STRATEGIC IMPLEMENTATION PLAN

FOR THE NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING

December 2013

Contents

INTRODUCTION

Today's dynamic operating environment challenges Federal, state, local, tribal, and private sector partners to continue improving information sharing and safeguarding processes and capabilities. While innovation has enhanced the ability to share and we have overcome many cultural barriers, increased sharing has created the potential for vulnerabilities requiring strengthened safeguarding practices.

> "Our national security depends on sharing the right information with the right people at the right time. We will therefore keep working to maintain an environment in which information is shared in a manner that is responsible, seamless, and secure."
>
> PRESIDENT BARACK OBAMA, DECEMBER 2012
> NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING

In December 2012 the President signed the National Strategy for Information Sharing and Safeguarding (*Strategy*) which is anchored on the 2010 National Security Strategy and builds upon the 2007 National Strategy for Information Sharing. The Strategy provides guidance for more effective integration and implementation of policies, processes, standards, and technologies to promote secure and responsible national security information sharing. This document provides a higher-level overview of a longer, more detailed implementation plan for the Strategy, and is intended to assist in briefing senior policy makers on plans, progress, and performance related to achieving the vision of the NSISS.

Under the collaborative leadership of the National Security Staff (NSS) and the Program Manager-Information Sharing Environment (PM-ISE), with departments and agencies participating through the Information Sharing and Access Interagency Policy Committee (ISA IPC), a government-wide effort is underway to plan and coordinate continued, agency-based implementation of the Strategy's 16 Priority Objectives. The ISA IPC, in coordination with the Senior Information Sharing and Safeguarding Steering Committee, Federal CIO Council, and other interagency oversight and governance bodies, will transparently monitor progress against milestones and achievement of outcomes described in this *Strategic Implementation Plan*.

Charles P. Bartoldus
Senior Director, Information Sharing and Safeguarding
National Security Staff

Kshemendra N. Paul
Program Manager
Information Sharing Environment

EXECUTING THE IMPLEMENTATION PLAN

In coordination with the National Security Staff, the ISE Management Plan, which incorporates the ISE's Annual Planning Cycle (Figure 1 below), provides the framework for managing the *Strategic Implementation Plan* and provides the ability to respond to changing priorities and individual department and agency resource allocations while integrating annual programmatic [1] and implementation guidance and assigning departments and agencies specific actions and milestones.

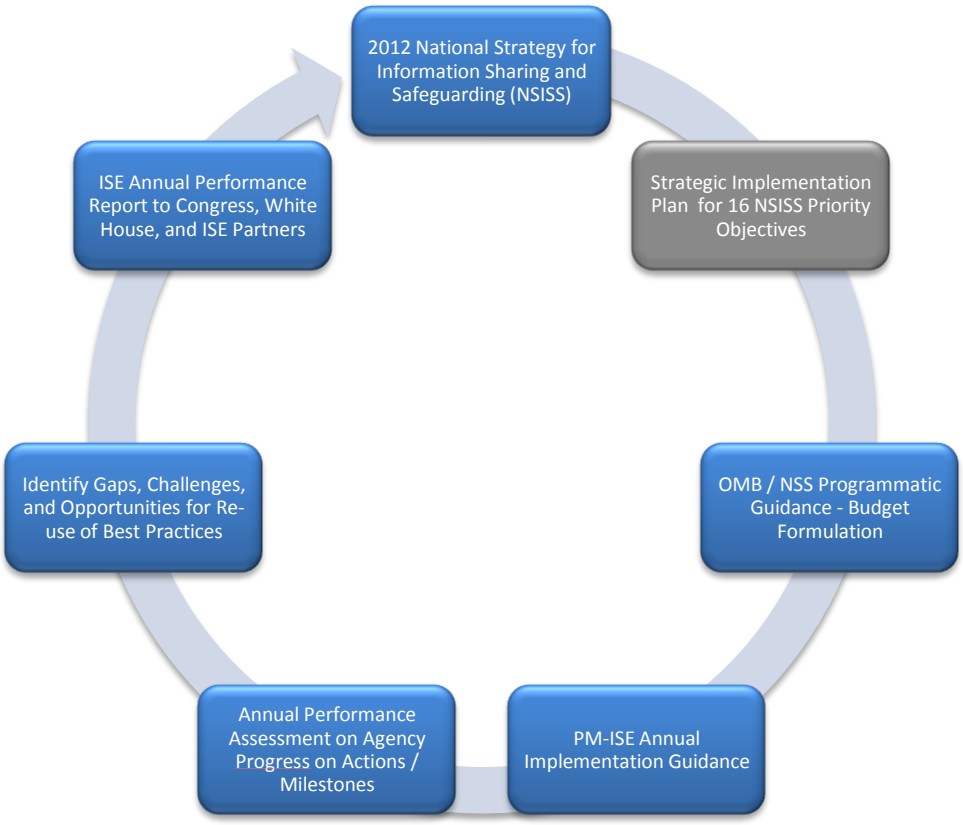


Figure 1. ISE Annual Planning Cycle

[1] NSS and OMB Programmatic Guidance is issued only when significant program changes are expected of Federal Government agencies.

This *Strategic Implementation Plan* establishes a construct for executing the *Strategy* by aligning each of the 16 Priority Objectives identified in the *Strategy* (see Appendix A) against the five strategic goals. The ISE Management Plan provides common business processes and tools to enable stakeholder collaboration while executing the *Strategy*.

