INFORMATION SHARING ENVIRONMENT IMPLEMENTATION PLAN

Prepared by the
Program Manager, Information Sharing Environment

This page intentionally blank.

TABLE OF CONTENTS

This page intentionally blank.

LIST OF FIGURES

LIST OF TABLES

This page intentionally blank.

FOREWORD

While it is often said—with good reason, but some exaggeration—that the first casualty in battle is the battle plan, there is no doubt that the plan is essential to get the forces ready for battle. This is what battle plans are designed to do: prepare for the effort, not control its every step. With this in mind the Program Manager for the Information Sharing Environment (PM-ISE) submits this Implementation Plan as the preparation for making a fully functional and useful Information Sharing Environment a reality for the struggle against terrorism. As such, it joins similar efforts in other areas to prepare for this struggle, such as the National Implementation Plan and the National Infrastructure Protection Plan.

The PM-ISE staff and the members of the Information Sharing Council (ISC) who worked so hard to write and edit this plan believe this plan will set us on the right path and help us through the initial phases of the effort. But we are all realistic enough to know we will need to be flexible over the coming three years as we carry out our work. This recognition is reflected in the limited (three-year) period covered by the plan, and in the specificity for the first year and more general planning for the final years.

No one can doubt that the pace of technology and the many basic changes and reforms we are proposing will force adjustments as we move forward. But move forward we must, and will. The plan represents the views of the 17 member agencies of the Federal government participating in the ISC, and is the product of many long hours of deliberation, discussion, and debate. It also reflects the perspectives of our colleagues in State, local, and tribal governments and the private sector to whom we went for additional advice and assistance.

We believe this plan can take us forward to meet the goals set by the Congress in the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), and by the President in his memorandum, *Guidelines and Requirements in Support of the Information Sharing Environment*, of December 2005.

This process does not end with the publishing of the plan. The plan prepares for the start of the real work—the implementation of the ISE. Those of us who worked to produce it are committed to developing all aspects of ISE outlined in these pages. We think it will lead to the single strategic goal that we all share and that President Bush articulated when he signed the IRTPA, “The many reforms in this act have a single goal: to ensure that the people in government responsible for defending America have the best possible information to make the best possible decisions.”

Thomas E. McNamara
Program Manager, Information Sharing Environment

This page intentionally blank.

EXECUTIVE SUMMARY

Strengthening our nation's ability to share terrorism information constitutes a cornerstone of our national strategy to protect the American people and our institutions and to defeat terrorists and their support networks at home and abroad. Recognizing the need to go beyond individual solutions to create an environment—the aggregation of legal, policy, cultural, organizational, and technological conditions—for improving information sharing, Congress passed and the President signed the landmark *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA). The Act requires the President to establish an Information Sharing Environment (ISE), "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." It also requires designation of a Program Manager for the Information Sharing Environment (PM-ISE). The PM-ISE, in consultation with the interagency Information Sharing Council (ISC), is charged with planning and overseeing the ISE's implementation and management. Among other duties, the PM-ISE is responsible for assisting the President in submitting to Congress an ISE Implementation Plan (ISE IP) that addresses eleven requirements set forth in Section 1016(e) of IRTPA.

This plan responds to those eleven requirements and describes the actions the Federal government intends—in coordination with its State, local, and tribal (SLT), private sector, and foreign partners—to carry out over the next three years.

Vision for the Future ISE

Today's ISE consists of multiple sharing environments designed to serve five communities: intelligence, law enforcement, defense, homeland security, and foreign affairs. Historically, each community developed its own policies, rules, standards, architectures, and systems to channel information to meet mission requirements. Prior to 9/11, the need for coordinated and trusted interagency partnerships was not universally recognized and thus gaps and seams existed in the sharing of information across all levels of government.

The highest priority in creating the ISE must be on facilitating, coordinating, and expediting access to protected terrorism information. This future ISE requires a vision based on national policies, priorities, and partnerships, and a clear understanding of the operating framework, roles, and responsibilities for effective information sharing.

We envision a future ISE that represents a *trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America.* Realizing this vision will impact the numerous organizations participating in the ISE and will require achievement of the following six goals.

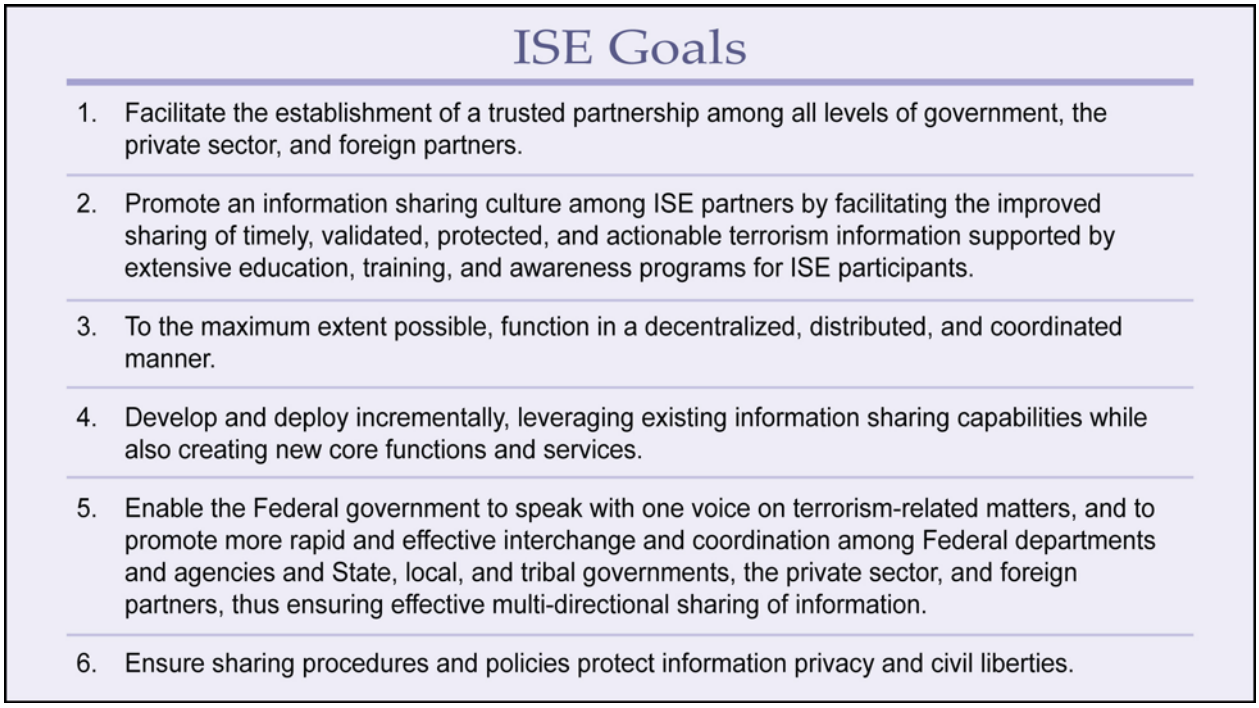


Figure ES-1. ISE Goals

The operating environment that flows from this vision and these goals will draw upon existing systems and capabilities, observe and respect the roles and responsibilities of participating Federal entities, and mandate a coordinated, collaborative approach to appropriate terrorism information sharing among all ISE participants. This environment will create a powerful national capability to share, search, and analyze terrorism information across jurisdictional boundaries and provide a distributed, secure, and trusted environment for transforming data into actionable information. The resulting environment will also recognize and leverage the vital roles played by State and major urban area information fusion centers, which represent crucial investments toward improving the nation's counterterrorism capacity.

The ISE must incorporate all types of data, at all levels of security. This includes structured and unstructured data and finished intelligence products. Ultimately, the goal is to integrate terrorism information from multiple sources and to provide maximum and appropriate access to such information. In this way, the ISE will meet the needs of all ISE participants by creating a more unified, coordinated environment. It will take advantage of and connect existing information sharing capabilities and organizational structures at all levels of government.

Underpinning this vision is a risk management approach to ensure that the ISE will protect this information at least to the same degree of security and assurance it receives today. Achieving this objective requires the development of policies, business rules, and technologies that balance the imperative to share with national security needs and the requirement to protect privacy and civil liberties. Further, the ISE will leverage ongoing Federal security initiatives; introduce auditing, authentication, and enforcement mechanisms to ensure a high degree of trust; and stimulate the development of technologies to improve security and access.

One point implicit in this vision and articulation of ISE goals warrants particular emphasis: The ISE has been designed and will be driven and implemented by the needs and missions of all participants, and technology will be used to enhance ISE operations. The ISE will not result in the construction of one government-wide computer system containing all terrorism information. To the contrary, and as stated, technology will play the role of facilitating, improving, and expanding information sharing in response to the counterterrorism needs of ISE participants.

Progress to Date

Transforming today's ISE is a complex undertaking. Today's ISE—and the ISE of the future—exist in a dynamic, unpredictable threat environment. As threats change, technologies evolve, and information needs shift, the ISE must prove resilient and adaptable. The Federal government and its partners have not been standing still over the past five years. Far from it—we have substantially improved our nation's ability to share terrorism information, as demonstrated by the following six major accomplishments.

First, the Federal government has constructed a strong legal and policy foundation upon which to improve information sharing. For his part, the President issued Executive Orders (E.O.) 13311, 13356, and 13388 (which replaced E.O. 13356), each of which successively strengthened the sharing of terrorism information across the Federal government. In addition, on December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies on the *Guidelines and Requirements in Support of the Information Sharing Environment*, which specified tasks, deadlines, and assignments necessary to further the ISE's development. The President also adopted the majority of information sharing recommendations put forth by the *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (the WMD Commission). Meanwhile, Congress enacted two laws in addition to IRTPA that provided the Federal government with greater authority for sharing information: *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001* and the *Homeland Security Act of 2002.*

Second, the establishment and maturation of the National Counterterrorism Center (NCTC) provides the Federal government an essential institution to develop an ISE fully capable of facilitating the flow, analysis, and integration of terrorism information.

Third, this legal and institutional foundation is complemented by measurable Federal progress in coordinating actions in the field. At the direction of the President, the NCTC produced the *National Implementation Plan (NIP)* for the War on Terror to further delineate Federal Department and Agency tasks to implement National Security Presidential Directive (NSPD)-46/Homeland Security Presidential Directive (HSPD)-15. At the same time, the Departments of Justice (DOJ), Homeland Security (DHS), Defense (DoD), and State (DOS) and the Director for National Intelligence (DNI) have enhanced their field operations and technical capabilities and strengthened their working relationships with SLT, the private sector, and foreign partners.

Fourth, States and localities have created and invested in fusion centers and charged those centers with collecting, analyzing, and sharing terrorism information. The collaboration between fusion centers and with the Federal government marks a tremendous increase in the nation's overall analytic capacity that can be used to counter terrorism.

Fifth, the PM-ISE, in consultation with the ISC and Federal departments and agencies, has advanced a number of important initiatives to remove impediments to, and create new capabilities for, sharing terrorism information. These include establishing an Initial Operating Capability (IOC) for Electronic Directory Services (EDS); fostering a culture of information sharing through training and incentives; and compiling a working inventory of existing resources (policies, procedures, programs, systems, architectures, and standards) for terrorism information sharing.

Sixth, the PM-ISE and the ISC have assisted in the compliance of, or complied with, all of the Presidential Information Sharing Guidelines and Requirements. The status of the recommendations being submitted to the President, in accordance with these Information Sharing Guidelines and Requirements, is summarized in the table below.

Table ES-1. Status of Recommendations Submitted to the President in Accordance with the Presidential Information Sharing Guidelines and Requirements

Guideline or Requirement	Title	Recommendation Status
Requirement 1	Leveraging Ongoing Information Sharing Efforts in the Development of the ISE	*Substantial Progress* Task 1(a): Completed Task 1(b): Completed Task 1(c): Due Dec. 2006
Guideline 1	Define Common Standards for How Information is Acquired, Accessed, Shared, and Used Within the ISE	*Substantially Completed*
Guideline 2	Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector	*Completed*
Guideline 3	Standardize Procedures for Sensitive But Unclassified Information	*In Progress*
Guideline 4	Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners	*Completed*
Guideline 5	Protect the Information Privacy Rights and Other Legal Rights of Americans	*Completed*
Requirement 2	Promoting a Culture of Information Sharing	*In Progress*

ISE Implementation

A dual imperative exists: to improve the sharing of terrorism information by taking immediate steps to improve ISE functionality and to simultaneously lay the foundation for ISE transformation and implementation. Consequently, this plan adopts a two-phased approach: **Phase 1** (those actions to be completed by June 2007) and **Phase 2** (actions to be completed in the period between June 2007 and June 2009). Specific implementation actions are contained throughout the ISE IP and are grouped into seven priority areas to include: ISE Operational Capabilities, Architecture and Standards, Sharing with Partners Outside the Federal government, Promoting a Culture of Information Sharing, Protecting Information Privacy and Civil Liberties in the ISE, Terrorism Information Handling, and ISE Enabling Activities. At the end of this three-year period, a strong and effective ISE should be functional in all of the areas outlined in this ISE IP. These areas are described in further detail below.

ISE Operational Capabilities

Enhancing the operational capabilities available to support ISE participants' business processes and functions is a major priority in both phases of implementation. The areas of emphasis include, but are not limited to: improving the access to and sharing of terrorism-related alerts and notifications; enhancing the ability of recipients of terrorism information to better search information databases; and improving collaboration across

all level of government. The objective is to add value to current and future processes in three dimensions:

1. Offering a suite of sharing and collaboration tools, subscription and notification services, and other common services;
2. Discovering and identifying data and services resident in other venues that should be added to the ISE; and
3. Providing the policies, processes, and technical means for introducing new capabilities into the ISE.

In Phase 1, activities will focus on identifying existing or emerging technologies or programs that may be appropriate for ISE adoption. Therefore, Phase 1 will identify standards and best practices, from both business process and technology perspectives, that can be leveraged in the ISE. Pilot programs, such as the Sensitive but Unclassified (SBU) Mobility Pilot for wireless access, will be closely monitored to identify policy, process, and technical lessons learned that could advance the plan for implementing the ISE sooner and better. Phase 2 will primarily concentrate on planning for, adopting and integrating these existing and emerging technologies. It will also include an incremental technology and capability review, comparing existing technologies and tools against the emerging needs of ISE users.

Architecture and Standards

Creating a fully functional ISE involves constructing, integrating, and maintaining information resource infrastructures across Federal and SLT entities with counterterrorism missions and establishing the mechanism for sharing, as appropriate, with our private sector and foreign partners. These information resources include personnel, equipment, funds, and information technology (IT). The current Federal approach to managing information resources involves use of strategic management tools—such as enterprise architectures—to help organizations understand the interrelationships of their missions and IT processes. Planning, integration, and implementation activities affecting information resources, both internal and external to agencies, are also effectively achieved through well-defined, conforming processes using common standards.

The PM-ISE, in consultation with the ISC, is developing an ISE Enterprise Architecture (ISEEA) Framework and Federal Enterprise Architecture-ISE Profile, along with the *Common Terrorism Information Sharing Standards (CTISS).* These initiatives help establish an overarching architecture and standards program from which to build a nationwide, integrated ISE. Once implemented, they will facilitate the sharing of analytic products and other information by all ISE participants. In both cases, these efforts represent starting points. During Phase 1, the PM-ISE will continue to generate versions of the ISEEA and CTISS, publishing products designed to define processes and standards. During Phase 2, the PM-ISE will continue to utilize existing processes with

Federal department and agency senior leadership, the Office of Management and Budget (OMB), the Office of the DNI (ODNI), DoD, the National Communications System, and the Committee on National Security Systems to ensure Fiscal Year (FY) 2009 enterprise architecture reviews and information resource investment budget requests incorporate ISEEA and CTISS requirements. Moreover, the PM-ISE will work with DHS, DOJ, and other Federal agencies to help State and major urban area fusion centers implement the ISEEA Framework and CTISS for eventual migration to SLT government infrastructures.

Sharing with Partners Outside the Federal Government

Realizing the full potential of the ISE requires sharing across all its participating organizations. Significant progress has been made in improving sharing with partners outside the Federal government. Specifically, the Attorney General and the Secretary of Homeland Security, in consultation with the PM-ISE, the ISC, and Federal departments and agencies, have established a Presidentially-approved framework (pursuant to Presidential Guideline 2) through which terrorism information can be shared in a distributed, decentralized, and coordinated manner between and among participating Federal, SLT, and private sector entities. Several steps were taken to improve integration of non-Federal participants into the ISE. The ISC has established a SLT Subcommittee and a Private Sector Subcommittee that serve as forums to address implementation issues related to SLT governments and the private sector respectively. Similarly, the interagency Foreign Government Information Sharing Working Group, led by the Department of State (DOS), prepared recommendations for the President to facilitate terrorism information sharing with foreign partners and allies, pursuant to Guideline 4.

Phase 1 will center on activities to stimulate the development of the SLT fusion center network, complete initial efforts to implement elements of the Guideline 2 framework across SLT governments and the private sector, and take the steps called for in the Guideline 4 recommendations to improve sharing with foreign partners. The second phase will fully implement the Guideline 2 framework, including further development of the fusion center network, and take further steps to protect U.S. information given to foreign partners and to protect foreign information provided to the United States while allowing for maximum dissemination.

