-users that have the potential to improve



information sharing and safeguarding. These pilots are not research activities, but rather are well defined, limited projects with clear outputs and manageable milestones. ISE stakeholders are required to dedicate resources, which can but do not necessarily include funding. These projects are typically one to two year efforts designed to deliver a prototype capability that supports the ISE community and advances the goals of the National Strategy. The goal of ISE pilots is to deliver field-tested prototype capabilities to stakeholder organizations that have agreed to transition, operate, and maintain them.

For more information, contact PM-ISE's Management and Oversight Division at [DNI-PM-ISE-ExecSec@dni.gov](mailto:DNI-PM-ISE-ExecSec@dni.gov).

The following example illustrates the benefits of using the tools and processes described above to communicate with target ISE audiences.

### **PRIVATE SECTOR OUTREACH AND FUSION CENTERS**

The degree to which private sector outreach programs are implemented across the National Network of Fusion Centers (National Network) varies widely and is largely dependent upon the available resources and relative value each fusion center places on sharing information with the private sector. The PM-ISE supports its ISE partners in their efforts to develop a sustainable model for promoting greater engagement and sustained connectivity between private sector executives and the National Network.

The DHS State and Local Program Office, the DHS Office of Intelligence & Analysis, the DHS National Protection and Programs Directorate, and the National Fusion Center Association (NFCA), recognize the importance of building partnership models that integrate the protection and resiliency of private sector critical infrastructure into the National Network of Fusion Center's Critical Operating Capabilities. DHS has worked with its NFCA partners to develop a number of resources that support the integration of this mission capability, including the *Infrastructure Protection Field Resource Toolkit*.

Fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities. Recognizing the importance of this valuable partnership, a number of fusion centers across the national network are exploring ways to enhance their leverage of private sector capabilities and expertise and expand their reach within their area of responsibility (AOR). A number of fusion centers are integrating private sector analysts within the fusion center to enhance their analytic capabilities and provide a direct conduit to key stakeholders within their AORs; Fusion centers are exploring ways to utilize the National Council of Information Sharing and Analysis Centers (ISACs) to expand the depth and breadth of their information sharing with the private sector; and the NFCA has established a working group dedicated to collecting and promoting the sharing of tools and best practices for private sector outreach by fusion centers across the national network.

## 5 CALL TO ACTION

There are a number of ways your organization can partner with the office of the PM-ISE to support your organization and the Information Sharing Environment:

**Using the ISE Building Blocks** – This tool shares the best practices of ISE mission partners. You can access the ISE Building Blocks at <http://www.ise.gov/building-blocks> to learn more about ISE governance, budget and performance, acquisition, standards and interoperability, communications and partnerships.

**Contributing to PM-ISE Communication Initiatives** – PM-ISE’s Stakeholder Engagement Team welcomes collaboration. ISE partners are encouraged to guest write blogs for [ise.gov](http://ise.gov), team on social media initiatives, co-host events, and co-author positions papers.

**Participating in Information Sharing and Safeguarding Committees and Working Groups** – There are a number of working groups tackling a range of challenges, from standards to interoperability including membership from all levels of government and private sector. [Contact us](#) to find out more about opportunities to support these working groups.

**Contributing to the ISE Annual Report** – The primary method for communicating ISE-related activities to the Congress is the ISE Annual Report to the Congress. We encourage you to review this year’s Annual Report at [www.ise.gov/annual-report](http://www.ise.gov/annual-report) and [contact PM-ISE’s Stakeholder Engagement Team](#) with ideas for content. The Annual Report is unclassified, but includes a classified annex that discusses classified programs and initiatives.

**Making your Systems Interoperable** – The ISE Interoperability Framework (I<sup>2</sup>F) provides the information you need to ensure your systems can effectively interoperate with others.

**Sharing Detailees and Assignees** – The office of the PM-ISE often has openings for rotational assignments, which are reimbursable positions and Intelligence Community Joint Duty eligible. PM-ISE also is looking for federal government employees to fill non-reimbursable assignee positions. Both types of positions support the Executive Offices of the President and lead a significant number of interagency and government-wide initiatives.

# APPENDIX A: CAPABILITY AREAS AND MATURITY

This Management Plan provides common business processes and tools to enable stakeholder collaboration while implementing the National Strategy, and as such will be integrated into the future ISE performance scenarios. The table below shows the spectrum of maturity levels by capability area.

Table A-1. ISE Capability Areas and Maturity Spectrum

	MATURITY STAGE 1	MATURITY STAGE 2	MATURITY STAGE 3
<b>COMMUNITY</b>	Community <b>Awareness</b>	Community <b>Involvement</b>	Community <b>Integration</b>
<b>PROCESS</b>	Process <b>Exploration</b>	Process <b>Adoption</b>	Process <b>Harmonization and Compliance</b>
<b>TECHNOLOGY</b>	Technology & Standards <b>Awareness</b>	Technology & Standards <b>Exploration</b>	Technology & Standards <b>Integration</b>

Questions in the annual ISE Performance Assessment Questionnaires (PAQ) align to each maturity stage. We use industry and government best practices to guide the assessment efforts, including [GAO’s framework for assessing and improving Enterprise Architecture](#), and for [assessing and improving the process maturity of Information Technology Investment Management](#).

The following list is a sampling of notional performance assessment questions that can be used by ISE Stakeholders to self-assess the level of maturity of applying the tools in this Management Plan.