GOAL 1

DRIVE COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY

Use governance models that enable mission achievement; adopt common processes to build trust, simplify the information sharing agreement development process, and support progress through performance management, training, and incentives.

GOAL 2

IMPROVE INFORMATION DISCOVERY AND ACCESS THROUGH COMMON STANDARDS

Improve discovery and access by developing clear policies for making information available to approved individuals through identity, authentication, and authorization controls, data tagging, enterprise-wide data correlation, common information sharing standards, and a rigorous process to certify and validate individual use.

GOAL 3

OPTIMIZE MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY

Optimize mission effectiveness through shared services, data and network interoperability, and increased efficiency in acquisition.

GOAL 4

STRENGTHEN INFORMATION SAFEGUARDING THROUGH STRUCTURAL REFORM, POLICY, AND TECHNICAL SOLUTIONS

Foster trust and safeguard our information through policy and coordinating bodies focusing on identifying, preventing, and mitigating insider threats and external intrusions, while departments and agencies work to enhance capabilities for data-level controls, automated monitoring, and cross-classification solutions.

GOAL 5

PROTECT PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES THROUGH CONSISTENCY AND COMPLIANCE

Maintain the public trust by increasing the consistency by which Federal departments and agencies apply privacy, civil rights, and civil liberties protections across the government, building corresponding safeguards into the development of information sharing operations, and promoting accountability and compliance mechanisms.

SAFEGUARDING AND THE PROTECTION OF INDIVIDUAL PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES UNDER THE RULE OF LAW

A fundamental precept of the *Strategic Implementation Plan* is that the Federal Government's actions must be consistent with the Constitution and in compliance with U.S. laws and regulations. Departments and agencies are responsible for identifying and complying with the law governing their activities and respective authorities. Compliance with the rule of law, particularly ensuring protection of First Amendment rights, and safeguarding our national security data are central to the *Strategy* and the execution of the *Strategic Implementation Plan*.

ROLES AND RESPONSIBILITIES

The *Strategic Implementation Plan* assigns Stewards for each Priority Objective listed in the *Strategy*. Stewards have primary responsibility for coordinating, integrating, and synchronizing activities to achieve the Priority Objectives and the overall goals of the *Strategy*.

EXPECTATIONS OF STEWARDS AND DEPARTMENTS AND AGENCIES

STEWARD

A governance entity (e.g., a department, agency, sub-committee, or working group) is responsible for leading partners[2] to take action and ensuring activities are effectively executed. The Steward is accountable for, among other things:

- Fostering communication among partners to ensure all parties understand how to complete the activity;
- Identifying, in collaboration with partners, the actions and resources needed to effectively execute the activity;
- Identifying and raising issues that impede progress; and
- Informing all departments and agencies on progress by the Steward and other Priority Objective partners, including impediments, modifications, or alterations to individual Priority Objective implementation plans.

[2] Partners are any supporting entity identified by the Steward as integral to the successful completion of desired outcomes; e.g., ISA IPC subcommittees, working groups, or any department or agency.

DEPARTMENTS AND AGENCIES

Collaborate with a Steward and other partners, to include state, local, tribal, territorial, and private sector partners, to accomplish an activity. Departments and agencies are accountable for:

- Accomplishing actions within their respective department or agency's area of responsibility in a manner that contributes to the effective execution of an activity;
- Providing status reports and assessments of progress on actions pertinent to the activity; and
- Identifying needs that impede progress on their department or agency's activities and prioritize the same needs within existing resources.

PRIORITY OBJECTIVE 1 GOVERNANCE

Align information sharing and safeguarding governance to foster better decisionmaking, performance, accountability, and implementation of the Strategy's goals.

STEWARD

ISA IPC Co Chairs

PROBLEM STATEMENT

Not all information sharing and safeguarding governance bodies of the U. S. Government have the processes and structures necessary to ensure effective and coordinated decision making within department and agency bodies and across interagency bodies.

DESIRED OUTCOME

Promotion of baseline best practices and common minimum requirements for department and agency information sharing and safeguarding governance, transparent and harmonized decision making, and coordinated efforts internally and interdepartmentally among relevant information sharing and safeguarding governance bodies.

APPROACH

The Governance Tiger Team, convened by the ISA IPC, will develop a roadmap and near-term goals for intra- and inter-agency information sharing and safeguarding governance. The Tiger Team will identify best practices and common requirements, coordinate an assessment of interagency governance structure effectiveness, and promote accountability using the ISE Annual Planning Cycle.

ALIGNMENT AND DEPENDENCIES

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Establish working group to develop a governance roadmap with near-term goals.	Tiger Team			
Identify best practices and common governance requirements.		Tiger Team		
Update relevant guidance and policy to reflect best practices.			All ISE Agencies	
Develop integrated Priority Objective timeline; synchronized with the ISE Annual Planning Cycle.				NSS and PM-ISE

PRIORITY OBJECTIVE 2 AGREEMENTS

Develop guidelines for information sharing and safeguarding agreements to address common requirements while allowing flexibility to meet mission needs.

STEWARD

Data Aggregation Working Group (DA WG) of the Information Integration Subcommittee (II SC), partnering with the Privacy and Information Technology Working Group (PIT WG) under the Privacy and Civil Liberties Subcommittee (PCL SC) of the ISA IPC

PROBLEM STATEMENT

Federal, state, local, tribal and international partners lack standardized guidelines to address common requirements for information sharing and safeguarding agreements.