Promoting a Culture of Information Sharing

As Congress recognized in IRTPA, there exists a need to develop a culture that promotes information sharing across the ISE. Accordingly, the PM-ISE and ISC are developing initiatives, including training and performance measurements that will stimulate the development of this culture and that will build trust among ISE participants. For example, Federal departments and agencies responsible for handling terrorism information designated an accountable senior official to provide direct, agency-wide oversight authority for planning, developing, and implementing all aspects of the ISE.

Further, an ISE training program will include a core training curriculum, common to all Federal departments and agencies, combined with department- and agency-specific training. Another element will be a process to review agency rules, regulations, or directives to identify and revise any such guidance that unnecessarily impedes terrorism information sharing.

During Phase 1, a core training module will be developed that will serve as the common educational baseline for the ISE. Additionally, a structure that offers incentives for adopting the ISE culture will be developed, reviewed, and measured. During the second phase, department- and agency-specific training and training guidelines for SLT governments will be developed. Phase 2 will also concentrate on ensuring that personnel responsible for handling terrorism information complete approved training programs, new employees complete information sharing training, and departments and agencies recommend modifications to internal policies needed to accommodate the ISE training, incentive, and accountability requirements.

Protecting Information Privacy and Civil Liberties in the ISE

In accordance with Presidential Guideline 5, the Attorney General and the DNI, in coordination with the PM-ISE and the heads of Federal departments and agencies, developed Privacy Guidelines, approved by the President, for Federal departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE. Specifically, these guidelines call for Federal departments and agencies to comply with current laws, regulations, and policies related to protected information and to adopt any internal policies required to ensure that their access to and use of protected information is consistent with the authorized purpose of the ISE and the need for privacy and other legal protections.

During Phase 1 of ISE implementation, each Federal department and agency will ensure at least one ISE Privacy Official has been designated. To ensure cross-agency coordination, the PM-ISE will also establish and designate a chair for the ISE Privacy Guidelines Committee. During Phases 1 and 2, the Committee will provide assessments of the ISE privacy and civil liberties protections as part of the annual ISE performance report.

Terrorism Information Handling

The ISE will rely on standardized, consistent policies and procedures for handling classified and unclassified terrorism information. The simplification of personnel clearance processes and the adoption of community-wide certification and accreditation policies and standards address the modification of security practices related to classified, national security information. At the same time, the standardization of SBU designations and markings is essential to ensure that the future ISE promotes and enhances the effective and efficient acquisition, access, retention, production, use, management, and sharing of unclassified information while also ensuring its appropriate

and consistent safeguarding. A Coordinating Committee has been created to complete the recommendation for standardizing SBU procedures, in accordance with Presidential Guideline 3.

For classified information, Phase 2 efforts will, on an ongoing basis, monitor and assess progress of ISC members in meeting the security clearance processing requirements of Section 3001 of IRTPA; support Information Security Oversight Office (ISOO) efforts to facilitate compliance with E.O. 12958, as amended, and its implementing directives; and support and leverage ODNI-led efforts to overhaul existing criteria and processes for certifying and accrediting Intelligence Community IT systems.

For unclassified information, in Phase 1, the Guideline 3 Coordinating Committee will submit recommendations for SBU standardization through the White House policy process to the Assistant to the President for Homeland Security and Counterterrorism (APHS-CT) and the Assistant to the President for National Security Affairs (APNSA).

ISE Enabling Activities

ISE performance management and planning, programming, and budgeting are necessary to enable the ISE. Performance management across the ISE requires a collaborative effort between the PM-ISE, ISC, and the ISE participants. ISE performance management will include ISE-wide goals and measures, while also integrating the performance goals, measures, and targets specific to individual departments and agencies. Dedication of specific funds and resources is also required to transform the current ISE into one that better facilitates protected access to terrorism information across ISE participants. Specific funding estimates, strategies, and proposals will need to be assessed, prioritized, cross-walked, and carefully integrated to achieve an overarching budget plan that can accomplish the two-phased implementation approach proposed in this plan.

During Phase 1, Federal departments and agencies will take several actions to develop and implement information sharing and terrorism-related goals, measures, and outcomes. The PM-ISE will also support OMB, which will provide Federal departments and agencies with budget guidance, and will begin planning for subsequent budget cycles.

Managing ISE Implementation

This plan contains nearly 100 short- and long-term actions to improve the sharing of terrorism information. To manage the ISE, the PM-ISE needs to monitor implementation progress, make mid-course adjustments, and elevate important issues to senior levels when they cannot be resolved. To ensure this plan is executed and coordinated properly, the PM-ISE will take several actions, to include:

1. Work with the ISC to obtain advice and recommendations and to gain Federal department and agency concurrence through its members;
2. Establish ISC Subcommittees and Working Groups to analyze complex issues and propose solutions;
3. Prioritize implementation actions to respond dynamically to changing conditions and ISE performance;
4. Conduct ISE Performance Reviews to set goals and measures to assess capabilities for sharing terrorism information;
5. Conduct operational exercises to test and evaluate information sharing capabilities;
6. Sponsor evaluation environments to identify new requirements, performance elements, capabilities, and standards; and
7. Compile an Annual Performance Report per the requirements of IRTPA to advise Congress on ISE performance.

Recommendations

Beyond these actions, the PM-ISE makes four major recommendations in this plan:

Recommendation 1: IRTPA defines the ISE as "an approach that facilitates the sharing of terrorism information . . ." IRTPA requires the PM-ISE, in consultation with the ISC, to recommend whether, and under what conditions, to expand the ISE to include other intelligence information. Pursuant to this Implementation Plan, and consistent with Guidelines 2 and 3 of the Presidential Information Sharing Guidelines, the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA Section 1016(a)(4), as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the *Homeland Security Act of 2002* (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland. Such additional information includes intelligence information.

The PM-ISE recommends deferring a decision to further expand the ISE to include additional intelligence information until policies, business practices, and systems are sufficiently mature to evaluate the impact of including such additional information, and revisiting the topic in the first annual ISE Performance Report (see Recommendation 3 below).

Recommendation 2: Continue the PM-ISE for three years. IRTPA requires that the PM-ISE, in consultation with the ISC, recommend a future management structure for the ISE, including whether the position of the PM should continue to remain in existence. Given that this plan contains actions through June 2009, the PM-ISE recommends continuation of the PM-ISE and ISC for the three years

covered by this plan to ensure its full implementation and to provide a fully operational ISE. This decision to continue the PM-ISE should be reviewed annually over the three-year period.

Recommendation 3: ISE Performance Report. The PM-ISE recommends that the President request the first ISE Performance Report, required by the IRTPA, be submitted to Congress at the end of June 2007, at the one-year mark for the plan and in time to inform the development of department and agency budgets. Subsequent reports would then be submitted at the end of June of each year thereafter.

Recommendation 4: Delegation of Authority. The need to grant the PM-ISE government-wide authority to issue procedures, guidelines, functional standards, and instructions for the management, development, and operation of the ISE, and options for doing so, should be considered. Such issuances would need to be consistent with the policies and directives issued by the President, the DNI, the Director of OMB, and other heads of departments and agencies having the authority to issue ISE policies and directives. Such issuance authority would not change or abrogate the authorities of the heads of such Federal departments and agencies, and all issuances would be coordinated through the ISE governance process described in Section 4.2 of this Implementation Plan. The delegation could be made consistent with the Presidential memorandum of June 2, 2005, and be through the DNI to the PM-ISE.

This page intentionally blank.

PART I

What We Want the ISE To Be

This page intentionally blank.

Chapter 1 – Introduction

1.1 Purpose and Scope

Improving information sharing constitutes a cornerstone of our national strategy to protect the American people and our institutions and to defeat terrorists and their support networks at home and abroad. The *National Commission on Terrorist Attacks Upon the United States* (the 9/11 Commission) identified a breakdown in information sharing as a key factor contributing to the failure to prevent the September 11, 2001 attacks on the United States. In the past five years, the Congress and Executive Branch have taken numerous steps to improve sharing of terrorism information among Federal departments and agencies, with State, local, and tribal (SLT) governments and, where appropriate, private sector and foreign partners. Despite this progress, the challenge enunciated by the 9/11 Commission remains: "The biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information."

In December 2004, Congress passed and the President signed the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA).[1] Section 1016 of IRTPA requires the President to establish an Information Sharing Environment (ISE) "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[2] Moreover, IRTPA defines the ISE to mean "an approach that facilitates the sharing of terrorism information."[3]

IRTPA also requires the designation of a Program Manager for the Information Sharing Environment (PM-ISE) "responsible for information sharing across the Federal Government" to oversee the implementation of and manage the ISE.[4;5] Working in consultation with the Information Sharing Council (ISC),[6] an interagency advisory body for Federal departments and agencies with counterterrorism missions, the PM-ISE's responsibilities include:

---

[1] *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law No. 108-458 (December 17, 2004).
[2] Ibid. Section 1016(b)(1)(A) of IRTPA.
[3] Ibid. Section 1016(a)(2) of IRTPA.
[4] Ibid. Section 1016(f) of IRTPA.
[5] Note with respect to the PM-ISE, the President's June 2, 2005 Memorandum on *Strengthening Information Sharing, Access, and Integration- Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment* states that "the DNI shall promptly designate the PM, and all personnel, funds, and other resources assigned to the PM, as part of the Office of the Director of National Intelligence (ODNI) pursuant to section 103(c)(9) of the National Security Act of 1947 and shall administer the PM and related resources as part of the ODNI throughout the initial 2-year term of the PM's office."
[6] IRTPA, Section 1016(g). See Section 4.2.3 and Appendix 6 for a more detailed description of the roles, responsibilities, and membership of the Information Sharing Council.

1. Planning for and overseeing the implementation of, and managing, the ISE;
2. Assisting in the development of policies, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the ISE; and
3. Assisting, monitoring, and assessing the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance, and regularly report findings to Congress.[7]

Among other duties, the PM-ISE is responsible for assisting the President in submitting an Implementation Plan for the ISE to Congress that addresses eleven specific requirements in Section 1016(e). In January 2006, the PM-ISE produced an Interim Implementation Plan (IIP) that partially responded to the eleven 1016(e) requirements. A number of IIP actions—many of which also responded directly to the President's December 16, 2005, Memorandum that set forth *Guidelines and Requirements in Support of the Information Sharing Environment*—have already been completed, and the others will be accomplished by December 2006. [8;9]

Building on work already completed, this ISE Implementation Plan (ISE IP) responds to all eleven IRTPA 1016(e) requirements, and represents a comprehensive plan for improving the ISE in the coming three-year period. [10] Figure 1.1-1 portrays the top level organizational structure of the ISE Implementation.

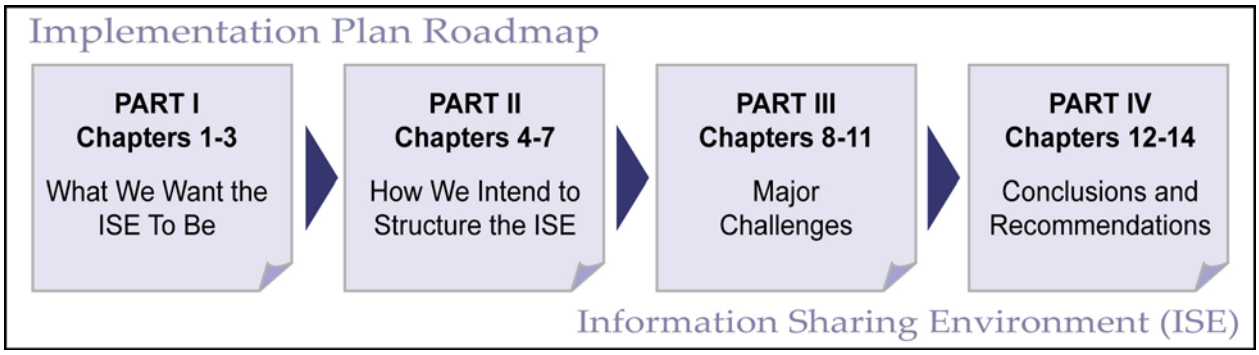


Figure 1.1-1. ISE Implementation Plan Roadmap

[7] Ibid. Section 1016(f)(2)(A) of IRTPA.

[8] Throughout the remainder of this plan, this memorandum and its contents will be referred to as "Information Sharing Guidelines and Requirements."

[9] See Appendix 3. Note: this Presidential memorandum contains two requirements and five guidelines: Requirement 1—*Leveraging Ongoing Information Sharing Efforts in the Development of the ISE; Information Sharing Guidelines;* and Requirement 2—*Promoting a Culture of Information Sharing*. The five guidelines include: Guideline 1—*Define Common Standards for How Information is Acquired, Accessed, Shared, and Used Within the ISE;* Guideline 2—*Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector;* Guideline 3—*Standardize Procedures for Sensitive But Unclassified Information;* Guideline 4—*Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners;* and Guideline 5—*Protect the Information Privacy Rights and Other Legal Rights of Americans.*

[10] See Appendix 1 for a complete list of the eleven IRTPA Section 1016(e) requirements.

1. **Part I (Chapters 1-3)** provides the foundation for the ISE IP, describing the ISE vision, goals, and operational framework to institutionalize and improve the sharing of terrorism information among ISE participants;
2. **Part II (Chapters 4-7)** outlines a two-phased implementation approach for the actions contained in the plan and describes the structural details for how the ISE will support the needs of ISE participants;
3. **Part III (Chapters 8-11)** highlights the major information sharing challenges facing ISE participants and articulates strategies for addressing them over the next three years; and
4. **Part IV (Chapters 12-14)** describes how the PM-ISE will use the ISE IP to manage the ISE by setting and adjusting priorities and regularly assessing implementation progress. This part also presents the PM-ISE recommendations.

Appendices to this plan provide more detailed background and reference material, including a detailed glossary and list of acronyms.

1.2 Definitions

IRTPA definitions of *terrorism information* and the *Information Sharing Environment* create the boundary conditions for the plan. These definitions describe the types of information to be accessed, shared, and disseminated and by what means. This Section also includes a definition of *ISE participants* drawn from language contained in IRTPA and multiple Presidential directives. In addition to framing the vision, strategy, and individual implementation actions in this plan, these definitions inform the PM-ISE's statutory requirement to recommend whether, and under what conditions, the ISE should be expanded to include other intelligence information.

1.2.1 Terrorism Information

IRTPA defines "terrorism information" as:

> All information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—
>
> (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
>
> (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
>
> (C) communications of or by such groups or individuals; or

(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.[11]

1.2.2 Information Sharing Environment

IRTPA calls for the creation of an "information sharing environment." Specifically, the enactment requires the President to: create an environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties; designate the organizational and management structures that will be used to operate and manage the ISE; and determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.[12] IRTPA further requires that the ISE provide and facilitate "the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector" and to the greatest extent practicable consist of "a decentralized, distributed, and coordinated environment" that:

1. Connects existing systems where appropriate, provides no single points of failure, and allows users to share information among agencies, levels of government, and, as appropriate, the private sector;
2. Ensures direct and continuous online electronic access to information;
3. Facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations, and operations;
4. Builds upon existing systems capabilities currently in use across the Government;
5. Employs an information access management approach that controls access to data, rather than just systems and networks, without sacrificing security;
6. Facilitates the sharing of information at and across all levels of security;
7. Provides directory services, or the functional equivalent, for locating people, organizations, and information;
8. Incorporates protections for individuals' privacy and civil liberties; and
9. Incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.[13]

1.3 Background

In the past five years, the Executive Branch has taken significant steps toward advancing our nation's ability to share terrorism information. Through Executive Orders (E.O.) 13311 and 13356, the President provided the foundation for improving

[11] Ibid. Section 1016(a)(4) of IRTPA.
[12] Ibid. Section 1016(b)(1) of IRTPA.
[13] Ibid. Section 1016(b)(2) of IRTPA.

information sharing. On October 25, 2005, the President added to this foundation by issuing E.O. 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans,* which states that the head of each Executive agency that possesses or acquires terrorism information "shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency" unless otherwise directed by the President, consistent with statutory responsibilities of the agencies providing and receiving such information, Attorney General guidelines, and other applicable law. In addition, the President has adopted the majority of information sharing recommendations put forth by the *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (the WMD Commission).

For its part, Congress enacted three laws providing the Federal government with greater authority and additional tools for sharing information: The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT) Act*, the *Homeland Security Act of 2002*, and IRTPA.

These legislative and policy advances were furthered by the President's establishment of the National Counterterrorism Center (NCTC)[14] and the Terrorist Screening Center, which have both illustrated the potential that can be realized by integrating existing information sharing capabilities. The Department of Justice (DOJ), Department of Homeland Security (DHS), and Department of Defense (DoD) have also enhanced their field operations and technical capabilities, strengthening their working relationships with other ISE participants. These combined activities form a strong foundation to further improve the sharing of terrorism information.

More recently, two additional Presidential actions have enhanced this foundation, identifying a set of expectations with which Federal departments and agencies must comply, and synchronizing and aligning ongoing information sharing efforts to improve response to overall U.S. counterterrorism strategies and objectives. First, consistent with IRTPA, Section 1016(d), the President issued the Information Sharing Guidelines and Requirements, which identified specific tasks, deadlines, and assignments necessary to further the ISE development. Second, at the direction of the President, the NCTC produced the *National Implementation Plan* (NIP) for the War on Terror to further delineate Federal department and agency tasks to implement National Security Presidential Directive (NSPD)-46 and Homeland Security Presidential Directive (HSPD) -15.