<b>ASSESSING THE MATURITY OF ISE MANAGEMENT CAPABILITIES</b>			
	<b>MATURITY STAGE 1</b>	<b>MATURITY STAGE 2</b>	<b>MATURITY STAGE 3</b>
<b>GOVERNANCE AND POLICY</b>			
<b>COMMUNITY</b>	Is your agency aware of the authorities and duties of the ISA IPC, Federal CIO Council, the Senior Information Sharing and Safeguarding Steering Committee, and other interagency bodies that serve your community and has it developed a plan to establish relationships between them and its governance body(ies)?	Is your agency involved in the ISE governance bodies that foster information sharing and safeguarding policies and processes promoted by the ISA IPC, Federal CIO Council, Senior Information Sharing and Safeguarding Steering Committee, and other bodies that serve your community?	Are your agency's information sharing and safeguarding policies, processes, and investments aligned and, where desirable, integrated with those of other ISE Stakeholders and does your agency benchmark its policies and business processes against other "best-in-class" ISE organizations?
<b>PROCESS</b>	Has your agency identified gaps in existing information sharing and safeguarding policy based upon a review and analysis of IRTPA Section 1016; Executive Orders 13388, 13587, 13636; NSISS Goals and Priority Objectives; GAO-13-283 High Risk Series; and any other statutory requirements, executive orders, or reports pertinent to your organization?	Has your agency created, or is your agency involved in one or more governance bodies with defined membership, guiding policies, operations, roles, responsibilities, and authorities for closing gaps in information sharing and safeguarding policy?	Does/do your agency's information sharing and safeguarding governance body(ies) implement, enforce, and ensure harmonization and compliance with policies through actions and budget processes; and by publishing policy guidance and tracking short- and long-term implications?
<b>BUDGET AND PERFORMANCE</b>			
<b>COMMUNITY</b>	Is your agency aware of the annual ISE Planning Cycle and has it developed a plan to participate in the development and, where required, respond to the requirements of the annual ISE Programmatic Guidance; ISE Implementation Guidance; ISE Performance Assessment, and ISE Annual Report to the Congress?	Is your agency involved in developing ISE performance measures that are used to assess strategic progress and inform action guidance and budgetary resource allocation to support the priority objectives of the NSISS and best practices of other ISE Stakeholders?	Are your agency's information sharing and safeguarding investments aligned and, where desirable, integrated with those of other ISE Stakeholders, and does your agency benchmark its investment approach against other "best-in-class" ISE organizations?
<b>PROCESS</b>	Are your agency and its employees aware of the ISE and are information sharing and collaboration criteria a component of performance appraisals?	Is your agency involved in leveraging cross agency guidance and policy (e.g., the Federal Resource Allocation Criteria Policy) in its budget and performance management processes to inform the allocation and development of personnel, as well as the delivery of other resources (i.e., training deliveries, exercises, etc.) to support interagency efforts?	Has your agency implemented an integrated performance management capability that is aligned with the ISE Performance Framework, using maturity-defined performance measures, to monitor the performance of responsible information sharing initiatives, and identifies the technologies, processes, and necessary integration with the wider ISE community required to mature those initiatives to the point where they achieve the goals of the NSISS?

<b>ASSESSING THE MATURITY OF ISE MANAGEMENT CAPABILITIES</b>			
	<b>MATURITY STAGE 1</b>	<b>MATURITY STAGE 2</b>	<b>MATURITY STAGE 3</b>
<b>INTEROPERABILITY AND STANDARDS</b>			
<b>COMMUNITY</b>	Is your agency aware of and does it engage with industry Standards Development Organizations to further voluntary consensus standards?	Does your agency’s pursuit of technical solutions involve the use of the I <sup>2</sup> F’s Common Profile Framework to search for solutions to determine what technical solutions are immediately available for its business problems and which consensus-based standards to incorporate into acquisitions and grants?	Are your agency’s corporate and subordinate Enterprise Architectures integrated with those of other ISE Stakeholders and does your agency benchmark its EA management processes against other “best-in-class” ISE organizations?
<b>PROCESS</b>	Does your agency have defined processes that allow coordination among operational elements to enable discovery and access to data by internal partners and systems?	Has your agency developed and adopted initial versions of corporate “as-is” and “to-be” Enterprise Architecture that describe the enterprise in terms of performance, business, data, services, technology, and security; and are architecture products being developed that comply with the I <sup>2</sup> F?	Do your agency’s segment and/or federated architectures exist and are they horizontally and vertically integrated within your organization, extend to align with external ISE partner architectures, and are subject to independent assessment?
<b>TECHNOLOGY</b>	Is there a general awareness and appreciation for interoperability and are technology solutions and standards for interoperability a consideration in your agency’s enterprise architecture development process?	Do your agency’s Enterprise Architecture planning and implementation activities examine, leverage and comply with the I <sup>2</sup> F, in particular the ISE Standards and Specifications Framework and the Common Profile Framework?	Does your agency’s EA management program integrate feedback from interagency information sharing programs and to drive its continuous technology improvement efforts?
<b>COMMUNICATIONS AND PARTNERSHIPS</b>			
<b>COMMUNITY</b>	Is your agency aware of information sharing and safeguarding cultural barriers and does your agency have proactive policies to address information sharing and safeguarding cultural barriers across various levels of government, to include federal, State, Local, Tribal or Territorial (SLTT), foreign governments, or the private sector, where appropriate?	Is your agency involved with writing guest blogs for <a href="http://ise.gov">ise.gov</a> , team on social media initiatives, co-host events, and co-author positions papers?	Are continuous improvement efforts around information sharing programs in your organization integrating the results of external assessments?

This page intentionally left blank.





## Program Manager, Information Sharing Environment

Washington, D.C. 20511

202.331.2490

[www.ise.gov](http://www.ise.gov)



@shareandprotect



[fb.me/informationsharingenvironment](https://fb.me/informationsharingenvironment)



<http://lnkd.in/zaCB97>



[youtube.com/shareandprotect](https://youtube.com/shareandprotect)



[ise.gov/blog](http://ise.gov/blog)



[ise.gov/email](mailto:ise.gov/email)