DESIRED OUTCOME

Create and provide standard information sharing agreement baseline guidelines, processes, and examples to shorten the time required to adopt agreements and enable compliance with legal and policy requirements.

APPROACH

The DA WG and the PIT WG will develop guidelines for information sharing and safeguarding agreements to address common requirements, including privacy, civil rights, and civil liberties, while allowing flexibility to meet mission needs. Once developed, agreement guidelines will be tested for ISE community use.[3]

ALIGNMENT AND DEPENDENCIES

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Create a framework of recommendations for the streamlining of information sharing and access agreements.	DA WG and PIT WG			
Create a toolkit for agreement templates, including all privacy and mission equities.		DA WG and PIT WG		
Select priority pilots to test agreements and methodologies.		II SC	All ISE agencies	
Develop and implement a sustainment plan to include creation of agreement templates.		II SC	All ISE agencies	
Extend and maintain toolkits to demonstrate the capabilities of automation and multi-lateral sharing.			All ISE agencies	All ISE agencies

[3] Guidelines will be developed in accordance with information safeguarding and dissemination policies issued by the Controlled Unclassified Information (CUI) Executive Agent under Executive Order 13556.

PRIORITY OBJECTIVE 3 DATA TAGGING

Adopt metadata standards to facilitate federated discovery, access, correlation, and monitoring across Federal networks and security domains.

ALIGNMENT AND DEPENDENCIES

STEWARD

Information Integration Subcommittee (II SC) of the ISA IPC, partnering with the Federal Identity, Credential, and Access Management (FICAM) Subcommittee of the Federal Chief Information Officer (CIO) Council

PROBLEM STATEMENT

A lack of common metadata tagging standards across all security domains inhibits effective data search, correlation, and the simultaneous safeguarding of data and Personal Identifiable Information.

DESIRED OUTCOME

Develop common metadata standards for data tagging across Federal agencies and security domains to advance information sharing and safeguarding.

APPROACH

Common metadata standards for data tagging will be developed by Federal agencies to advance information sharing and safeguarding. Standards will be developed for a common lexicon that can be applied across the ISE, information from foreign sources, and processes around lifecycle management of data tagging protocols.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Document functional requirements for data tagging.	II SC			
Develop technical standards for data tagging and a technical specification aligned to functional requirements established by the II SC.			II SC and ISOO / NARA	
Implement and align data tagging standards to FICAM.			All ISE Agencies	All ISE Agencies

PRIORITY OBJECTIVE 4 FICAM

Extend and implement the Federal Identity, Credential, and Access Management (FICAM) Roadmap across all security domains.

ALIGNMENT AND DEPENDENCIES

STEWARD

Senior Information Sharing and Safeguarding Steering Committee (SISS SC), partnering with the Identity Federations Coordination Working Group (IFC WG) that dual reports to the ISA IPC and Federal CIO Council

PROBLEM STATEMENT

A government-wide capability does not exist to control access to sensitive information on computer networks, and to assure compliance with legal, regulatory and mission-area policies, while simultaneously allowing access to that same sensitive information by authorized persons.

DESIRED OUTCOME

Enable users[4] across all security domains to access information appropriate to their authorized mission purposes; reduce stored user-Personal Identifiable Information; and increase efficiencies for information custodians to validate users' "need to know" in order to better protect sensitive information.

APPROACH

Assess the current baseline and determine the desired end state for each security domain; develop an accompanying plan to reach that end state; and identify and implement shared services to support identity, credentialing, and access management implementation efforts.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Assess baseline and develop Implementation Plans for all security domains.		IFC WG and All ISE Agencies		
Develop and publish a candidate list of ICAM shared services for all security domains and a cost model for delivery of initial ICAM services.		ICAM SC and IFC WG		
Publish attribute and digital policy governance guidance and CONOPS.		ICAM SC and ACAG WG		
Develop internal plans and policies for implementing FICAM on all security domains.			All ISE Agencies	
Demonstrate compliance with the Implementation Plan via reporting specified by the IFC WG.			All ISE Agencies	All ISE Agencies

[4] Users include "Non-Person Entities" with a digital identity.

PRIORITY OBJECTIVE 5 SAFEGUARDING

Implement safeguarding capabilities to support information sharing.[5]

STEWARD

Senior Information Sharing and Safeguarding Steering Committee (SISS SC), partnering with the Federal CIO Council

PROBLEM STATEMENT

Cybersecurity presents one of the most serious national security, public safety, and economic challenges the nation faces. Challenges associated with technology, organizations, people, and performance require creative solutions to address emerging and increasingly sophisticated threats, and new vulnerabilities.

DESIRED OUTCOME

Establish and implement processes, procedures, and standards that improve information safeguarding and raise confidence among information sharing partners. Align departments' and agencies' oversight across all security domains; implement the improved governance and reporting processes and procedures by the end of 2015.

APPROACH

In 2013 and 2014, the SISS SC, the Federal CIO Council, and the ISA IPC develop safeguarding efforts across all Federal Government classification security domains. 2013 and 2014 have different priorities for classified and unclassified domains. The way forward will include a joint set of priorities for both classified and unclassified domains, which will be jointly established by the Federal CIO Council and the SISS SC.