For their part, many States and localities emphatically moved to create and invest in fusion centers in the post-9/11 environment. These fusion centers now play a prominent role in collecting, analyzing, and sharing terrorism information. Individually, these centers represent vital assets for collecting terrorism-related information. Collectively,

[14] Reference Executive Order 13354 (August 27, 2004), *National Counterterrorism Center*.

their collaboration with the Federal government, with one another (State-to-State, State-to-locality), and with the private sector represents a tremendous increase in both the nation's overall analytic capacity and the multi-directional flow of information. It is important to note that these centers are not homogenous—considerable variations exist in terms of operations and mission focus (e.g., homeland security, law enforcement, emergency response). To date, more than 40 such centers have been established across the United States, and significant effort has gone into developing and adopting standards to facilitate easier information access, sharing, and use.[15]

To capitalize on this collective progress, the PM-ISE and Federal departments and agencies took a number of important steps in the past year that are making a positive impact on the nation's ability to share terrorism information:

1. Implementing an Initial Operating Capability (IOC) for Electronic Directory Services (EDS) across Sensitive Compartmented Information (SCI) and Secret networks. The PM-ISE, in consultation with the ISC, and as required by IRTPA, delivered electronic directory services that enabled certain ISE participants to access an organizational directory ("blue pages") that provides 24/7 contact information for those organizations that possess or acquire terrorism information;[16]
2. Capturing the inventory of existing terrorism information sharing resources (policies, procedures, programs, systems, architectures, and standards). Consistent with Presidential Requirement 1(a), the PM-ISE completed a working inventory of these resources, which form the basis for some of the specific implementation actions in this plan;
3. Developing a framework through which terrorism information can be shared between and among Federal and SLT governments and the private sector. Consistent with Presidential Guideline 2, the Attorney General and the Secretary of Homeland Security, in consultation with the PM-ISE, the ISC, and other Federal departments and agencies, have established a Presidentially-approved framework that will strengthen the sharing of terrorism information across these jurisdictional boundaries and will coordinate Federal efforts with those at the State and local levels;[17]
4. Addressing issues related to sharing Sensitive but Unclassified (SBU) information. In accordance with Guideline 3, the Secretary of Homeland Security and the Attorney General have captured an inventory of Federal government SBU procedures and conducted work towards formulating recommendations for standardizing marking and handling procedures for homeland security information, law enforcement information, and terrorism

[15] For example, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Washington, DC: 2005). Developed in collaboration by the Department of Justice (DOJ), Department of Homeland Security (DHS), and members of the DOJ's Global Justice Information Sharing Initiative and DHS's Homeland Security Advisory Council.
[16] See Chapter 5 for further details.
[17] See Chapter 7 for a fuller discussion of Guideline 2.

information (efforts to complete the Guideline 3 recommendations continue);[18]

5. Facilitating and strengthening the sharing of terrorism information with foreign partners. In accordance with Presidential Guideline 4, the Secretary of State and the interagency Foreign Government Information Sharing Working Group, in coordination with the PM-ISE, developed recommendations approved by the President to facilitate terrorism information sharing with foreign partners and allies;[19]
6. Ensuring the protection of privacy and civil liberties. Consistent with Presidential Guideline 5, the Attorney General and the Director of National Intelligence (DNI), in coordination with the PM-ISE and the heads of Federal departments and agencies that possess or use intelligence or terrorism information, developed privacy guidelines approved by the President for the ISE;[20]
7. Fostering a culture of information sharing across the Federal government and with all ISE participants regardless of their organizational affiliation. In accordance with Presidential Requirement 2, the PM-ISE and ISC members are developing initiatives, including training and performance measurement, that will stimulate the development of this culture and that will build trust among ISE participants;
8. Testing and fielding operational demonstrations that illustrate the benefits of sharing information. The PM-ISE is actively working with Federal departments and agencies to field tangible demonstration projects that support the ISE participants. An example is a joint project with the Federal Bureau of Investigation (FBI) to upgrade its existing wireless infrastructure to function as a test bed for evaluating advanced SBU wireless technologies and capabilities. The objective is to transmit federally held terrorism information into a usable form to Federal, State, and local counterterrorism personnel through wireless devices, including laptops and personal electronic devices; and
9. Assisting the Records Access and Information Security Policy Coordination Committee (RAIS PCC) to review and possibly update E.O. 12958, *Classified National Security Information.* WMD Commission Recommendation 9.7 called for proposed standards to simplify and modernize the information classification system with particular attention to implementation in a network-centric ISE.[21]

[18] See Chapter 10 for a fuller discussion of Guideline 3.
[19] See Chapter 7 for a fuller discussion of Guideline 4.
[20] See Chapter 9 for a fuller discussion of Guideline 5.
[21] Note details of the proposed E.O. 12958 (April 17, 1995) amendments are documented in: Records Access and Information Security PCC, *Proposed Amendments to E.O. 12958 Responding to WMD Commission Recommendation 9.7 As of June 9, 2006* (PCC: Washington, DC, 2006).

1.4 Today's ISE

The ISE must enable all levels of government, the private sector, and our foreign partners to fill vital roles in preventing, preparing for, and quickly responding to terrorist threats and attacks. Mission-oriented information sharing solutions must support the analysis of disparate pieces of information and their translation into concise, actionable, and, where possible, unclassified formats. Further, these solutions must ensure the appropriate access to—and the sharing, integration, and use of—terrorism information by ISE participants. Despite growing recognition that State and local fusion centers represent a critical component of our nation's counterterrorism efforts, no national strategy or protocols define how Federal departments or agencies will collaborate with these centers. Accordingly, each center has developed its own way of interfacing with the various Federal departments and agencies involved in terrorism prevention and response. At the same time, those same Federal departments and agencies have established protocols with different fusion centers in a manner that varies across the States.

Historically, terrorism information sharing occurred in multiple sharing environments designed to primarily serve the intelligence, law enforcement, defense, homeland security, and foreign affairs communities.[22] Each community developed its own policies, rules, standards, architectures, and systems to channel information to meet mission requirements.[23] Accordingly, few coordinated and collaborative processes existed to address information sharing, and there emerged gaps in sharing.

Identifying and rectifying these gaps is a highly complex undertaking. Today's ISE—and the ISE of the future—exist in a dynamic, unpredictable threat environment. As threats change, information needs shift, and technologies evolve, the ISE must prove resilient, sustainable, and adaptable. To their great credit, over the past five years all levels of government, the private sector, and our foreign partners have taken concrete steps to strengthen the nation's ability to share terrorism information. These steps include revisions to existing policies and procedures and development of new policies and guidelines; creating and investing in information fusion centers at all levels of government; funding and fielding new collaborative capabilities and programs that allow ISE participants to share with one another; and implementing systems, architectures, and standards to provide solutions for ISE users that enable them to access, share, and analyze terrorism information.

Despite this progress, significant hurdles in the current or "As-Is" ISE remain that prevent it from delivering the full range of functions and services needed by ISE participants.[24] Accordingly, a robust information sharing framework is required to

[22] For the purposes of the ISE IP, the term "homeland security community" includes the Department of Homeland Security and those agencies with public health and welfare, emergency response, transportation, fire, and emergency management.
[23] In actuality, some Federal departments and agencies belong to more than one Community. For example, the FBI is part of the law enforcement community but has an element that is part of the Intelligence Community.
[24] See Section 3.2.1 of this plan for a more detailed description of today's ISE.

address these deficiencies and to establish an integrated approach through which ISE participants coordinate and share terrorism information—vertically between levels and horizontally within each level.

1.5 Overview of the Future ISE

Transforming the current ISE into one that facilitates improved coordination and expedited access to protected terrorism information by all levels of government and, when appropriate, the private sector and foreign partners is a national imperative. This transformation requires a vision to clearly define the framework, roles, and responsibilities for future information sharing around which national policies, priorities, and partnerships coalesce. The vision for the ISE is:

> A trusted partnership between all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America by the effective and efficient sharing of terrorism information.

Flowing from this vision is the requirement for an operating environment that draws upon existing systems and capabilities, empowers Federal departments and agencies in the fulfillment of their assigned roles and responsibilities, builds the analytic capacity and technical methodologies that enable all ISE participants to improve the sharing and analysis of information, and mandates a coordinated, collaborative, and interconnected approach to sharing terrorism information.

This operating environment also recognizes the important role played by State and local fusion centers and, while assisting them in meeting certain thresholds of capability and complying with all applicable privacy laws, integrates those fusion centers into a national information sharing structure. Ultimately, this framework is intended to improve the flow of terrorism information, broaden the connectedness of all ISE participants, enhance the nation's overall analytic capacity, and clarify roles, responsibilities, and reporting expectations. Further, this operating environment recognizes the "all-crimes and all-hazards" nature of State and local sharing, where SLT organizations may share and fuse together multiple types of information to address a variety of needs including law enforcement, preparedness, and response and recovery. In many instances, this information may not initially be recognized as terrorism information, but may be information that could ultimately prove crucial in preventing, preparing for, or responding to terrorism. The ISE focus on terrorism information will not impede or interrupt these additional fusion center functions.

To be effective, the ISE must meet six goals (see Figure 1.5-1 below).

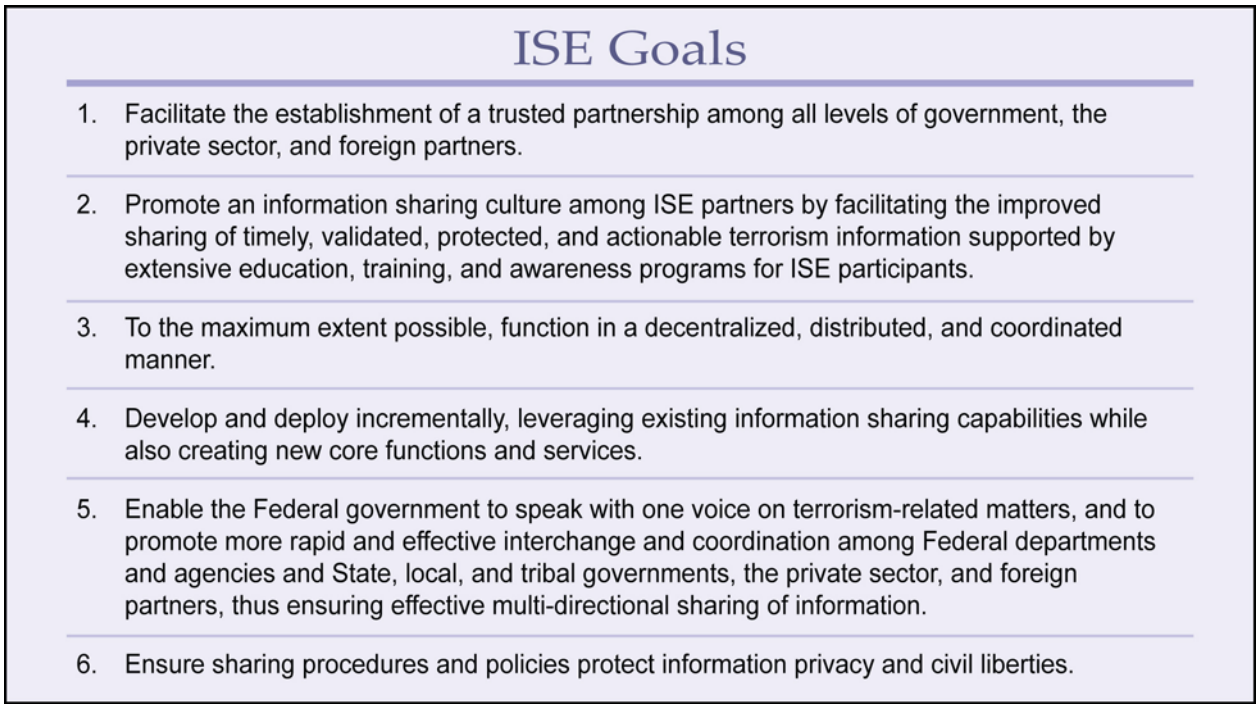


Figure 1.5-1. ISE Goals

To realize these goals, the ISE must be structured in a more unified, coordinated manner to empower ISE participants to capitalize on enhanced information sharing capabilities and functions. Specifically:

1. *For the President, and his advisors*, it must provide complete, accurate, and valid information drawn from multiple sources upon which to base policy and operational decisions;
2. *For Federal departments and agencies*, it must provide new sources of information from other Federal, SLT, private sector, and foreign partners in a secure, trusted environment that protects information and sources and methods;
3. *For SLT governments*, it must create a recognizable Federal focus for federally coordinated terrorism information, one that generates more tailored, actionable information and improves situational awareness at all levels and supports the development of a true national analytic capacity;
4. *For the private sector*, it must establish a coordinated source—across Federal, State, local, and tribal boundaries—for access to terrorism information, alerts, warnings, and situational awareness;
5. *For foreign partners*, it must create an environment in which terrorism information provided to or received from foreign governments is appropriately and adequately safeguarded and is made available, as appropriate to Federal departments and agencies;

6. *For individuals*, it must protect information privacy and other legal rights of Americans;
7. *For all ISE participants*, it must create an environment where users rely on a clearly defined set of institutionalized authorities, roles, and responsibilities and trusted systems, not the traditional emphasis on personal relationships; and
8. *For all ISE participants*, it must create common certification and accreditation and other security policies and standards that allow for the efficient implementation of technology solutions.

This page intentionally blank.

Chapter 2 – Information Sharing Strategy, Roles, and Needs

2.1 Information Sharing Strategy

In the aftermath of the September 11, 2001, attacks and the ensuing War on Terror, multiple groups examined terrorism and homeland security issues, and produced recommendations to strengthen the sharing of terrorism information.[25] The recommendations included creating a distributed, decentralized, and trusted information network with equivalent or greater levels of security; facilitating better sharing of terrorism information across Federal agencies with collection, analysis, and dissemination authorities, roles, and responsibilities; reducing impediments to the multi-directional flow of information across Federal, SLT, private sector, and foreign partners; and sorting out the myriad of legal, policy, organizational, cultural, and technical barriers to sharing. Consistent with those recommendations, IRTPA and the Presidential Information Sharing Guidelines and Requirements call for creating an ISE to provide and facilitate the means for sharing terrorism information among all appropriate Federal agencies, SLT governments, and the private sector through the use of policy guidelines and technologies.[26]

The strategy for achieving this vision involves using all authorities, resources, programs, and capabilities available to ISE participants to execute this plan as effectively as possible and to promote a culture where sharing terrorism information is a core value. While IRTPA largely focuses on Federal departments and agencies sharing terrorism information with one another or with non-Federal ISE participants, the resulting environment—the aggregation of the legal, policy, cultural, organizational, and technological conditions that influence terrorism information sharing—holds the promise of greatly improving information sharing among all ISE participants (e.g., Federal-to-State, State-to-State, State-to-locality, government-to-industry, Federal government-to-foreign ally). Only through the coordinated efforts of Federal, SLT, private sector, and foreign partners can the ISE realize this full potential.

2.2 Organizational Roles, Missions, and Responsibilities

Under the direction of the DNI, the PM-ISE and Director of the NCTC, in coordination with the heads of relevant Federal departments and agencies, reviewed and identified the respective missions, roles, and responsibilities of those executive departments and agencies with regard to terrorism information sharing, in accordance with Requirement 1(b) of the Presidential Information Sharing Guidelines and Requirements. To accomplish this task, the NIP, in addition to responding to the priorities of NSPD-

[25] The National Commission on Terrorist Attacks Upon the United States, the Markle Foundation's report *Creating a Trusted Information Network for Homeland Security*, and numerous Government Accountability Office (GAO) reports examining Federal information sharing issues (e.g., GAO-06-15, GAO-06-497T, GAO-06-385, and GAO-06-383).
[26] IRTPA, Section 1016(b)(2).

46/HSPD-15, addresses the deliverables called for in Requirement 1(b). At the direction of the President, NCTC led the effort and Federal departments and agencies coordinated and collaborated in its development.

In addition, pursuant to Presidential Guideline 2, the Attorney General and the Secretary of Homeland Security developed recommendations that were approved by the President regarding the creation of a common framework for sharing terrorism information among Federal departments and agencies and SLT governments, law enforcement agencies, and the private sector. The NIP and Guideline 2 will be further leveraged when implementing the missions, roles, and responsibilities for the ISE.

IRTPA also requires that this plan identify "the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE)."[27] Although it is possible that any ISE participant may be called on to provide infrastructure, the primary infrastructure providers for the five communities are as follows:

- Intelligence Community—Director of National Intelligence;
- Law Enforcement—Attorney General;
- Defense—Secretary of Defense;
- Homeland Security—Secretary of Homeland Security; and
- Foreign Affairs—Secretary of State.

In implementing the ISE, ISE participants should avoid unnecessary infrastructure duplication by participating in interagency agreements that promote shared use of ISE infrastructure by multiple departments and agencies. This includes leveraging ongoing infrastructure modernization activities, agency enterprise architecture efforts, and the Federal Enterprise Architecture (FEA).[28]

2.3 Information Sharing Needs of ISE Participants

By its nature, the ISE involves many diverse participants, each with their own responsibilities and needs for terrorism information. Each Federal department and agency, SLT government, the private sector, and foreign ally acquires, uses, and retains various types of terrorism information and operates within a set of established laws, policies, and business rules. In many instances, however, these laws, policies, and rules differ and create both real and perceived impediments to information sharing. ISE implementation will take into account ISE participants' needs and missions as outlined in the following sections.

[27] IRTPA, Section 1016(e)(10).

[28] FEA is a business-driven framework that defines and aligns Federal business functions and supporting technology using a set of five common models (performance, business, services, data, and technology). See Chapter 6 for a fuller description of ISE architecture efforts.

2.3.1 Federal Department and Agency Needs

At the Federal level, each department and agency involved in counterterrorism has its own mission and attendant information needs and maintains its own mission-specific criteria for identifying, assessing, and managing risks. In the current threat environment, however, there is a risk that seams in these missions may allow terrorist activity to go undetected. Consistent with IRTPA, the Presidential Information Sharing Guidelines and Requirements, and the NIP, objectives at the Federal level related to sharing terrorism information include:

1. Managing the risks associated with broadly sharing terrorism information to address national and homeland security interests while protecting the information privacy and other legal rights of Americans as well as the information itself, including sources and methods;
2. Promoting a culture that produces analysts from across the ISE who are aware of the need to share terrorism information and are trained in the legal, policy, security, and procedural issues;
3. Utilizing technologies and business processes that maximize the effectiveness of sharing, analyzing, and disseminating terrorism information;
4. Ensuring secure access to terrorism information and reliable communication (the accessible and reliable means by which terrorism information is transmitted);
5. Connecting all levels of government and, as appropriate, the private sector to maximize the flow of information to facilitate its use in analysis, investigations, and operations;
6. Making complete, tailored, timely, and validated terrorism information available to decision makers and operational personnel responsible for detecting, preparing for, identifying, and responding to threats;
7. Ensuring the ISE facilitates and improves the transmission of maximum forewarning and situational awareness of terrorist activities to increase the time available to mount an effective national response;
8. Leveraging current and developing new systems and capabilities to ensure direct, continuous online access to electronic directory services to link to analysts in a secure, trusted environment; and
9. Treating the Federal government as a consumer as well as a supplier of terrorism information, recognizing that the Federal government requires access to SLT and private sector information as well as information from foreign sources.

2.3.2 State, Local, and Tribal Government Needs

Since 9/11, over 40 states and major urban areas have established statewide and regional fusion centers to deal with terrorist threats.[29] Moreover, a growing number of localities, particularly in major urban areas, are establishing similar fusion centers to coordinate the gathering, analysis, and dissemination of law enforcement, public safety, and terrorism information. These fusion centers—and other SLT and regional initiatives—represent enormous financial, human, and technical resources at the State and local levels to combat the threat of terrorism.

Recognizing the need to enhance information sharing with these centers, several Federal departments and agencies—including DHS, FBI, and DoD—launched efforts to develop strategies to incorporate these fusion centers into their information and intelligence activities. Most of these planning efforts, however, focused on how individual agencies collaborate with those centers.[30] As these centers continue to proliferate, consume additional Federal, State, and local resources and investments, and grow in sophistication, there is a need to focus even greater attention on leveraging and connecting them together—through policy, business processes, and technology—to increase the nation's overall analytic capacity.[31]

The needs of SLT governments continue to mount as they incorporate counterterrorism and homeland security activities into their day-to-day missions. Specifically, they need to ensure that personnel protecting local communities from a terrorist attack—or responding to an attack—have access to timely, credible, and actionable information and intelligence regarding individuals and groups intending to carry out attacks within the United States (including homegrown terrorists), their organization and financing, at-risk potential targets, pre-attack indicators, and other major events or circumstances requiring action by SLT governments. Thus, objectives of SLT governments related to sharing terrorism information include:

1. Sharing information to address terrorism investigations in a manner that protects the information privacy and other legal rights of Americans;
2. Fostering a culture that recognizes the importance of fusing all-crimes and all-hazards information to identify information that might provide indications of terrorist plots;
3. Supporting efforts to detect and prevent terrorist attacks by maintaining situational awareness of threats, alerts, and warnings;
4. Promoting the compatibility of homeland security strategies and Critical Infrastructure Sector Specific Plans with the ISE to ensure the security,

[29] *State and Regional Intelligence Fusion Center Contact Information*, National Criminal Intelligence Resource Center (March 8, 2006).
[30] For example, DHS is developing a departmental strategy for collaborating with State and local fusion centers. The FBI is developing a strategy for linking the activities of its Field Intelligence Groups with those same centers. DoD is working through the National Guard and U.S. Northern Command with the fusion centers in support of its homeland defense mission.
[31] See Section 7.1 of this plan for more details on collaborating with fusion centers and next steps.

resiliency, and prompt restoration of infrastructure operations (e.g., electric power, transportation, telecommunications, etc.) within a region, State, or locality;

5. Working with the Federal government to determine the appropriate allocation of funding, capability development, and other resource decisions relating to the sharing of terrorism information; and
6. Developing training, awareness, and exercise programs to ensure that the ISE is implemented in a way that better enables SLT personnel to recognize and address terrorist strategies, tactics, capabilities, and intent and to effectively manage attendant risks.

2.3.3 Private Sector Organization Needs

Private sector information represents a crucial element in both understanding the current threat environment and protecting our nation's critical infrastructure from targeted attacks. Protecting the interconnected and interdependent U.S. infrastructure also requires a robust public-private partnership that provides the private sector with information on incidents, threats, and vulnerabilities, as well as protects private sector information in such a way that the private sector is willing to share it with government partners. The National Infrastructure Protection Plan (NIPP), released recently by DHS, is the cornerstone document that creates a public-private partnership structure through which to affect a national implementation strategy for HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*.[32]

In today's business world, corporate executives face competing pressures that include meeting global market demands, managing risks to their enterprise, protecting trade secrets and proprietary information, and limiting corporate and shareholder exposure to legal liabilities. As the owners and operators of the vast majority of the nation's critical infrastructure, private industry has terrorism information of potential value to the government. At the same time, the private sector needs and seeks appropriate access to terrorism information for situational awareness, to manage risks to their enterprises, and to understand the national security implications posed by terrorist threats.

The primary conduits for sharing terrorism information today are the Sector Coordinating Councils and sector-specific Information Sharing and Analysis Centers (ISACs) established by the NIPP, and the National Infrastructure Coordination Center. To date, however, sharing through these mechanisms has yielded mixed results. Four factors are frequently cited to explain the obstacles to the bi-directional flow of information with the private sector. First, significant distinctions among the seventeen critical infrastructure and key resources sectors as defined in HSPD-7 (e.g., regulatory regimes, number of players, willingness to collaborate) make it difficult to create a single

[32] HSPD-7 instructs Federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. See Section 7.2 of this plan for more details on HSPD-7 and the NIPP.

approach to information sharing operations, structure, and processes. Second, the private sector reports that the demand from Federal, State, and local governments for critical infrastructure and other information since 9/11 has multiplied many times over, imposing more demands on industry to collect information and report it. Third, requests for such information are rarely coordinated or consistent, resulting in duplicative requests. Finally, from the private sector's perspective, the interrelationships between Federal and SLT governments are ambiguous. Accordingly, objectives of the private sector related to sharing terrorism information include:

1. Sharing information to manage risks to business enterprises and in a manner that protects the information privacy and other legal rights of Americans;
2. Creating a national framework and culture for sharing information that rationalizes requests for terrorism information to the private sector and that adequately protects the risks and proprietary interests of corporations;
3. Creating an integrated, trusted environment in which information can be shared, maintained, and protected;
4. Ensuring access to the integration and analysis of data from multiple sources to provide industry with indicators of impending threats or current attacks;
5. Receiving actionable alerts and warnings concerning specific industries that improve their situational awareness of terrorist threats and enable them to prioritize risks and security investments, and shape the development of plans to ensure the security, continuity, and resiliency of infrastructure operations; and
6. Implementing policies and mechanisms that provide liability and antitrust protections to the private sector in connection with sharing information in good faith.

2.3.4 Foreign Partner Needs

Collaboration with foreign partners also is critical to our nation's strategy to execute the War on Terror. Ensuring strong, effective cooperation with our foreign partners requires sharing terrorism information in many forms. In doing this, we must protect the privacy, civil liberties, and other legal rights of individuals; sensitive sources and methods; and law enforcement and national and homeland security equities.

In return, the Federal government, in handling terrorism information obtained from foreign partners, must observe foreign government security and other requirements. Accordingly, objectives for sharing terrorism information with foreign partners include:

1. Developing with foreign governments the practices, rules, cultures, and standard language for dealing with the information privacy and other legal rights of Americans;

2. Maintaining the privacy and security restrictions of foreign governments, possibly through "tear line" approaches that maximize the distribution of foreign government information;
3. Creating a central, electronically accessible repository of information on foreign government and international organization marking and handling regimes so that ISE participants can more readily understand the safeguarding and handling rules for different kinds of foreign government information;
4. Developing appropriate common standards or protocols for electronic handling of foreign government information within the ISE to ensure that any necessary foreign government requirements are respected;
5. Developing systems, training programs, and agency-specific disclosure procedures for foreign disclosure officers to make and expedite sharing decisions and to release classified information to foreign governments;
6. Reviewing authorities and related issues created while determining standards for sharing SBU information with foreign partners; and
7. Making information regarding foreign government protection of U.S. information more widely available and (where needed) providing foreign partners technical assistance on best practices for protecting U.S. information to increase the flow of terrorism information to foreign governments.

2.3.5 Information Privacy and Civil Liberties Needs

Protecting the information privacy and other legal rights of Americans remains paramount in establishing the ISE. In its report, the 9/11 Commission stated, "While protecting our homeland, Americans should be mindful of threats to vital personal and civil liberties. This balancing is no easy task, but we must constantly strive to keep it right." E.O. 13388 requires that "To the maximum extent consistent with applicable law, agencies shall … give the highest priority to … the interchange of terrorism information between agencies… [and shall] protect the freedom, information privacy, and other legal rights of Americans." With this in mind, ISE privacy and civil liberties objectives related to sharing terrorism information include:

1. Reviewing and adopting policies and procedures for handling protected information within the ISE and clarifying ISE participant responsibilities as custodians of that information; [33]

[33] "Protected information" is information about U.S. citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the Intelligence Community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the Federal government expressly determines by Executive Order, international agreement, or other similar instrument to be covered by Presidential Guideline 5.

2. Cataloguing agency data holdings to ensure that protected information that an agency makes available through the ISE has been lawfully obtained and made available consistent with authorized purposes;
3. Implementing mechanisms to enable ISE participants to determine the nature of the protected information that an agency is making available and to ensure it is handled in accordance with applicable legal requirements;
4. Adopting and implementing procedures to ensure the protected information is accurate and is not erroneously shared through the ISE;
5. Implementing appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction;
6. Developing policies and procedures for reporting, investigating, and responding to violations of policies and procedures regarding the handling of protected information;
7. Training personnel authorized to share protected information through the ISE on their agency's requirements and policies for the collection, use, and disclosure of protected information; and
8. Designating an ISE Privacy Official to receive reports and coordinate agency-specific privacy policies and procedures to ensure their consistency and compliance with ISE Guidelines.

Chapter 3 – ISE Operational Concept

3.1 Introduction

How we obtain, use, and share information is a major factor in our success in preventing terrorist attacks within the United States, reducing our vulnerabilities to terrorism, and minimizing the effects of any attacks that do occur. The following operational concept captures the ISE vision, goals, and attributes identified in Chapter 1 and the information sharing needs of Federal agencies, SLT governments, the private sector, and foreign partners articulated in Chapter 2. Under this concept, the ISE will leverage the roles, responsibilities, and capabilities of individual ISE participants to develop and institutionalize a "shared" environment in which information becomes the true *force multiplier* needed for the effort to combat terrorism.

The ISE will enable the rapid exchange of terrorism information whether collected, produced, or distributed by intelligence, law enforcement, defense, homeland security, foreign affairs, or other communities, including the private sector and foreign partners. It will provide access to and accommodate all types of data, including structured and unstructured data and finished intelligence products, at all levels of security. Whenever possible, the ISE will include data provided from multiple sources to build a composite picture of the terrorist threat. The following are general characteristics of terrorism information that will help in determining what should be shared within the ISE:

1. Terrorism information as defined in IRTPA, including information that, when correlated with other data and analyzed, may identify terrorists and show patterns of terrorists or terrorism related activities;
2. Information that is timely and can potentially influence actions to be taken;
3. Information tailored to the needs of individual ISE participants—the right information provided at the right time, over the right pathways—to support the mission needs of ISE participants; and
4. Information that can be exchanged within the system of rules established to protect that information, including sensitive sources and methods as well as the information privacy and other legal rights of Americans.

3.2 The Information Sharing Environment

3.2.1 The Current ("As-Is") Environment

Since 9/11, Federal departments and agencies have made significant progress toward establishing processes and protocols and developing technologies to support terrorism information sharing. More often than not, these efforts focused on creating capabilities critical to the counterterrorism missions of individual Federal departments and agencies.

Over the past five years, Federal and SLT governments have taken major strides in each mission area. However, optimal performance requires a greater degree of coordination and integration than exists today. Decision-makers in Federal and SLT governments and the private sector require access to a broad spectrum of terrorism information to provide an integrated view that supports collaborative counterterrorism operations. Today's "As-Is" environment does not consistently provide the optimal level of cross-community terrorism information sharing.

Ultimately achieving the Future ("To Be") state first requires a comprehensive understanding of the "As-Is" (or pre-IRTPA) environment. IRTPA and the Presidential Information Sharing Guidelines and Requirements point to six areas essential to the development of the ISE:

1 Policies. Absent an overarching, cross-community policy for terrorism information access and sharing, individual policies evolved to meet the needs of Federal departments and agencies shaped by their respective statutory authorities and responsibilities. The result is a body of overlapping or independent policy regimes, inconsistent procedures for handling SBU information, and multiple forums at the Federal level, for SLT and private sector organizations;

2. Procedures. No single framework for information priorities exists to guide the non-Federal counterterrorism community. The Office of the DNI (ODNI), FBI, and DHS have all launched efforts to address this particular shortfall. These efforts, however, have yet to be fully integrated to meet the needs of SLT and private sector organizations. Additionally, although warning and notification processes have improved, alert, tip, advisory, situational awareness, and warning systems are often incompatible and not well understood outside of individual agencies or communities;

3. Programs. Each State conducts counterterrorism operations in a unique environment, often in accordance with its State-specific laws and regulations. The creation of statewide and major urban area fusion centers presents an important opportunity to create a unified Federal interface that can be customized to meet SLT government needs. In addition, these fusion centers have the potential to become integrated with the numerous Federal information sharing and access programs in the field. Finally, there is no integrated, community-wide, comprehensive training program for sharing terrorism information;

4. Systems. There are robust national systems for sharing information at all classification levels, but these systems are not fully interoperable. In addition, terrorism information is often difficult to access because of wide variations in system-specific interfaces. These interfaces inhibit and sometimes prevent information indexing that would allow users to conduct meaningful database searches. In many cases, those who require the information do not even know that such systems exist. Finally, interoperability is achieved via system-

to-system or application-to-application integration, not through "many-to-many" approaches to exchanging data that would enable disparate users and applications to manipulate the same data in ways that meet their respective objectives;

5. Architectures. Federal departments and agencies appear to have made solid progress in developing enterprise architectures according to FEA guidelines. However, it is difficult to judge whether this progress is developmental versus functional. Also unclear is the extent to which individual agencies have focused business-process reengineering efforts on cross-organizational terrorism information sharing and access; and
6. Standards. Strong initiatives to develop standards across the ISE are only beginning to be developed, and creating such standards is a multi-year effort that will need the continued alignment and consolidation as required by Presidential Guideline 1. For example, there are currently no uniform Internet web browser standards; common information protection standards are not used across the community; and, where standards have been established (e.g., the Intelligence Community Public Key Infrastructure standard), they may not be enforced.

Considerable progress has been made towards improving terrorism information sharing and access capabilities among Federal departments and agencies, but much work remains to fully integrate these capabilities and create the ISE envisioned in IRTPA and the Presidential Information Sharing Guidelines and Requirements.

In summary, the "As Is" information sharing environment described in these six functional areas is dominated by a variety of horizontal and vertical distribution paths that result from:

1. Overlapping roles and responsibilities among organizations tasked with counterterrorism and security-related missions;
2. Cultural, policy, and technological differences among organizations tasked with disparate missions;
3. Policy, process, and procedural differences;
4. Incompatible legacy systems; and
5. The absence of universally adopted standards to facilitate the exchange of information.

The lack of defined cross-jurisdictional agreements and clear organizational responsibilities led to an environment in which the flow of terrorism information was inconsistent across the Federal government, and was often limited and uncoordinated among various levels of government. In that environment, without common guidance on information sharing, Federal departments and agencies made independent decisions regarding the value and content of terrorism information to be shared, had limited ability

to share important information broadly, and engaged in varying levels of participation with NCTC and the former Terrorist Threat Integration Center (TTIC). The result was multiple uncoordinated information products distributed among Federal departments and agencies and to SLT governments. More recently, NCTC has developed terrorism information sharing agreements with several Federal departments and agencies, and the NCTC Online (NOL) has enhanced the ability to share terrorism information across the Federal government.

This stove-piped environment is a patchwork of mission-specific information sharing flows that can produce conflicting, confusing, or unusable information. The result is that the information sharing needs spelled out in Chapter 2 may not be met, especially those of State and local ISE participants.