ALIGNMENT AND DEPENDENCIES

[5] Priorities for safeguarding have evolved since the issuance of the NSISS. Planning described in the document aligns with current priorities defined by the SISS SC and Federal CIO Council. NSISS Priority Objective 5 reads: "*Implement removable media policies, processes and controls; establish programs, processes and techniques to deter, detect and disrupt insider threats; provide timely audit capabilities of assets, vulnerabilities, and threats; and share the management of risks, to enhance unclassified and classified information safeguarding efforts.*"

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Continue implementing capabilities specified on Classified (SC goals) and Unclassified networks (CAP goals).	All ISE agencies	All ISE agencies	All ISE agencies	
Create an action plan for consolidated information safeguarding reporting.		SISS SC		
CONTROLLED UNCLASSIFIED INFORMATION SAFEGUARDING[6]				
Convene a Joint FY15 Working Group (J15 WG) to determine the combined FY15 safeguarding priorities.	J15 WG			
Develop new progress tracking criteria for sharing and safeguarding of classified information and systems aligned with SISSSC priorities and goals.	PM-ISE, DoD, NSA, IC CIO, ONCIX, and FBI			
Develop a set of metrics for assessing the J15 implementation.	J15 WG			
Develop consolidated plan for safeguarding implementation and oversight.		SISS SC		
Annually baseline information security practice assessments.	OMB	OMB	OMB	OMB
CLASSIFIED INFORMATION SAFEGUARDING				
Conduct quarterly assessments on progress of classified information sharing and safeguarding initiatives.	SISS SC	SISS SC	SISS SC	SISS SC
Report progress on all EO 13587 information sharing and safeguarding activities.	SISS SC		SISS SC	SISS SC

[6] Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA) is included as a participant in all planning associated with safeguarding unclassified information across Executive Branch departments and agencies.

PRIORITY OBJECTIVE 6 INTEROPERABILITY

Define and adopt baseline capabilities and common requirements to enable data, service, and network interoperability.

STEWARD

Information Integration Subcommittee (II SC) of the ISA IPC

PROBLEM STATEMENT

The limited or lack of interoperable information exchanges between systems inhibits or precludes timely information sharing.

DESIRED OUTCOME

Establish the common requirements and security controls for data interoperability to enable effective data exchanges between heterogeneous systems.

APPROACH

Identify needed capabilities, requirements, and restraints associated with data, service, and network interoperability in the context of an ISE Interoperability Framework (I2F) which incorporates enterprise reference architectures.

ALIGNMENT AND DEPENDENCIES

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Develop the ISE Interoperability Framework (I2F).	II SC			
Implement the I2F.				All ISE agencies
Define capabilities and services.		II SC		
Develop sustainment plan to include development and maintenance of a repository of capabilities and services.			II SC	
Select priority pilots or use-cases for reuse (i.e., reference architectures or profiles) using an ISE capability roadmap.			II SC	

PRIORITY OBJECTIVE 7 TRAINING

Provide information sharing, safeguarding, and handling training to appropriate stakeholders using a common curriculum tailored to promote consistent yet flexible and trusted processes.

STEWARD

Training Working Group (PO 7 WG) of the ISA IPC

PROBLEM STATEMENT

The absence of up-to-date shared, core-training requirements restricts workforce proficiency and effective implementation of the ISE.

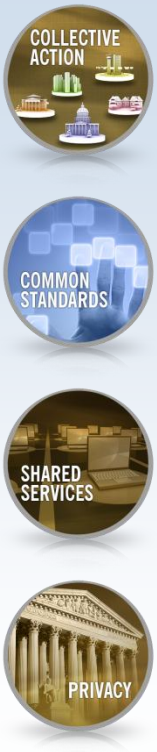
DESIRED OUTCOME

A standardized, up-to-date training curriculum which recognizes the unique needs of departments and agencies while developing a more uniformly trained and proficient ISE workforce to better enable information sharing and safeguarding.

APPROACH

Validate the 2013 training survey which identifies requirements for additional core training. Once validated, translate training requirements into learning objectives, and initiate actions for training acquisition and delivery. Once new training requirements are operational, develop and deliver training, and assess user satisfaction with training and impact to ISE culture to determine suitable change requirements.

ALIGNMENT AND DEPENDENCIES



	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Identify and validate training requirements and translate them into learning objectives.	PO 7 WG			
Develop and acquire core awareness training.		PO 7 WG		
Launch and deliver core awareness training.		All ISE agencies		
Measure effectiveness of core awareness training – survey emerging needs.		All ISE agencies	All ISE agencies	All ISE agencies

PRIORITY OBJECTIVE 8 DISCOVERY AND ACCESS

Define and implement common processes and standards to support automated policy-based discovery and access decisions.

STEWARD

Information Integration Subcommittee (II SC) of the ISA IPC

PROBLEM STATEMENT

The lack of an automated, policy-based decision approval process restricts information discovery, access, and delivery of high-value datasets. Current disparate, overly bureaucratic policies across the Federal Government result in a time-consuming approval process for information discovery and access.

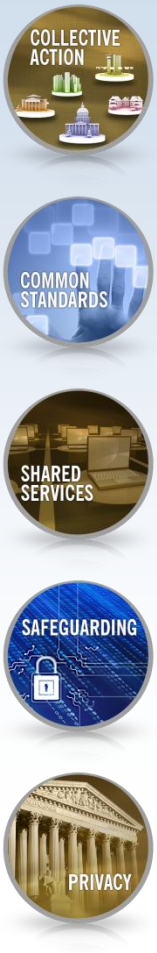
DESIRED OUTCOME

Better defined, common processes and policy standards supporting automated, policy-based decisions will provide a government-wide management framework to enable more efficient and cost-effective use of information sharing and safeguarding best practices.