Significant strides have been made in bringing together Federal and State information sources through the NCTC, State and regional fusion centers, and other sharing initiatives such as the Joint Terrorism Task Forces (JTTF), Field Intelligence Groups (FIG), and ISACs. However, much more must be accomplished to facilitate sharing terrorism information in a way that can maximize efforts at the Federal and SLT levels to fuse and correlate terrorism information to strengthen counterterrorism and security-related efforts. For example, FIG activities that are integrated with and complement SLT activities will ultimately enhance fusion center efforts.

The challenge remains to improve coordination of sharing within and across the five Federal communities with counterterrorism responsibilities—intelligence, law enforcement, defense, homeland security, and foreign affairs—and with SLT governments, the private sector, and foreign partners to achieve the coordinated, multi-agency perspective necessary for comprehensive analysis as well as to ensure dissemination of the right information to the right people at the right time.

3.2.2 The Future ("To-Be") Environment

The proposed ISE framework is designed to meet the needs of consumers of terrorism information at every level of government and, as appropriate, with the private sector and foreign partners and allies. It will enable the rapid exchange of terrorism information by creating a more unified, coordinated environment that reflects organizational realities while overcoming unnecessary barriers to information sharing. The ISE will offer a collaborative structure through which terrorism information is shared among ISE participants to support a number of different activities including: preventive and protective actions, immediate actionable response, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from terrorist attacks. To the maximum extent possible, the ISE structure will draw upon and integrate existing capabilities and systems.

At the Federal level, the ISE will affect the operations of a large number of agencies across five previously mentioned communities that process and use terrorism information. Figure 3.2-1 depicts the conceptual basis for the ISE at the Federal level and identifies ISE participants at the SLT levels of government, the private sector, and foreign partners. Strong and effective cooperation at each level, between mission partners, and between each of the organizations engaged is vital for success in the War on Terror. The ISE depicted in this model is intended to be inclusive—to support and facilitate terrorism information sharing between Federal departments and agencies, with SLT governments, with the private sector, and with foreign partners and allies. Chapters 5 and 6 provide additional detail on the Federal ISE, and Chapter 7 extends these capabilities to SLT, the private sector, and foreign partners. Furthermore, as ISE implementation proceeds, the PM and the ISC will continue to develop the policies, business process, and capabilities required to fully realize this operational concept.

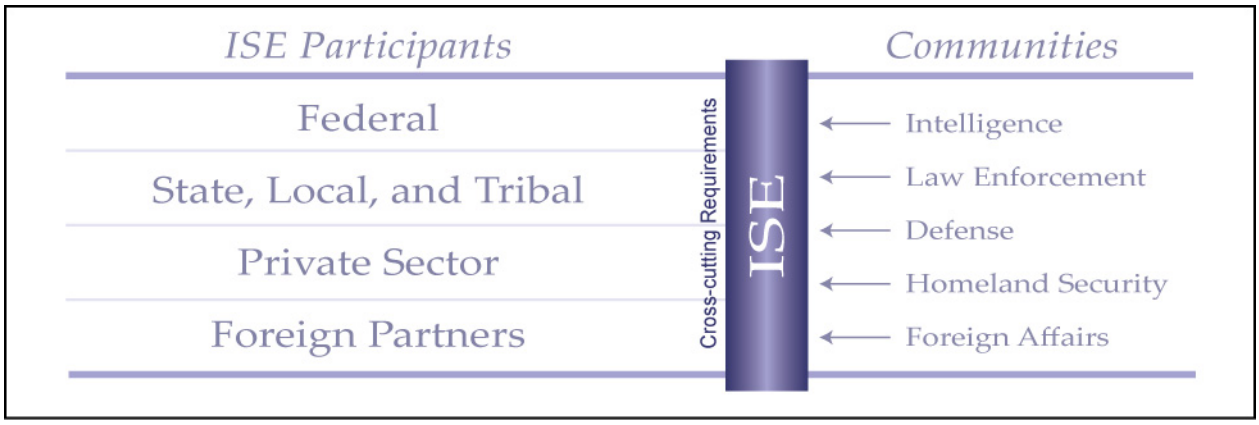


Figure 3.2-1. Conceptual Basis for the ISE

3.3 Federal Level Elements and Functions

The Federal component of the future ISE will provide access to terrorism information using the three constructs described below.

3.3.1 The National Counterterrorism Center

The NCTC is the primary organization in the Federal government for analyzing and integrating all intelligence possessed or acquired by the Federal government pertaining to terrorism and counterterrorism (except for intelligence specific to domestic terrorism and domestic counterterrorism).[34] Consistent with applicable law and the direction from the President, the NCTC may receive intelligence pertaining exclusively to domestic

[34] National Security Act of 1947, as amended (50 U.S.C. 402 et seq.).

counterterrorism from any Federal or SLT government, or other source necessary to fulfill its responsibilities and retain and disseminate such intelligence.[35]

NCTC serves as the central and shared knowledge bank on known and suspected terrorists and international terror groups; ensures agencies, as appropriate, have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis; and ensures that such agencies have access to and receive intelligence needed to accomplish their assigned activities. Any agency authorized to conduct counterterrorism activities may request information from the Center to assist it in its activities, consistent with applicable law and guidelines provided for the provision of and access to intelligence.[36] NCTC enables the sharing of a wide spectrum of terrorism intelligence and related information among thousands of users in the Federal counterterrorism community through its secure web site, NOL that operates in separate security domains.

3.3.2 Federal Departments and Agencies

Figure 3.2-1 depicts the five communities that participate in the ISE at the Federal level and that also support the SLT and private sector framework developed in response to Presidential Guideline 2. The objective of this framework is to empower participating Federal organizations in the fulfillment of their respective roles and responsibilities, and ensure a coordinated, collaborative approach to sharing terrorism information with SLT, private sector, and foreign partners in the ISE. It will support and leverage the success of ongoing initiatives at each level of government, offer practical solutions to challenges that emerge *en route* to ISE implementation, and provide the multi-agency perspective necessary to achieve the objectives of information sharing. In addition, as the ISE matures, policy and technology will introduce additional data sets not currently included or available within these Federal communities.

All Federal departments and agencies that possess or acquire terrorism information must provide access to such information to NCTC for analysis and integration in the broader context of the War on Terror unless prohibited by law or otherwise directed by the President. NCTC, in its capacity as the Federal entity with primary responsibility "for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism," will work in partnership with and in support of appropriate Federal departments and agencies, to enable the development of terrorism information products tailored to the needs of SLT governments.[37] Under the framework established for Presidential Guideline 2, Federal departments and agencies assigned mission-specific roles will also provide terrorism information to the newly formed Interagency Threat Assessment and Coordination Group (ITACG), which will facilitate the production of "federally-coordinated" terrorism information products intended for dissemination to State, local,

[35] National Security Act of 1947, as amended, Section 119(e)(1).
[36] IRTPA, Section 1021.
[37] IRTPA, Section 1021.

and tribal officials and private sector partners. Mission-specific information provided by existing, agency-specific channels (e.g., FBI, DHS, DoD) would continue to be disseminated in accordance with established procedures.

3.3.3 Interagency Threat Assessment and Coordination Group

Participants in the ITACG will engage in collaborative decision-making to ensure timely and effective production, integration, vetting, sanitization, and communication of terrorism information that cuts across multiple agencies to inform and empower State, local, and tribal partners. This information will be integrated from the maximum available sources. Consistent with the directives of Congress and the President to build upon existing systems and capabilities, the ITACG will be at the NCTC. DHS will assign a senior official to manage and direct the day-to-day activities of the ITACG. Decision-making authority regarding how various types of information will be disseminated to SLT officials and the private sector will be primarily shared between DHS and DOJ and will include other agencies as appropriate.

DOJ and DHS will lead an effort to develop standard operating procedures to govern how best to integrate the activities of the ITACG with existing Intelligence Community (IC) production protocols. The ITACG will include representatives from DHS, FBI, DoD, and other relevant Federal organizations. A primary purpose of the ITACG will be to ensure that classified and unclassified intelligence produced by Federal organizations within the intelligence, law enforcement, and homeland security communities is fused, validated, deconflicted, and approved for dissemination in a concise and, where possible, unclassified format. When appropriate and practicable, reports disseminated to SLT governments will contain suggested action items. Although collocated with the NCTC, the ITACG will not be a part of NCTC and will not replicate or supplant the analytic and/or production efforts of the NCTC; nor is it intended to duplicate, impede, or otherwise interfere with existing and established counterterrorism roles and responsibilities. Information flow between Federal, SLT, and private sector partners will be consistent with processes and procedures defined in Presidential Guideline 2.

3.4 State, Local, and Tribal Level Elements and Functions

SLT-level components of the ISE are expected to build on current efforts to incorporate the functions of gathering, processing, analyzing, and disseminating terrorism information into their core missions. Designated fusion centers will serve as the primary points of contact within states or regions for further disseminating terrorism information consistent with DOJ/DHS *Fusion Center Guidelines and* applicable State, local, and tribal laws and regulations. The functions these centers perform—commonly referred to as “information fusion”—are now operational in more than 40 States and major urban areas across the United States. In the spirit of a federated or shared-responsibility approach to information sharing, the Federal government will work to leverage these initiatives to facilitate effective nationwide terrorism information sharing. Fusion centers will become the focus—but not exclusive focal points—within SLT governments for

receiving and sharing terrorism information. This approach will require that the fusion centers achieve a baseline level of capability and comply with all applicable privacy laws as described in the recent Global/Homeland Security Advisory Council (HSAC) Fusion Center Guidelines—many of which have already been incorporated into the business processes of a number of existing fusion centers.

3.4.1 State and Major Urban Area Fusion Centers

The Federal government will promote the establishment of a nationwide and integrated network of State and major urban area fusion centers to facilitate effective terrorism information sharing. Consistent with their respective roles and responsibilities, Federal departments and agencies will provide terrorism information to SLT authorities primarily through these fusion centers. Fusion centers will collaborate with such organizations as the JTTFs, FIGs, and ISACs.

Unless specifically prohibited by or subject to classification restrictions, these fusion centers may further customize federally supplied information for dissemination to meet intra- or interstate needs. It is envisioned that locally generated information that is not threat or incident related will be gathered, processed, analyzed, and interpreted by those same fusion centers—in coordination with locally based Federal officials—and disseminated to the national level via the FBI, DHS, DoD, or other appropriate Federal agencies.

Where practical, Federal organizations will assign representative personnel to these fusion centers and, to the extent practicable, will strive to integrate and collocate resources. Furthermore, Federal organizations should undertake the efforts necessary to ensure that all personnel working within the framework understand its essential attributes and the necessity for close coordination and collaboration with Federal counterparts and SLT partners. Activities and responsibilities to be undertaken by State, local, and tribal governments, in consultation and/or coordination with Federal departments and agencies are described in Chapter 7.

3.5 Information Sharing Evaluation Environments

The IIP introduced the concept of information sharing evaluation environments as a cost effective approach for identifying requirements for ISE policies, business processes, capabilities, and standards, and as platforms to demonstrate and evaluate solutions to operational needs in a relatively controlled environment.[38] The experiences of the NCTC contributed to the ideas that formed the basis for the “To Be” environment described in sections 3.2 and 3.3. The use of evaluation environments to address issues that are typical of those confronting the broader ISE will continue to serve as an important tool for refining and expanding on the ISE operational concept. Consequently, ISE implementation will continue to leverage the NCTC as a platform for developing and

[38] Office of the PM-ISE, *The Information Sharing Environment Interim Implementation Plan,* January 2006, page 10.

evaluating solutions to Federal information sharing issues. In addition, DHS, DOJ, and the PM-ISE are in the final planning stages of an effort to identify a State or regional Evaluation Environment as a means of further developing the concepts outlined in section 3.4.

3.6 Cross-Domain Sharing

The Federal portion of the ISE will encompass policies, business processes, and technologies to ensure that terrorism information can be freely and transparently shared across three broad security domains—SCI, Secret, and SBU information as shown in Figure 3.6-1.[39] Since there are requirements for terrorism information in all three domains, the ISE must ensure that the two-way flow of terrorism information across these three domains is accomplished smoothly and securely to support information discovery and knowledge extraction.

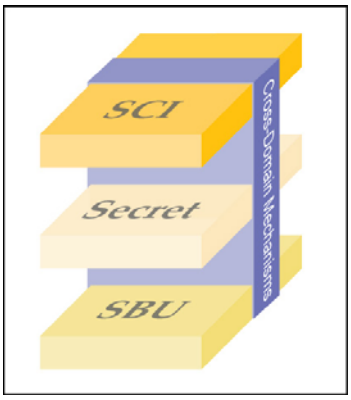


Figure 3.6-1. ISE Security Level Domains

The ISE must provide a relatively seamless environment, recognizing there will be gaps created by the classification of information, the need to meet criteria for access to information, and the physical separation of existing networks. While cross-domain sharing is a difficult problem, an objective of the ISE will be to develop solutions that will support the exchange of information across the different security levels in the ISE with, to the extent possible, minimal need for human review. Cross-domain mechanisms will be designed to facilitate sharing and coordination between different classification levels. These mechanisms include, among others:

1. Tearlines that enable the flow of information to a lower security domain by extracting portions shareable at that level;
2. Controlled interfaces that provide automated, secure, two-way transfer of information between domains;

[39] Strictly speaking, the Secret domain includes all classified, non-SCI systems. The term "Secret" is used to reflect the fact that the vast majority of these systems operate at the Secret level.

3. Information identifiers that inform users, when appropriate, that particular information exists but that is not available to them;
4. Proxies that may be used by a higher-level domain user to access services at a lower level domain while complying with domain security requirements; and
5. Organizational messaging that ensures a trusted exchange of organizational electronic messages between two domain levels.

PART II

How We Intend to Structure the ISE

This page intentionally blank.

Chapter 4 – ISE Implementation Overview

4.1 Two-Phase Implementation Approach

Over the last six months, a number of important steps have been taken to improve the process of implementing and managing the ISE. In consultation with ISC members, the PM-ISE is developing a cross-agency enterprise architecture (EA) that will map ISE business processes and technology onto current agency enterprise architectures. This will help transform existing information resources and infrastructures to support information sharing across Federal organizations, SLT organizations, the private sector, and foreign partners. In addition, the completion of the initial phases of EDS has provided a working model for future ISE implementation efforts. Based on these efforts and the work to address the Presidential Information Sharing Guidelines and Requirements, there is now a better understanding of the steps needed to implement an improved ISE and the approach to carrying them out.

Notwithstanding this progress, achieving the vision and goals set forth in Chapter 1 will entail significant changes to existing policies, business processes, and technical solutions across a complex environment, many of which will involve substantial efforts by ISE participants. Some changes may even require establishing new organizations and relocating others to achieve the degree of collaboration required. Such institutional changes will take time; they cannot be accomplished overnight. Therefore, the plan reflects an approach to develop the ISE incrementally over the next three years.

Recognizing the need to improve the ISE quickly while simultaneously laying the foundation for more comprehensive implementation, this plan adopts a two-phase implementation approach as depicted in Figure 4.1-1. The two phases will overlap, with the initial work for some Phase 2 actions taking place in the latter months of Phase 1.

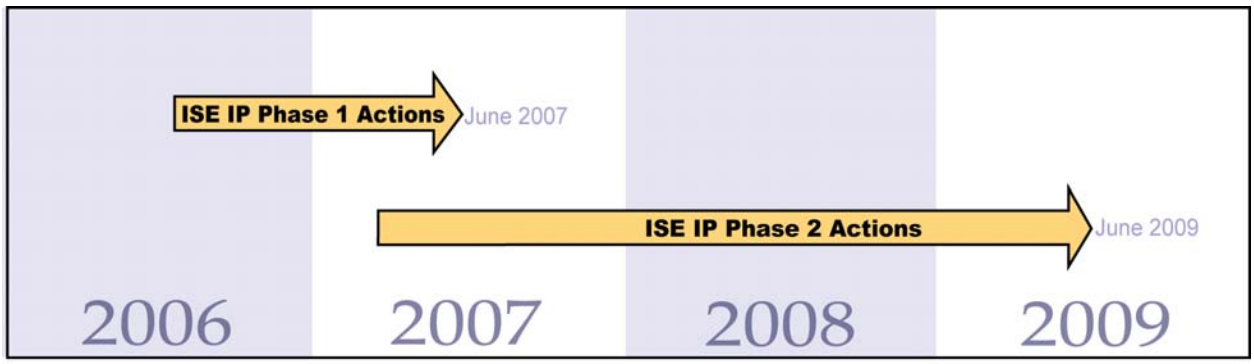


Figure 4.1-1. Two-Phase ISE Implementation Approach

Phase 1 encompasses those actions scheduled for completion by June 2007. These steps are the first in a continuous process to improve the way terrorism information is shared across the Federal government; between Federal agencies and SLT governments; and, as appropriate, with private sector organizations and foreign partners. Phase 1 actions will address the highest priority information sharing requirements and will be sufficiently well defined so that work can begin immediately and be completed by June 2007. In general, these actions will be accomplished with currently planned and programmed resources, primarily by leveraging existing resources, infrastructure, and activities. However, some adjustments to FY 2007 plans and FY 2008 budget submissions will also be required.