APPROACH

Complete requirements development process for a broad-based approach to automated discovery and access and subsequently establish a state-of-the-art digital policy to support discovery and access, which leverages current Federal Government and commercial capabilities.

ALIGNMENT AND DEPENDENCIES



	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Identify automated policy-based discovery and access decision set of requirements.	ODNI NSA	II SC		
Contribute access and discovery elements to the FICAM segment architecture.			II SC	
Complete an authoritative access control and discovery model.				All ISE Agencies
Complete user acceptance testing for automated access and discovery systems.				All ISE Agencies

PRIORITY OBJECTIVE 9 PRIVATE SECTOR

Establish information sharing processes and sector-specific protocols with private sector partners to improve information quality and timeliness and secure the nation's infrastructure.

ALIGNMENT AND DEPENDENCIES

STEWARD

Department of Homeland Security and the Federal Bureau of Investigation, partnering with the Cyber IPC, Transborder Security, Resilience and Cybersecurity Directorates, National Security Staff (NSS) directed by PPD 21 and EO 13636.

PROBLEM STATEMENT

ISE agencies and critical infrastructure owners and operators must put in place standard processes and procedures that guarantee the mutual and responsible sharing of all information[7] necessary for identifying and mitigating risks to the Nation's critical infrastructure, including cybersecurity threats.

DESIRED OUTCOME

A Nation in which physical and cyber critical infrastructure remains secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response to and recovery from attacks hastened.

APPROACH

Work supporting this Priority Objective will be anchored to and leveraged by ongoing efforts associated with the 2013 National Infrastructure Protection Plan (*National Plan*), directed by Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* and Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*, and will incorporate the complementary body of work developed by the joint critical infrastructure public-private information sharing initiative concluded in October 2013 by DHS, Office of the Director of National Intelligence (ODNI) and PM-ISE, and the FBI's private sector outreach programs, including the Domestic Security Alliance Council, InfraGard, and other Headquarters and field-based programs.

[7] Processes and procedures put in place related to Controlled Unclassified Information (CUI) will be developed with the concurrence of the CUI Executive Agent and consistent with the CUI Program established under Executive Order 13556.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
With the National Fusion Center Association, establish and develop objectives for a working group on private sector engagement.	PM ISE			
Develop standard procedures for making relevant fusion center products accessible to critical infrastructure owners and operators via HSIN-CS and socialize best practices with ISE agencies.		DHS, FBI		
Develop decision options and doctrine that establishes the private sector as a partner and recipient of threat information.		ODNI		
Identify and develop plans that incorporate a unified approach for tools that provide near real-time situational awareness of critical infrastructure vulnerabilities and interdependencies across the IC.			ODNI, DHS, FBI	
Identify and document public-private partnership best practices for sector-specific agencies.			ODNI, DHS, FBI	
Identify FBI products that could be useful to critical infrastructure owners and operators; develop and implement a dissemination plan.			FBI	
Identify and address gaps in training and analytic products related to emerging threats (e.g., insider threat, supply chain, and counterintelligence).			ODNI, DHS, FBI	
Prepare a response to the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC) Tribal Working Group White paper on Critical Infrastructure Key Resources (CIKR) in Indian Country with accountable actions to address the findings.			DHS, FBI, DOI, DOJ	
Complete actions as directed by the 2013 National Infrastructure Protection Plan, PPD-21 and EO 13636.	Ongoing, All Agencies as directed			

PRIORITY OBJECTIVE 10 REFERENCE ARCHITECTURE

Develop reference architecture to support a consistent approach to data discovery and correlation across disparate datasets.

ALIGNMENT AND DEPENDENCIES

STEWARD

Data Aggregation Working Group (DA WG) of the II SC, ISA IPC

PROBLEM STATEMENT

National security missions and operations are currently hindered due to a sub-optimized information sharing environment caused by non-standard means to discover, aggregate, and correlate data from disparate datasets.

DESIRED OUTCOME

Develop, implement, and sustain a data aggregation and standards framework that allows government and industry partners to efficiently discover, aggregate, and correlate data from disparate datasets and, if necessary, in a timeframe that allows users to execute critical time-sensitive operations.

APPROACH

The DA WG will identify required government-wide stakeholder capabilities to drive a single coordinated requirements document to inform development of an enterprise-wide architecture for the information sharing environment and associated reference architectures that together provide the strategic approach and technical roadmap to shape information systems and datasets to enable information access and discovery by authorized users, and to allow sharing of best practices.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Identify stakeholder needs and distill them into a single common architecture and requirements document.	II SC			
Submit Request for Information with industry white papers.	ISA IPC			
Develop a data aggregation reference architecture using I2F templates.		II SC		
Based on system maturity and other factors, implement tools and needed changes to business rules/processes to realize the capability envisioned.			All ISE agencies	All ISE agencies

PRIORITY OBJECTIVE 11 SHARED SERVICES

Implement the recommendations and activities of the Federal IT Shared Services Strategy among appropriate stakeholders to facilitate adoption of shared services.

ALIGNMENT AND DEPENDENCIES

STEWARD

Federal CIO Council supported by the ISA IPC and the SISS SC

PROBLEM STATEMENT

ISE agencies lack awareness of the Commodity IT, Support, and Mission Services platforms currently in use and available to them in order to build considerations for shared services into their strategic investment and planning processes.