Phase 2 includes activities scheduled for completion between June 2007 and 2009. They will often require substantial design and implementation of business processes, supplemented in some cases by fundamental engineering work or incorporation of new technologies. Accordingly, this plan identifies specific Phase 2 actions but acknowledges that they are not currently defined at the same level of detail as those in Phase 1. Typically, Phase 2 activities will require additional planning and design before definitive plans and schedules can be developed. Moreover, Phase 2 activities will often require more significant funding requirements involving multiple ISE participants over several years. Therefore, as the first phase nears completion, the PM-ISE and the ISC will review and prioritize Phase 2 actions and recommend changes to the budgets for FY09 and the out years to ensure that all actions are adequately resourced.

4.2 ISE Governance

4.2.1 General

Given the complexity of managing a two-phased ISE implementation, a sound governance structure is essential to ensure that these activities are carried out and that appropriate mid-course corrections can be made. The existing ISE governance structure is based on the principle that ISE issues should be resolved at the lowest organizational level wherever possible, but that, when necessary, an organized process is in place to elevate these issues for resolution, up to and including the Cabinet level and the President.

In accordance with IRTPA, the President will "determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE."[40] In consultation with the ISC, the PM-ISE is responsible for planning for, overseeing the implementation of, and managing the ISE, including monitoring and assessing progress, and for assisting in "the development of policies, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the ISE."[41]

[40] IRTPA, Section 1016(b)(1)(C).
[41] IRTPA, Section 1016(f)(2)(A)(ii).

The ISC is integral to the success of the ISE—assisting and advising the President and the PM-ISE on establishing, implementing, and maintaining the environment, and ensuring coordination among Federal departments and agencies participating in the ISE. Although the PM-ISE is responsible for overseeing and monitoring ISE implementation, the Federal departments and agencies are responsible for performing actual implementation. Specifically, Federal departments and agencies perform two distinct aspects of ISE implementation: (1) implementing departmental policies, business processes, and systems that are part of the ISE and (2) implementing ISE-wide activities for which the Federal department or agency may be designated as an Information Technology Implementation Agent (ITIA). Chapter 12 provides additional information on the roles and responsibilities of ITIAs.

The PM-ISE regularly interacts with various ISE participants. Through this interaction, the PM-ISE attempts to secure agreement and establish common understanding among ISE participants referring any unresolved issues to the ISC for collaborative resolution. If necessary, matters may be further elevated to senior executive branch officials for consideration and resolution. The existing ISE governance structure is depicted in Figure 4.2-1 and described below.

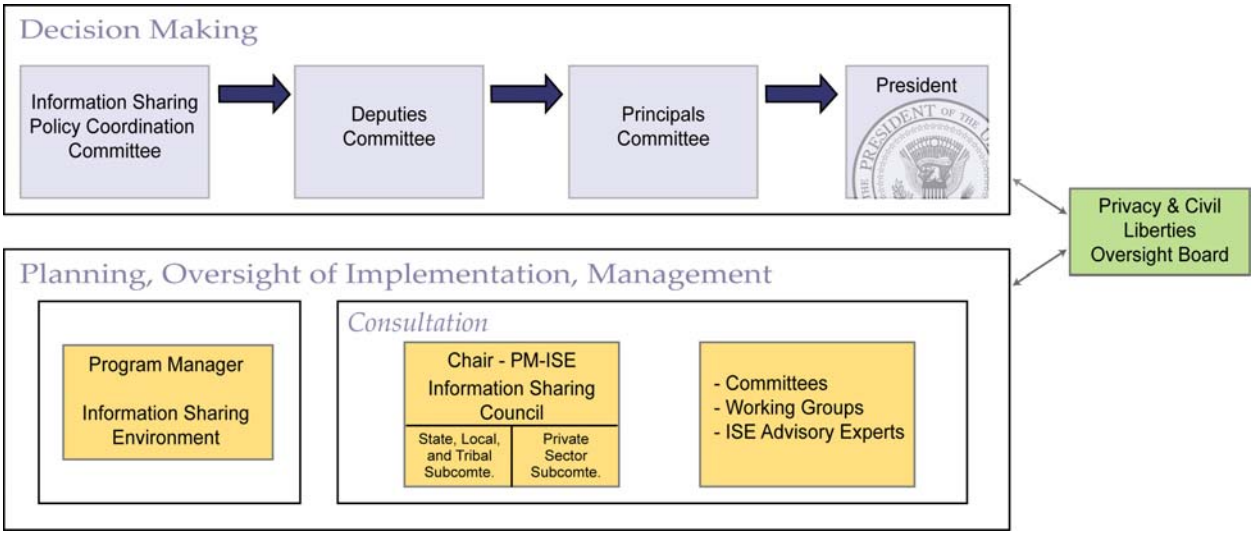


Figure 4.2-1. ISE Implementation Governance Roles and Responsibilities

4.2.2 The Program Manager

IRTPA requires that the PM-ISE, in consultation with the ISC, "assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency, and policy compliance; and regularly report the findings to Congress."[42] In carrying out these responsibilities, the PM-ISE leverages current information sharing efforts across the government, and engages ISC

[42] IRTPA, Section 1016(f)(2)(A)(iii).

departments and agencies through regular communication, interaction, and inclusion in ISE decision-making processes. In June 2005, the President placed the PM-ISE in the ODNI, assigning the DNI the responsibility to exercise "authority, direction, and control over the PM."[43] The PM-ISE acts as the central agent to improve terrorism information sharing among ISE participants by working with them to remove barriers, facilitate change, and ensure that ISE implementation proceeds efficiently and effectively. To oversee ISE implementation actions, the PM-ISE has staff from across government and the private sector with experience in counterterrorism, information sharing, technology, and policy.

4.2.3 The Information Sharing Council

IRTPA and E.O. 13388 established the ISC, which is chaired by the PM-ISE and composed exclusively of designees of: the Secretaries of State, Treasury, Defense, Commerce, Energy, and Homeland Security; the Attorney General; the DNI; the Director of the Central Intelligence Agency; the Director of the Office of Management and Budget (OMB); the Director of the FBI; the Director of the NCTC; and such other heads of Federal departments or agencies as the DNI may designate.[44] The ISC advises the President and PM-ISE on developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE. Additionally, it works to ensure coordination among the Federal departments and agencies participating in the ISE, and recommends means by which the ISE can be extended to allow interchange of information between the Federal government and appropriate SLT entities. A current list of ISC members is provided in Appendix 6.

4.2.4 ISC Subcommittees and Working Groups

The ISC may establish standing or *ad hoc* ISC subcommittees or working groups to address important issues requiring specialized expertise. In accordance with IRTPA, the ISC must consider input from persons and organizations outside the Federal government having significant experience and expertise in ISE-related matters.[45] Accordingly, two standing subcommittees—one to address SLT information sharing, and the other dealing with information sharing with the private sector—have been established under the ISC. DOJ and DHS serve as co-chairs of both subcommittees.[46] On April 27, 2006, the SLT subcommittee met to provide substantive input on how the Federal government can improve efforts to exchange terrorism information with SLT authorities. The results of this meeting helped shape the framework described in this plan for sharing with SLT governments. In addition, SLT officials have provided input on

[43] Presidential Memorandum, *Strengthening Information Sharing, Access, and Integration - Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment*, June 2, 2005.
[44] IRTPA, Section 1016(g) and E.O. 13388. *See* Appendix 4 for further detail.
[45] Ibid., Section 1016(g)(3).
[46] The subcommittees are composed of persons and entities outside the Federal government who provide the ISC with expert advice and guidance in accordance with Section 1016(g)(3) of IRTPA.

the framework for State and local support, standardization of SBU procedures, the implementation of EDS IOC, and the contents of this plan.

4.2.5 HSC and NSC Decision Process

In June 2005, the President formally established the Information Sharing Policy Coordination Committee (ISPCC), chaired jointly by the Homeland Security Council (HSC) and the NSC. The ISPCC is made up of representatives from Federal departments and agencies participating in the ISE and was established to address major information sharing policy issues, including resolving issues raised by the PM-ISE, and provide policy analysis and recommendations for decision by the Deputies or Principals of organizations represented on the HSC and NSC. The PM is a member of the ISPCC and participates in the HSC/NSC Deputies Committee on ISE issues.

4.2.6 Privacy and Civil Liberties Oversight Board

The Privacy and Civil Liberties Oversight Board (PCLOB) was established by IRTPA to ensure that an enhanced system of checks and balances is in place to protect individual privacy and civil liberties during the establishment and conduct of government efforts to protect the nation against terrorism.[47] The PCLOB's role is to provide advice to the President or to the head of any executive department or agency on the development and implementation of policies related to efforts to protect the nation from terrorism, including the ISE's development, adoption, and implementation.

[47] IRTPA, Section 1061(a)(2).

This page intentionally blank.

Chapter 5 – ISE Operational Capabilities

5.1 Introduction

This Chapter addresses key elements needed to enable the ISE's operational capabilities. Since other portions of this plan—in particular those sections describing the efforts-undertaken in response to the President's December 2005 Guidelines—discuss the ISE from operational and process perspectives, this chapter focuses on the technical side of ISE implementation. More specifically, this chapter focuses on information technology services needed to enable maximum information sharing. It warrants renewed emphasis that, although this chapter describes technical approaches for achieving these capabilities, ISE development will be driven not by technology but by current and future business processes that support terrorism information sharing, combined with required policies and procedures. Put differently, the ISE will not result in the construction of a single interconnected computer system touching all levels of government and containing all terrorism information, but the ISE will use technology to the maximum extent possible to enhance information sharing.

5.1.1 ISE Enabling Policy and Business Processes

In order for the future ISE to become truly operational, policies must enable and authorize both the business processes and underlying technical solutions. These policies will be formulated in Phase 1. Underlying ISE business processes will affect ISE participants in both supply-side activities, such as production, reporting, and content management, and consumer-side activities, such as collaborative, analytical, and investigative functions.

5.1.2 Overarching ISE Capabilities

The ISE has three high-level overarching capabilities, each of which includes a sub-set of operational capabilities. The overarching capabilities, and the operational capabilities associated with each, are:

1. The sharing environment and the associated business processes and policies currently in place. The ISE will be implemented in a manner that enables users, to the maximum extent possible, to access and exchange the information necessary to perform their counterterrorism responsibilities. This approach may include, for example, posting intelligence reports to a common site, searching for information on a particular individual or group, and exchanging viewpoints on the risk posed by a particular piece of information. This suite of common services will draw upon systems and processes already in place within the defense, homeland security, intelligence, foreign affairs, and law enforcement communities

2. The continuous process and capability for discovering and identifying essential data and services that should be added to the ISE. The discovery of new capabilities can be driven by evolving practices, tactics, techniques, and procedures within the counterterrorism communities or by introducing a new capability within Federal, SLT, or private sector organizations.
3. The policies, processes, and technical means for introducing new capabilities into the ISE.

5.1.3 Two-Phased Approach

Phase 1 activities focus on identifying existing or emerging technologies and programs that may be appropriate for ISE adoption. Pilot programs, such as the SBU Mobility Pilot for wireless access at the SBU level, will be closely monitored to identify policy, process, and technical lessons learned that could be applied to the ISE. Additionally, Phase 1 will identify standards and technical and process-oriented best practices that can be codified to support the ISE business processes, and will involve adopting mature technologies and capabilities for immediate insertion into the ISE. It will conclude with the adoption of underlying technologies and development of a detailed plan for implementation, including goals, measures, and targets. Phase 1 activities will include:

1. Identify and monitor pilots (e.g., SBU Mobility Pilot);
2. Identify policies, business processes, standards, architectures, and technologies associated with ISE capabilities;
3. Identify best practices and tools for sharing for inclusion in the initial and future implementation efforts;
4. Incrementally adopt technologies;
5. Develop goals and performance measures for specified outcomes; and
6. Develop a detailed plan of action.

The second phase will include adopting and integrating existing and emerging technologies identified in Phase 1. It will also include an incremental technology and capability review, comparing existing technologies and tools against the emerging needs of ISE users. Phase 2 activities will include:

1. Integrating technologies identified in the first phase;
2. Measuring for expected outcomes for improving Federal, SLT, and private sector counterterrorism operations; and
3. Incrementally enhancing ISE capabilities.

The ISE will result in certain common services being provided to users. The five communities will have to agree on those services as part of the ISE implementation. From an Information Technology (IT) perspective, the services may include: single sign-

on at computer terminals and across multiple computer applications; customized subscription to areas of interest; provision of trusted and dependable security features; tools to measure the operational success flowing from the sharing of particular information; and means to locate subject matter experts around the globe.

The following subsections address these services from a technical perspective. The subsections have been written to assist those persons within departments and agencies who are responsible for assisting ISE implementation from a systems and IT perspective.

5.2 Alerts and Notifications

The ISE will have the capability to allow participants to provide and receive relevant alerts and notifications. Standard counterterrorism-related alerts and notifications will be delivered to the user's desktop or mobile device through a subscription service that allows users to select from a list of available alerts (e.g., mission-area, role, or geographic responsibility).

5.2.1 Implementation Actions

During Phase 1 of ISE implementation:

Action 1.1 The PM-ISE and ISC members will identify the alerts and notifications to be available to Federal and non-Federal ISE participants and the enabling policies and business processes necessary to implement the alert and notification capability. (Planned Completion: First Quarter, Calendar Year (CY) 2007)

During Phase 2:

Action 2.1 The PM-ISE and ISC members will identify the subscription and delivery technologies required to deliver the alert and notification capability, and develop a detailed set of requirements and Project Plan for implementing alert and notification requirements. (Planned Completion: Third Quarter, CY 2007)

5.3 Easier User Access

ISE participants must have the ability to access terrorism information to support their business processes in an unobtrusive and intuitive manner. This includes accessing terrorism information using existing terminal devices, such as Web interfaces, mobile terminal devices, and end user applications that support their ongoing activities. As directed by IRTPA, the objective is to provide users with access to more than systems and networks, but to the actual data.

Additionally, a single ISE sign-on into the environment will grant users access to data and services based on their individual user/terminal device combinations. A single user may access terrorism information through multiple different terminal devices depending on the user's particular function, work environment, and mission. While the user may have full authorization to access data and services based on role and security clearances, the terminal device may not.

Easier user access can be achieved by implementing an access control method that recognizes the terminal device (and its accreditation) and using an identification, authentication, and authorization service to grant individual users access to data and services that they have been authorized to access. This method of role- and technology-based access is based on a trusted and standard method of defining, issuing, and storing user identities. A centralized repository of user identities will be used for the identification-authentication-authorization process, regardless of the method of access. The identity repository will be a core ISE service provided by EDS.

5.3.1 Access Control

5.3.1.1 Levels of Access by Role

The access control process must mediate access to resources (data and services) based on the user's role. Roles must be defined and maintained using a standard process that is dynamic and updated in a timely manner. Defined roles must be mapped to sets of resources that support the business processes associated with those roles.

5.3.1.2 Levels of Access by User Clearance and Accesses

As ISE participants will have varying levels of clearances and access, the access control process must mediate access to resources based on the clearances of the individual users. Clearance information will be stored as a component of the user identity to facilitate this mediation.

5.3.1.3 Levels of Access by Resource Classification

A standard process for describing the classification of individual resources (e.g., applications, data repositories, and transport resources) will be implemented to grant access of resources to those users with appropriate roles, clearances, and access devices.

5.3.2 Implementation Actions

During Phase 1 of ISE implementation:

Action 1.2 The PM-ISE and ISC members will identify existing technologies, capabilities, and programs (e.g., HSPD-12 and Federal Information

Processing Standard [FIPS] 201) that provide easier user access, but still support identity management through audits, authentication, and access controls. The ISC will assess the technologies and pilot programs to determine whether or not the technologies support its user base and are suitable for ISE adoption. (Planned Completion: Second Quarter, CY 2007)

Action 1.3 The PM-ISE and ISC members will determine what ISE-wide identity management capabilities are practical and develop a detailed set of requirements and Project Plan for implementation of such capabilities in a time frame consistent with technology maturity and available budgetary resources. (Planned Completion: Second Quarter, CY 2007)

5.4 Information Discovery and Search

This capability will allow ISE users to discover the information they need without having to know in advance that the particular information exists or having to know its location. This capability will be designed to support the needs of a diverse user base with varied computer skills to search and discover information across the ISE. Examples of these types of search capabilities include:

1. Searching for specific entities (people, places, or things);
2. Searching for records (e.g., intelligence reports);
3. Conducting multi-cultural name resolution;
4. "Drilling-down" through other related data;
5. Using personally identifiable information (e.g., fingerprints, photographs, biometrics, etc.) to discover the actual identity of suspects using multiple identities;
6. Searching for queries previously performed by other users;
7. Conducting basic and advanced searches;
8. Supporting processing based on business rules (e.g., filtering, scoring, ranking of results); and
9. Returning output from automated correlation and relationship services.

5.4.1 Enterprise Search

Enterprise search refers to the act of searching structured and unstructured content from throughout the enterprise to discover data, information, and knowledge wherever it exists. The enabling technologies are search engines, metadata standards, and network-accessible repositories. The ultimate goal is achieving a measurable level of "findability," where the user searches all relevant data stores and receives the data he

or she seeks. Query results should also indicate when information is available, but the user or network does not have the required access privileges, consistent with appropriate protection of sensitive information. In such cases, contact information should be provided so the user can contact the data steward for potential release. The enterprise search capability will be a decentralized, distributed, and federated process that minimizes central repositories of data or metadata.