DESIRED OUTCOME

Create a "shared-first" culture in the ISE that enables agencies to integrate existing capabilities that best align with their needs, missions, and goals. This will enable better delivery of targeted services to end-users, helping to eliminate inefficient spending and duplicative service offerings and systems.

APPROACH

The Federal IT Shared Services Strategy provides the foundation for the work by the Federal CIO Council's Shared Services Sub Committee (SS SC). The Classified Shared Services Working Group (CSS WG), reporting to the Federal CIO Council and the SISS SC, allows the SS SC to govern and set priorities for Federal-wide services across security classifications. Priority Objective 4, FICAM, is one such priority that will assist and inform in future shared service implementations.

The Sensitive but Unclassified Working Group (SBU WG) of the ISA IPC is a forum to discuss and resolve implementation issues identified through the shared services activities of other NSISS Priority Objectives. Stewards for NSISS Priority Objectives will also make use of the governance structure and processes described in the Federal Shared Services Implementation Guide.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Revisit and implement organizational constructs (roles and responsibilities, charters, memberships) for FICAM, SBU WG, and CSS WG.	Fed CIO Council, ISA IPC			
Identify and prioritize shared services to be governed by the CSS WG.		Fed CIO Council, SISS SC		
Determine service provisioning mechanism to include identifying budget, appropriation and procurement issues for resolution.			SS SC	
Implement pilot service offerings.			SS SC	
Federal IOC and FOC will implement prioritized shared services.				All ISE agencies

PRIORITY OBJECTIVE 12 STANDARDS-BASED ACQUISITION

Refine standards certification and conformance processes enabling standards-based acquisitions among departments and agencies, standards bodies, and vendors to promote interoperable products and services.

ALIGNMENT AND DEPENDENCIES

STEWARD

II SC partnering with General Services Administration

PROBLEM STATEMENT

The absence or inconsistent use of common technical standards in acquisition packages increases costs, limits interoperability, and complicates system operations, maintenance, and long-term sustainment.

DESIRED OUTCOME

Interoperable products and services which are realized, in part, through an approved baseline of technical standards available to all departments and agencies, adopted in enterprise architectures, and included in future acquisition packages.

APPROACH

Efforts will focus on policy review, government-to-industry communications, and inconsistent use of standards in acquisitions. By leveraging sequential use cases, the approach will provide iterative improvements to these areas and develop and refine a user's guide in the form of a desktop handbook. Additionally, the government will engage industry and professional societies through industry days to keep all parties abreast of its progress and its strategic direction. Furthermore, the government will emphasize standards-based acquisitions to promote interoperable products and services as part of its procurement request for information activities.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Review standards use policies and formulate update recommendations.		II SC		
Approve recommendations.		ISA IPC		
Plan for, execute, and garner best practices from use cases.			II SC	
Develop and implement government-to-industry engagement strategy.			II SC	
Develop and refine standards handbook.			II SC	

PRIORITY OBJECTIVE 13 FOREIGN PARTNER SHARING

Promote adherence to existing interagency processes to coordinate information sharing initiatives with foreign partners, as well as adopt and apply necessary guidelines, consistent with statutory authorities and Presidential policy, to ensure consistency when sharing and safeguarding information.

ALIGNMENT AND DEPENDENCIES

STEWARD

Foreign Partner Sharing Working Group (FPS WG), reporting to the ISA IPC

PROBLEM STATEMENT

The government lacks a coordinated approach to information sharing with its foreign partners and, as a result, information sharing efforts with foreign partners are currently sub-optimized.

DESIRED OUTCOME

Agencies have access to a best-practices toolkit, so that they can better inform their foreign partner sharing strategies and in turn minimize or eliminate overlapping or duplicative efforts, better utilize resources, and maximize information safeguarding.

APPROACH

Survey stakeholders' best practices with current agreements. FPS WG will subsequently develop, publish, and maintain foreign partner information sharing agreement toolkit containing a repository of best practices and agreement templates.[8]

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Collect and catalog existing agreement templates and/or model agreements for interagency use.	DOS			
Establish a method and centralized resource whereby agencies can find selected arrangements and agreements, templates approved for existing exchanges, and a list of best practices.		DOS		
Design a toolkit that includes a checklist of recommended procedures for interagency coordination.			FPS WG	

[8] Any such requirements related to Controlled Unclassified Information (CUI) will be developed with the concurrence of the CUI Executive Agent and consistent with the CUI Program established under Executive Order 13556.

PRIORITY OBJECTIVE 14a RFI PROCESS

Create a common process across all levels of government for Requests for Information (RFIs)[9] to enable timely receipt and dissemination of information and appropriate response.

ALIGNMENT AND DEPENDENCIES

STEWARD

Requests for Information Working Group (RFI WG) of the ISA IPC

PROBLEM STATEMENT

The lack of common terminology and transparent information across all levels of government creates redundancy within action agencies, causes delays when RFI requestors have to search for the appropriate action agency, and makes it difficult for stakeholders to request, track, and manage RFIs.

DESIRED OUTCOME

Common guidance for RFIs will enable Federal Intelligence Community and Non-Title 50 (NT-50s) agencies as well as state, local, tribal, and territorial partners that request or process information related to national security and homeland security threats and anticipated or ongoing homeland security events.