5.4.2 Implementation Actions

During Phase 1 of ISE implementation:

Action 1.4 The PM-ISE and ISC members will investigate existing or emerging capabilities that discover data and information within the Federal government and industry. The initial implementation of enterprise search will apply a search engine to index both structured and unstructured data. This activity will include the evaluation of several ongoing pilot programs using technologies that integrate data across heterogeneous networks and data stores to enhance the "findability" of relevant information and the interoperability of data and information. (Planned Completion: Second Quarter, CY 2007)

During Phase 2:

Action 2.2 The PM-ISE and ISC members will develop a detailed project plan for implementing the enterprise search technologies selected in Phase 1. (Planned Completion: Third Quarter, CY 2007)

5.5 Security

5.5.1 ISE Security Requirements

Access and security are integral to many of the capabilities delineated in this Chapter. In such an environment, all ISE participants expect that information they provide will be protected and used appropriately, that information they access will be valid and accurate, and that ISE users will be vetted and authenticated. Access and security must accommodate two types of information. The first is information the Federal government produces and over which it maintains originator control. The second is information that flows to the Federal government for which it becomes the custodian, although others may govern the information's distribution and use (e.g., State and local proprietary information provided by the private sector, foreign information provided by foreign partners). Requirements for addressing access to and security of such information include:

1. Adopting policies, standards, architectures, and practices for IT security and trusted access control, including a common framework of IT security risk management processes across all security domains;
2. Adopting a standardized reciprocal security clearance and visitor request system in the Federal government to eliminate delays in passing clearances;
3. Revising the use of originator controls on terrorism information to promote a culture of information sharing;
4. Standardizing and creating interoperable identity management and access management systems, thereby reducing the number of separate computers, accounts, and logons required to access terrorism information across systems, domains, and networks; and
5. Creating a standards-based universally accessible repository of access authorization information that is current, complete, valid, and sufficient to explicitly associate individuals and terminals with their respective discrete access privileges.

In general, the discussion in this Section focuses on two attributes for the ISE required by IRTPA. First, to the greatest extent practicable, the ISE must employ an information access management approach that controls access to data in addition to systems and networks, without diminishing security.[48] Second, to the greatest extent practicable, the ISE must facilitate the sharing of information at and across all levels of security.[49]

5.5.2 Common IT Security Framework

The actions specified in this Section are designed to ensure that ISE security addresses the following IRTPA requirements:

1. Transitioning the ISE from a system- or application-centric model to one that is data-centric. In terms of security, this means that terrorism information will eventually be tagged with security-relevant metadata (e.g., XML markings) that provide confidence that access control decisions are consistent with overall security policy and each ISE user's access privileges.[50]
2. Ensuring that ISE security features operate effectively in all three security domains—SCI, Secret, and SBU (see Chapter 3)—and that streamlined approaches for exchanging information across domains are developed and deployed. Clearly information at the higher levels may require more stringent controls. Wherever possible, however, ISE IT security techniques and practices should operate uniformly across the three domains and be usable by organizations at all levels of government. The ISE must have a common

[48] IRTPA, Section 1016(b)(2)(E).

[49] IRTPA, Section 1016(b)(2)(F).

[50] See the discussion on ISE common standards in Chapter 6.

> Federal IT security and risk management framework—potentially extensible to the State and local levels—that can protect information wherever it is collected, processed, stored, or disseminated.

Traditionally, Federal IT security policy has mandated separate standards and processes for protecting national security systems that are different from those for protecting other Federal government IT systems. A "national security system" is defined as:

> Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—
>
> (i) the function, operation, or use of which—
>
> (I) involves intelligence activities;
>
> (II) involves cryptologic activities related to national security;
>
> (III) involves command and control of military forces;
>
> (IV) involves equipment that is an integral part of a weapon or weapons system; or
>
> (V) … is critical to the direct fulfillment of military or intelligence missions [but does not include a system that is to be used for routine administrative and business applications]; or
>
> (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.[51]

The law requires, however, that "to the maximum extent feasible… standards and guidelines [for other Federal systems] are complementary with standards and guidelines developed for national security systems."[52] The sharp distinction between national security systems and other Federal systems was a reasonable approach when separate intelligence and military systems were easy to define and clearly distinct from other systems. In the context of the ISE, however, this line is blurred. Expanded use of tear-lines means that the same information will exist in multiple forms in different parts of the ISE. Employing different security guidelines and standards to protect this information becomes increasingly difficult and costly.

It is not uncommon for single departmental or agency security teams to support both national security and non-national security systems. In so doing, they may employ multiple sets of security policies, procedures, standards, and guidelines that generate

[51] 44 U.S.C. Section 3542(b)(2).
[52] 44 U.S.C. Section 3543(a)(3).

implementation complexity, impose higher costs, and result in inconsistent and incompatible levels of protection. This problem also exists across Federal departments and agencies because different criteria are used to develop security policy and certify and accredit systems. These criteria must be better aligned across security domains and communities of interest.

Although certain aspects of IT security, such as cryptographic standards, will always be more stringent for national security systems, most of the fundamental access control policies can operate across all security domains. The increasingly important concept of role-based access controls, for example, can be implemented identically on both national security and non-national security systems.

The ISE must adopt a unified risk management and IT security framework that serves all five of its communities. The framework should have the following characteristics:

1. A risk management approach that aims to achieve appropriate levels of security. This approach must recognize that unauthorized disclosure of terrorism information is a risk to be managed rather than one that can be avoided. This applies to both technical and human-oriented risk management;
2. A data-centric approach, as required by IRTPA;
3. Common security controls, including standards for access control and audits that can be adopted by and be made available to all Federal ISE participants where appropriate. Although these standards should recognize that the three domains might have different requirements in some cases, the intent—consistent with direction in the Federal Information Security management Act (FISMA)—is to apply compatible standards and guidelines for national security systems and non-national security systems where possible.[53] These controls will be identified during the development of the IT common security framework.
4. Common standards flexible enough to support the diversity of missions and security needs. They must be sufficiently rigorous and robust to meet all needs, allowing for unique security requirements within the standard framework;
5. Common streamlined processes for certification and accreditation of IT systems, including full reciprocity of certification and accreditation (C&A) determinations among ISE participants; and
6. Common human- and computer-readable security markings that conform to ISE common standards (see Chapter 6).

[53] Ibid.

5.5.3 Cross-Domain Solutions

The overarching requirement in order to generate terrorism information at the lowest possible security level—unclassified, wherever possible—is the ability to securely exchange information across security domain boundaries. Trusted, two-way cross-domain solutions (CDS) play an integral role in meeting this need. CDSs are available today, but existing approaches have failed to keep pace with growing requirements and changing technology. Based largely on searches of textual information, these solutions do not typically support a robust exchange of graphic or multimedia information, and almost always require human review as part of the high-low transfer process. These approaches must be improved to meet ISE needs.

In March 2006, the Chief Information Officers (CIOs) of the IC and DoD established a DoD/IC Cross Domain Management Office (CDMO) to ensure that CDSs are available to meet IC and DoD needs at acceptable levels of cost, schedule, and risk. While this is a promising initiative, it must be expanded beyond DoD and IC to fully encompass the needs of all ISE participants.

5.5.4 Implementation Actions

During Phase 1 of ISE implementation:

Action 1.5 The PM-ISE and the ISC will work with the CDMO to establish a process to ensure that cross-domain solutions developed through this office meet the needs of ISE participants. (Planned Completion: First Quarter, CY 2007)

During Phase 2 of ISE implementation:

Action 2.3 The DNI CIO and the CIOs of DoD, DHS, DOJ, and the Department of State (DOS) will work with the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the Committee on National Security Systems (CNSS) to develop a common IT security framework for the ISE as described in Section 5.5.2. DOJ and DHS will ensure that this framework addresses the requirements of SLT CIOs. The results of this effort will be presented to the PM-ISE and ISC for incorporation into ISE implementation priorities. (Planned Completion: The PM-ISE and ISC members will develop a detailed project plan for implementing the technologies selected in Phase 1. (Planned Completion: Third Quarter, CY 2007)

Action 2.4 Federal departments and agencies will implement the common IT security framework developed in Phase 2 across the ISE. (Planned Completion: Third Quarter, CY 2008)

Action 2.5 Federal departments and agencies will deploy CDSs developed by the CDMO across the ISE to provide two-way cross-domain transfers of terrorism information with minimal human review. (Planned Completion: Third Quarter, CY 2008)

5.6 Collaboration

The ISE will also provide a secure mechanism to allow participants to share multimedia data and information. Additionally, ISE users will be able to find communities of interest through searches or ISE recommendations based on user activities and behaviors. Collaborative environments can be either enduring, such as the ongoing sharing of information on a particular target or target methodology, or *ad hoc*, such as mission planning, investigation, or course-of-action development. The ISE's collaboration requirements include:

1. Enabling the broadest collaborative efforts by making collaboration tools accessible to all ISE users;
2. Providing a mechanism and process for the user to easily create a community of interest;
3. Delivering capabilities for a user to publish multimedia information to a community of interest;
4. Providing capabilities for a user to retrieve multimedia information from a community of interest;
5. Providing a mechanism for a user to search for and find a relevant community of interest;
6. Employing a cross-domain chat capability; and
7. Creating a common workspace application.

5.6.1 Implementation Actions

During Phase 1 of ISE implementation:

Action 1.6 The PM-ISE and ISC members will identify existing collaborative tools that are used and operational in the counterterrorism or other analytic or investigative communities and review the feasibility of adopting common tools for use across the ISE. (Planned Completion: First Quarter, CY 2007)

Action 1.7 The PM-ISE and ISC members will develop requirements to implement new and emerging collaborative technologies. (Planned Completion: Second Quarter, CY 2007)

5.7 Electronic Directory Services

IRTPA required the ISE, to the greatest extent practicable, to provide "directory services, or the functional equivalent, for locating people and information."[54] The first ISE service deployed to meet this requirement was the EDS, a collection of directories that enable ISE users to search for and locate people, organizations, data, and services related to the counterterrorism mission. It is envisioned that SLT information will be available to users, but it is currently undefined how data will be made available or if it will be centrally stored and accessed. Implicit in EDS is support for various business processes such as communication and collaboration. The major directory services to be delivered and enhanced are blue, yellow, green, and white pages.

5.7.1 Blue Pages

EDS Blue Pages provide contact information for counterterrorism-related watch centers, sorted by organizational hierarchy. They are similar to a telephone book's "Blue Pages" listing. Blue Pages are generally available to anyone who has access to the SCI and Secret security domains. However, some filtering of Secret network users and enclaves may be conducted to limit what organizational hierarchy and contact information is made available to certain users.

5.7.2 Yellow Pages

EDS Yellow Pages are an expanded set of Blue Page organizational contacts that are further enhanced by attaching attributes that describe organizational roles, responsibilities, and expertise. A user can search the attributes to provide a customized list of counterterrorism-related organizations and associated contact information. Not all users will be able to view or search all organization attributes. In addition, similar to the Blue Pages, some filtering of Secret network users may be conducted.

5.7.3 Green Pages

EDS Green Pages provide a searchable listing of counterterrorism-related information sharing resources, systems, and data repositories to support users searching for specific data and capabilities. The Green Pages provide system descriptions and technical and operational contact information for gaining access. EDS Green Pages will also support the provisioning of common services by including technical descriptions that will facilitate using web services or other technologies to add systems to the ISE.

[54] IRTPA, Section 1016(b)(2)(G).

5.7.4 White Pages

EDS White Pages provide names and at least one method of contact for named personnel. Additional contact information may include phone numbers, email addresses, and postal addresses. For urgent needs, an alternate 24/7 method of contact may be included. An ISE user can locate contact information for an individual by entering a first and last name. When ISE users want to contact individuals with particular roles, responsibilities, or expertise, they will use the Yellow Pages search capability to identify an organization or office that has individuals with the desired capabilities. A White Pages-like directory will also support ISE-wide identity management, authentication, and authorization services that will provide multi-level access capability for different classes of ISE users as described in Section 5.3. This access control and identity management capability may be independent from the EDS White Pages, based upon further investigation.

5.7.5 Implementation Actions

During Phase 1 of ISE implementation:

Action 1.8 The PM-ISE and the ISC members will implement EDS Blue, Yellow, and Green Pages in the SCI, Secret, and SBU security domains. (Planned Completion: Second Quarter, CY 2007)

Action 1.9 The PM-ISE and the ISC members will implement EDS White Pages in the SCI and Secret security domains. (Planned Completion: Second Quarter, CY 2007)

During Phase 2 of ISE implementation:

Action 2.6 For Sections 5.2, 5.3, 5.4, 5.6, and 5.7, the PM-ISE and ISC will review the status in all areas and reassess Phase 2 Actions. (Planned Completion: Ongoing with a first progress check to occur by First Quarter, CY 2008)

This page intentionally blank.

Chapter 6 – Architecture and Standards

6.1 Introduction

A fully functional future ISE requires the construction, integration, and maintenance of information resource infrastructures across Federal departments and agencies, SLT governments, the private sector, and foreign partners. Information resources are information and related resources, such as personnel, equipment, funds, and IT.[55] To plan for and manage information resources, the Federal government currently uses strategic management tools, including EAs. The U.S. House Committee on Government Reform, in defining EAs, stated, "Successful public and private-sector organizations have used such architectures as best practices for effective business and technology transformation."[56] Similarly the Government Accountability Office maintains, "An enterprise architecture provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., a Federal department) or a functional or mission area that cuts across more than one organization."[57] Planning, integration, and implementation activities affecting information resources, both internal and external to organizations, are also effectively conducted through well defined, conforming processes using common standards. OMB *Circular A-130* states that agencies must use or create an EA Framework, and they are expected to adopt and enforce standards to support the entire EA.[58]

A business process-driven ISE Enterprise Architecture (ISEEA) Framework, including an FEA Profile, and a functional standards development approach are being used to implement the ISE across Federal information resources, consistent with OMB FEA Framework guidelines. Furthermore, this approach defines the connection for information resources of SLT governments, the private sector, and foreign partners, and leverages and integrates the diverse landscape of existing policies and management processes across the Federal government. This approach coordinates activities with agency CIOs who are responsible for ensuring agency compliance with, and the prompt, efficient, and effective implementation of, information policies and the management of information resources within their respective agencies.[59] This approach also recognizes that national security systems, physically and managerially isolated from the majority of civil systems in these agencies, provide support to intelligence and military operations. Current legislation affecting Federal information resources and information security acknowledges the "unique needs" and "longstanding statutory

[55] 44 U.S.C. 3502(6).
[56] U.S. House Committee on Government Reform, *Report 107-787: E-Government Act of 2002* (U.S. Government Printing Office: Washington, DC, 2002), p. 48.
[57] U.S. Government Accountability Office, *Report GAO-06-219* (U.S. Government Printing Office: Washington, DC, 2005), 7
[58] Office of Management and Budget, *Circular A-130* (OMB: Washington, DC, 2000), p. 15-16.
[59] 44 U.S.C. 3506(a)(3).

treatment of military and intelligence mission-related systems and classified systems."[60] As such, the DNI CIO has a responsibility to manage activities relating to the IT infrastructure and EA requirements of the IC; the DoD CIO has a responsibility to manage IT and national security systems supporting the activities of the U.S. Military; and the Secretary of Homeland Security has the responsibility to oversee management of the National Communications System (NCS), those national security and private sector infrastructures supporting national security and emergency preparedness (NS/EP) telecommunications.[61]

A challenge to building an integrated, functional ISE is the diversity and distinct separation of information resources and policies affecting Federal and SLT agencies, the private sector, and foreign partners. Implementation of the ISE will be driven by the needs and missions of all participants, and technology will be used to enhance ISE operations. To be effective, the ISE must cross diverse domains and supporting infrastructures, including private sector, civil, and national security systems.

To begin to address this transformational challenge within Phases 1 and 2 and to recognize existing authorities as required by Section 1016 of IRTPA, programmatic processes, and best practices, the PM-ISE is developing, with the ISC, a business process-driven, cross-agency EA Framework Document (ISEEA Framework). This approach will include, within the ISEEA Framework, a description of the structure of the ISE's associated business processes, information flows and relationships, services, and high-level data packet descriptions and exchange relationships. The ISEEA Framework will provide guidance at a level of detail greater than that provided by the FEA Framework, but will not drive down into the operational level, which is the level appropriate for individual departments and agencies to include in their EAs as they implement the ISE.

In addition to an ISEEA Framework, an FEA-ISE Profile will be developed that describes how department and agency participants use their EAs to connect to the ISE. The ISEEA Framework and FEA-ISE Profile will be communicated to departments and agencies through OMB's Federal Transition Framework (FTF) process. Maximum use of existing EA processes is an essential element of ISE implementation. While policy may not exist to address all necessary processes to provide connection points for individual SLT governments, the private sector, and foreign partners, the artifacts created by this approach can serve as guidelines on how their critical resources also interoperate with and within the ISE.

[60] U.S. House Committee on Government Reform, Ibid., p. 77; National Security Act of 1947, as amended, 50 U.S.C. 403-3g(c)(1); 10 U.S.C. 2223(a).

[61] *Executive Order 12472* (April 3, 1984), Section 1, as amended by *Executive Order 13286* (February 28, 2003), Section 46.