APPROACH

Establish well-defined, common RFI guidance across all levels of government; define what constitutes a valid RFI for use among and between levels of government; identify levels of information classification and clearance and need-to-know of requesting individual(s); identify relevant RFI stakeholder groups across all levels of government that fit within implementation plan scope; and determine and make transparent appropriate action agencies for different national security and homeland security threats and incidents.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Identify, validate, and update RFI definitions, problem statement, scope, stakeholders, and desired outcome.	RFI WG			
Perform current analysis of the state of RFI terminology and information flows to develop a year-one work plan.		RFI WG		
Derive best-practices and recommendations for business processes.			ISA IPC	
Assign action agencies to perform analysis of RFI information elements and develop a standardized set of RFI elements.			ISA IPC	All ISE Agencies
Progress RFI interoperability across ISE through guidance and policy.				All ISE Agencies

[9] Priority Objective 14a refers to requests for intelligence or national security related information and does not include market research related requests for information.

PRIORITY OBJECTIVE 14b AWN PROCESS

Create a common process across all levels of government for Alerts, Warnings, and Notifications (AWN) to enable timely receipt and dissemination of information and appropriate response.

ALIGNMENT AND DEPENDENCIES

STEWARD

AWN Working Group (AWN WG) of the ISA IPC

PROBLEM STATEMENT

Federal, state, local, tribal, territorial, and private sector stakeholders, as well as fusion centers, coordinate, produce, analyze, disseminate, and follow-up on AWNs through non-standard processes, thereby inhibiting the flow of information to enable incident preparedness and mitigation.

DESIRED OUTCOME

Common guidance for generating, disseminating, and receiving AWNs will enable Federal, state, local, tribal, territorial, and private sector organizations and fusion centers to generate or receive information related to national security and homeland security threats or incidents.

APPROACH

Establish common AWN guidance across all ISE stakeholders, including defining a valid AWN, identifying relevant AWN stakeholder groups, identifying best practices, determining clearance level of requestor(s), validating appropriate need-to-know, and determining appropriate action agencies for specific national security and homeland security threats and incidents.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Identify, validate, and update AWN definitions, problem statement, scope, stakeholders, and desired outcome.	AWN WG			
Perform current-state analysis of AWN terminology and information flows to develop a year-1 work plan.		AWN WG		
Derive best-practices and recommendations for business processes.			ISA IPC	
Assign action agencies to perform analysis of AWN information elements and develop a standardized set of AWN elements.			ISA IPC	All ISE Agencies
Progress AWN interoperability across ISE through guidance and policy.				All ISE Agencies

PRIORITY OBJECTIVE 15 NATIONWIDE SAR INITIATIVE

Complete the implementation of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) programs in the National Network of Fusion Centers and Federal entities while expanding training and outreach beyond law enforcement to the rest of the public safety community.

ALIGNMENT AND DEPENDENCIES

STEWARD

Responsible Information Sharing Sub Committee (RIS SC) of the ISA IPC

PROBLEM STATEMENT

The NSI program is transitioning from its development, deployment, and initial operating capability to long-term operations and sustainment, with program management responsibility transitioning to FBI and DHS. The NSI system and its capabilities must remain operational during this transition with no degradations. Additionally, NSI training and outreach must continue uninterrupted.

DESIRED OUTCOME

Seamless transition with no system interruptions or capability degradations while maintaining required levels of operator proficiency and readiness. Ensure the program matures to provide technology enhancements that meet user requirements, while ensuring all training and outreach services are continually updated to reflect the most current threat environment.

APPROACH

Leverage lessons learned and best practices to ensure successful transition from NSI Program Management Office. In order to achieve these outcomes, Federal partners must continue to work with local jurisdictions to help improve quality and the quantity of shared information and the analysis performed at all levels of government.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY16-18
Ensure all partners have received the Unified Message and that all Building Communities of Trust (BCOT) and similar outreach efforts are coordinated at the Federal level and include approved NSI messaging.	RIS SC			
Coordinate the sharing and deconfliction of Roll Call Releases, FBIs *Significant Activity Baseline Report* (SABR), and FBI Tripwires.	DHS and FBI			
Ensure all new or updated SAR analytic products and associated indicator and warning products are distributed to fusion centers as soon as they are published or released.	DHS and FBI			
Determine the optimal IT platform to host online training programs, update training accordingly, and incorporate content on behaviors associated with current threats or incidents.		DHS		
Ensure all SAR analysts have access to relevant classified and unclassified databases.		RIS SC		
Identify best practices and user requirements, in coordination with state and local users, to enhance existing analytic tools.		DHS and FBI		
Refine and enhance SAR analysis tools.			DHS and FBI	
Implement process to audit fusion center processes for compliance with privacy, civil rights, and civil liberties protection practices.			DHS and FBI	
Secure long-term programmatic funding and update all training/outreach materials in accordance with new policy and/or technical advancements.				DHS and FBI

PRIORITY OBJECTIVE 16 FUSION CENTERS

Achieve the four Critical Operational Capabilities, four Enabling Capabilities, and other prioritized objectives across the National Network of Fusion Centers to enable effective and lawful execution of their role as a focal point within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information.

ALIGNMENT AND DEPENDENCIES

STEWARD

Responsible Information Sharing Sub Committee (RIS SC) of the ISA IPC

PROBLEM STATEMENT

Timely and well integrated operational information sharing between the Federal Government and the National Network of Fusion Centers (National Network) has not been fully embraced by all Federal partners, which limits state and local information environments' ability to receive, analyze, and disseminate threat-related information.

DESIRED OUTCOME

A fully integrated and sustainable National Network, in which each fusion center has achieved the four Critical Operational Capabilities (COC), four Enabling Capabilities (EC), and other prioritized objectives essential to executing the fusion of information.

APPROACH

The RIS SC will ensure that the fusion center assessment process evaluates the maturity of the National Network against the COCs and ECs. Based on assessment findings, the RIS SC will coordinate continued implementation of the Federal Resource Allocation Criteria (RAC) policy to optimize Federal support to fusion centers and coordinate provisioning of training, products, and other resources to increase analytic competencies and collaboration. The RIS SC will continue to strategize mechanisms to sustain capabilities and maintain operational relevance to include monitoring and tracking Federal partners' provisioning of services and resources to fusion centers and compliance with the Federal RAC policy.

	Q1-Q2 FY14	Q3-Q4 FY14	FY15	FY 16-18
Issue implementation guidance for the Federal RAC policy.		RIS SC		
Implement a process to track the expenditure of Homeland Security Grant Program (HSGP) funds allocated to support fusion centers.		DHS		
Enhance collaboration between fusion centers and field-based information sharing entities to increase analytic competencies and collaboration.			RIS SC	
Ensure all appropriate Federal analytic products are posted, shared, and cataloged within HSIN Intelligence.			RIS SC	
Mature the fusion center assessment process including a performance management framework.			RIS SC	
Develop a long-term approach to support sustainment of the National Network, including monitoring and projecting necessary costs and resource requirements.				RIS SC

CONCLUSION

National security stakeholders across the government can now act in concert to carry out the implementation plans for the 16 Priority Objectives to realize the goals in the Strategy. Through the execution of this Implementation Plan, departments and agencies will advance the Strategy's goals by enabling the policy-compliant sharing and safeguarding of information. Implementation will enable authorized users to discover and retrieve critical information, thereby driving decisions to protect our country and its people. Success depends upon the collective ability to manage risk and achieve the proper balance between sharing and safeguarding, to build on past accomplishments, and to continue progress implementing the Information Sharing Environment. As we work together, hold ourselves accountable, and take ownership to advance the Strategy's goals, we will achieve success.

APPENDIX A – PRIORITY OBJECTIVES ALIGNED WITH NSISS GOALS

NSISS PRIORITY OBJECTIVES	GOAL #1 	GOAL #2 	GOAL #3 	GOAL #4 	GOAL #5 
1 Governance	✓	✓	✓	✓	✓
2 Agreements			✓	✓	✓
3 Data Tagging		✓	✓	✓	✓
4 Federal Identify, Credential, and Access Management (FICAM)		✓		✓	
5 Safeguarding	✓			✓	
6 Interoperability		✓	✓		
7 Training	✓	✓	✓		✓
8 Discover and Access	✓	✓	✓	✓	✓
9 Private Sector	✓		✓		
10 Reference Architecture		✓	✓		
11 Shared Services			✓		
12 Standards-Based Acquisition		✓	✓		
13 Foreign Partner Sharing	✓				✓
14 Requests-For-Information and Alerts-Warnings-Notifications (RFI and AWN)	✓				
15 Nationwide Suspicious-Activity-Reporting Initiative (NSI)	✓				
16 Fusion Centers	✓		✓		

APPENDIX B – ACRONYMS

ACAG	Access Control & Attribute Governance
AWN	Alerts, Warnings, and Notifications
BCOT	Building Communities of Trust
CAP	Cross Agency Priority
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
COC	Critical Operational Capabilities
CONOPS	Concept of Operations
CSS WG	Classified Shared Services Working Group
DA WG	Data Aggregation Working Group
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
EC	Enabling Capabilities
EO	Executive Order
FBI	Federal Bureau of Investigation
FC SC	Fusion Center Subcommittee
FICAM	Federal Identity, Credential, and Access Management
FOC	Final Operating Capability
FPS WG	Foreign Partner Sharing Working Group
FY	Fiscal Year
HSIN-CS	Homeland Security Information Network – Critical Sectors
I2F	ISE Interoperability Framework
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
IFC	Identity Federations Coordination
II SC	Information Integration Subcommittee

IOC	Initial Operating Capability or Initial Operational Capability
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISE	Information Sharing Environment
ISOO	Information Security Oversight Office
J15	Joint FY 2015
NARA	National Archives and Records Administration
NSA	National Security Agency
NSI	Nationwide Suspicious Activity Reporting Initiative
NSISS	National Strategy for Information Sharing and Safeguarding
NSS	National Security Staff
NT-50	Non-Title 50
ODNI	Office of the Director for National Intelligence
OMB	Office of Management and Budget
ONCIX	Office of the National Counterintelligence Executive
PCL SC	Privacy and Civil Liberties Subcommittee
PIT WG	Privacy and Information Technology Working Group
PM-ISE	Program Manager-Information Sharing Environment
PO	Priority Objective
PPD	Presidential Policy Directive
RFI	Requests for Information
RIS SC	Responsible Information Sharing Sub Committee
SBU	Sensitive but Unclassified
SC	Subcommittee
SISS SC	Senior Information Sharing and Safeguarding Steering Committee
SLTTG CC	State, Local, Tribal and Territorial Government Coordinating Council
SAR	Suspicious Activity Report(ing)
SS SC	Shared Services Sub Committee
WG	Working Group