6.2 ISE Enterprise Architecture Framework and Profile

6.2.1 IRTPA and Presidential Memorandum Requirements

IRTPA directs the ISE Implementation Plan to provide a description of the functions, capabilities, resources, and conceptual design of the ISE. IRTPA further requires a description of how the ISE impacts the EAs of participating agencies.[62] Similarly, the December 2005 Presidential Memorandum directs that the ISE be built on existing Federal government resources that include standards, systems, and architectures.[63] Together the ISEEA Framework and its associated FEA-ISE Profile, driven by business processes derived from ISE operational concepts, describe and map ISE business processes and technology into Federal information resources, and identify the connection points for information resources of SLT governments, the private sector, and foreign partners. The pages that follow describe the ISEEA Framework process and impacts of this approach, through the FEA-ISE Profile, on ISE participant EAs.

6.2.2 Presidential Memorandum Observations and Recommendations

In response to IRTPA and the direction in the December 2005 Presidential Memorandum to evaluate existing information sharing resources (IIP Task 1.1), the PM-ISE reviewed existing information sharing resources and observed that though robust national systems exist for sharing information of varying security classification levels, they are not interoperable within and between classification levels. The PM-ISE reviewed a wide range of architecture initiatives related to information sharing, including the DoD Global Information Grid (GIG), the Department of Energy Corporate Systems Information Architecture and Office of Intelligence Architecture Initiatives, the FBI EA, the Intra-DOJ Information Exchange Architecture, and the DOS Technical Infrastructure Architecture. The review observed that Federal departments and agencies have made solid progress in developing EAs according to the FEA, the business-driven framework for the Federal government. However, it was difficult to judge whether this progress was developmental in nature or was actually functional. Additionally, it was unclear whether departments and agencies were focusing business process reengineering efforts on cross-organizational terrorism information sharing.

To begin to address these issues, the PM-ISE recommended using an EA development checklist, consistent with the Federal Enterprise Architecture's Assessment tool, as an objective evaluation tool to assess whether agency EAs were compatible with information sharing objectives. To address information security, it was recommended cross-domain solutions, supporting multiple security classification levels, should extend to the broader information sharing community.

---

[62] IRTPA, Section 1016(e)(1)-(2).

[63] *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements In Support of the Information Sharing Environment* (White House: Washington, DC, 2005), Section 1.

6.2.3 ISEEA Framework

An ISEEA Framework based on the FEA Framework and aligned to ISE requirements is shown in Figure 6.2-1 below. The ISEEA Framework consists of an Architect's View with four partitions (Business, Data, Applications and Services, and Technical), which are mapped to the five FEA Reference Models (Business, Performance, Data, Service Component, and Technical). While Figure 6.2-1 shows the relationship of the ISEEA Framework to the FEA through the Architect's View, it also provides further detail in the Implementer's View on the seven business process-driven architectural models of the ISEEA. The Implementer's View contains mappings to implementation processes to aid departments and agencies with ISE-related information resource investment planning and implementations. Both the Architect's View and Implementer's View are discussed in detail below. As part of the ISE development process, the PM-ISE will continue to develop, define, and refine the Architect's and Implementer's Views of this ISEEA Framework through the ISEEA Working Group (ISEEAWG), comprised of EA representatives from ISC organizations.

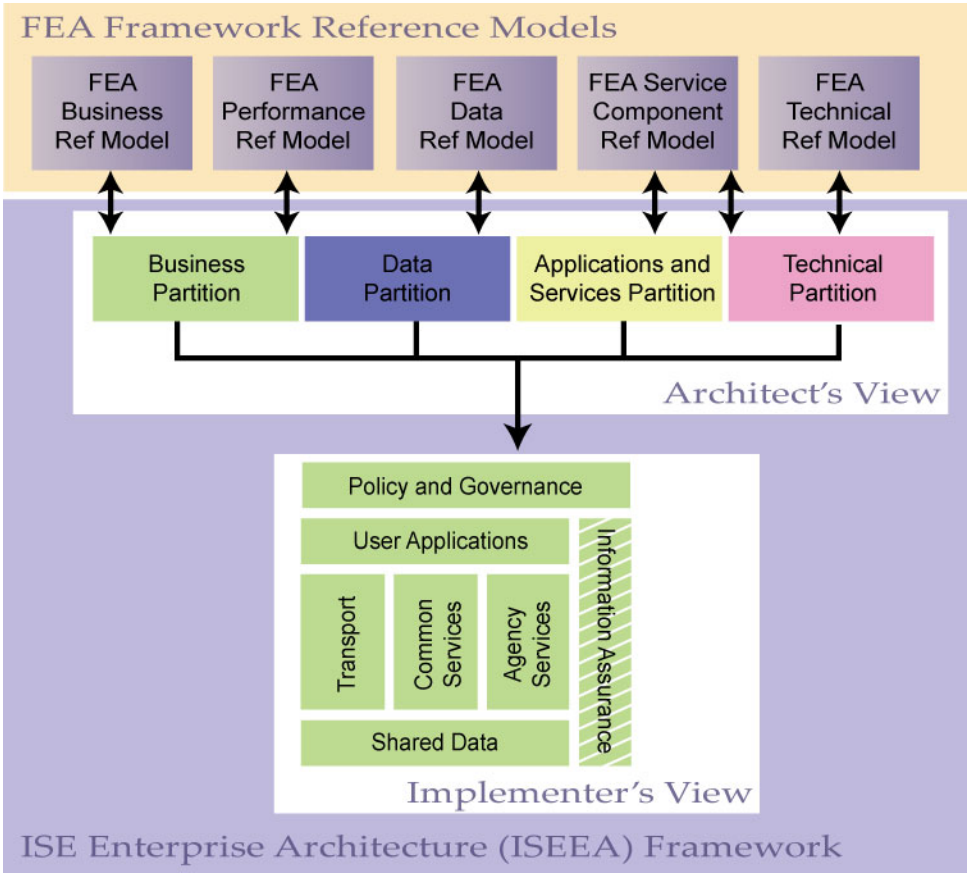


Figure 6.2-1. ISE Enterprise Architecture (ISEEA) Framework and FEA Mapping

The Architect's View of the ISEEA Framework consists of four partitions.

1. The *Business Partition* presents the business activities and processes supporting the ISE mission. These descriptions are at a level that connects the high-level FEA Framework to the detailed business process provided in department and agency EAs.
2. The *Data Partition* defines high-level descriptions and categories of data that will be shared in the ISE. Agency and department EAs will provide the detailed data descriptions through their EAs.
3. The *Applications and Services Partition* describes the high-level applications and common services that support the ISE business processes.
4. The *Technical Partition* characterizes hardware, operating systems, programming, and network solutions used across the ISE. This view will not specify solution requirements for the ISE participants, but will be an artifact driven by the departments and agencies in the implementation of the ISE.

These four partitions are mapped to the five FEA Reference Models to enable tracking of the development of the ISEEA Framework across agencies using existing OMB policies and processes regarding department and agency EAs and budgetary processes.

While the FEA provides the necessary mapping of the ISEEA Framework into Federal civil systems, the ISEEA Framework, as a subset of the FEA Framework, will also provide an architectural mapping into national security systems. The ISEEA Framework will integrate with the Intelligence Community Enterprise Architecture (ICEA), the Department of Defense Enterprise Architecture (DODEA), and the NCS Committee of Principals (COP) Continuity Communications Enterprise Architecture (CCEA), which will integrate the terrorism information sharing capabilities from these architectures into the overall ISE. New policies, as needed, should clarify that the ISEEA Framework and FEA-ISE Profile will be promulgated uniformly to all Federal information sharing resources through EA and information resource lifecycle processes. This should include appropriate protections of information including sources and methods uniquely associated with these national security systems.

SLT government EAs are anticipated to integrate with the ISEEA Framework through architecture policy and development processes established with the fusion centers (see Section 3.4). As such, the PM-ISE suggests that existing SLT EAs begin incorporating the ISEEA Framework and the FEA Framework to improve and speed connection of these architectures into the ISE.

As shown in Figure 6.2-1, the Implementer's View of the ISEEA Framework is composed of seven architectural models for the ISE shared environment.

1. The *Policy and Governance Model* provides the means for implementing and promulgating the necessary ISE issuances and standards for establishing and transforming the ISE.
2. The *Agency Services Model* includes those services specific to a given agency that provides external access to internal agency data and capabilities.
3. The *Common Services Model* includes those services that by their nature must be common across agencies (e.g., search, warning notification, and security) or that are provided to reduce unnecessary duplication of effort (e.g., data translation).
4. The *Transport Model* documents the hardware, software, and transport media that provide the path for the transmission and reception of data.
5. The *Shared Data Model* provides a controlled vocabulary and exchange structure for the information to be shared.
6. The *User Applications Model* includes applications, developed by a department or agency, to provide counterterrorism business process needs capability using the ISE with access to required information and services provided external to that agency.
7. *Information Assurance,* consistent with attributes in the FEA Security and Privacy Profile, provides the means for managing those standards and designs that allow access to information by authenticated users while assuring the integrity, availability, and privacy of that information, and protecting sources and methods of collection.

Collectively, these models, all taken together, provide the building blocks for the development of capabilities and configurations that meet the requirements and vision of the ISE. Overall the ISEEA Framework, defined in concert with the FEA Framework, the ICEA, the DODEA, and the CCEA, establish a broad architecture to support an inter-connected, nationwide, and international ISE capability.

6.2.4 FEA-ISE Profile

As Figure 6.2-2 shows, the ISEEA artifacts include the ISEEA Framework Document and the FEA-ISE Profile (modeled after other existing FEA Profiles). The FEA-ISE Profile is a framework that cuts across the interrelated FEA reference models providing guidance to Federal departments and agencies for use in implementing the ISE. Departments and agencies will incorporate ISE capability needs into their EAs and subsequently develop or enhance department or agency systems to deliver ISE capabilities. Access to ISE participant data will be provided via methods such as the provisioning of data into the ISE shared space or, as appropriate, access to department or agency systems and data repositories. ISEEA Core components will be assigned to specific department or agencies to implement and make available to all ISE participants.

Specifically, the implementing agencies will develop detailed specifications for these components and implement them based on the ISEEA Framework and the FEA-ISE Profile.

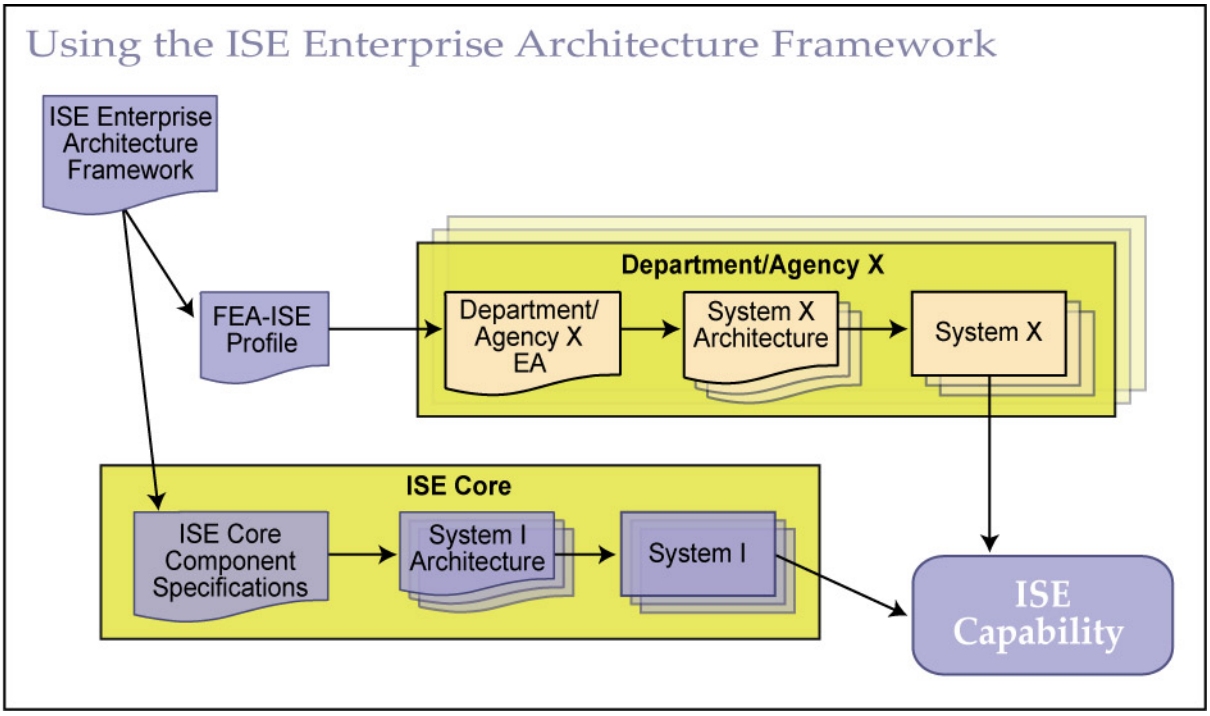


Figure 6.2-2. ISEEA Framework Documentation Package

6.2.5 Implementation Actions

As previously described, the ISEEA Framework and FEA-ISE Profile will provide the ability for the PM-ISE, in conjunction with the ISC, to advise on implementing elements of department and agency EAs in a manner that achieves the overall goal of terrorism information sharing. This guidance will leverage existing EA processes and documentation to enable cross-agency information sharing.

6.2.5.1 Phase 1 Actions

During Phase 1 of ISE implementation:

Action 1.10 The PM-ISE, in consultation with the ISC, will publish a preliminary version of the ISEEA Framework Document providing the models with major portions of the ISE and their attributes. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.11 OMB, in the FEA Business Reference Model (BRM), will include "Information Sharing" as a new government sub-function, BRM code 143, with the "Information and Technology Management" Line

of Business, BRM code 404. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.12 The PM-ISE will work with NSA, NIST, the DNI/CIO, and the CNSS on incorporating network security and information assurance policies and practices for the ISEEA Framework and associated functional standards. (Planned Completion: First Quarter, CY 2007)

Action 1.13 The PM-ISE, in consultation with the ISC, will publish a fully documented ISEEA Framework Document and an FEA-ISE Profile. The development process will be worked in collaboration with the OMB, department and agency CIOs, and ISC members. (Planned Completion: First Quarter, CY 2007)

Action 1.14 The PM-ISE, in consultation with the ISC, will develop a configuration management process for the control and management of updates to the ISEEA Framework Document and FEA-ISE Profile. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.15 OMB, in the FEA Reference Models, will add the ISEEA Framework and the FEA-ISE Profile as compliance requirements in the *Federal Transition Framework*, a catalog of cross-agency initiatives, and the *FEA Program: Enterprise Architecture Assessment Framework*, the maturity assessment guide for Federal EAs. (Planned Completion: First Quarter, CY 2007)

Action 1.16 DHS will work with the PM-ISE to review existing policies and procedures for ascertaining relevant and effective approaches to migrate the ISEEA Framework models and attributes into the private sector. (Planned Completion: Second Quarter, CY 2007)

6.2.5.2 Phase 2 Actions

During Phase 2 of ISE implementation:

Action 2.7 Departments and agencies will introduce the ISEEA Framework and the FEA-ISE Profile into their EA planning affecting investments beginning execution in FY 2008. Agencies that have been identified to provide ISE Core services and transport components will include these into their planning. The DNI CIO and the DoD CIO will introduce the ISEEA Framework and FEA-ISE Profile elements into their EAs affecting national security investments beginning execution in FY 2008. Agencies will also incorporate ISEEA Framework attributes in their information resource lifecycle processes, to include capital planning and investment control (CPIC) processes. The Common Terrorism Information Sharing Standards (discussed in section 6.3) will provide the source of functional standards for information sharing in

the FEA's Technical and Data Reference Models. (Planned Completion: Fourth Quarter, CY 2007)

Action 2.8 The PM-ISE, working with the NCS Manager, will coordinate and monitor the incorporation of the ISEEA Framework and the FEA-ISE Profile into the NCS and the CCEA planning affecting investments beginning execution in FY 2008. (Planned Completion: Fourth Quarter, CY 2007)

Action 2.9 OMB will publish a new version of the Federal Transition Framework and the FEA Program: EA Assessment Framework incorporating the ISEEA Framework and the FEA-ISE Profile. (Planned Completion: Fourth Quarter, CY 2007)

Action 2.10 OMB will conduct FY 2009 EA reviews, including those affecting national security systems, and ensure these reviews demonstrate incorporation of the ISEEA Framework and the FEA-ISE Profile across Federal agencies. (Planned Completion: Second Quarter, CY 2008)

Action 2.11 The PM-ISE will work with DHS to promote, coordinate, and distribute the ISEEA Framework for incorporation by the private sector into new technology and products supporting terrorism information sharing. Consistent with the National Infrastructure Protection Plan, these efforts will incorporate requirements and actions specified in Sector-Specific Plans. (Planned Completion: Third Quarter, CY 2008)

Action 2.12 The PM-ISE will work with DOJ, DHS, and other Federal agencies to coordinate and implement the ISEEA Framework and FEA-ISE Profile elements into the fusion centers initially as translation infrastructures to SLT governments. As SLT government infrastructures transform to integrate more directly with the ISEEA Framework, the requirement for continuing to operate and maintain translation infrastructures will be reduced. (Planned Completion: Fourth Quarter, CY 2008)

6.3 ISE Standards

6.3.1 Review of Presidential Guideline 1 Developments

The Presidential Information Sharing Guidelines and Requirements direct that the ISE will be built upon existing Federal government resources and be based on common standards.[64] Specifically, Presidential Guideline 1 directs the DNI, in coordination with the Secretaries of State, Defense, Homeland Security, and the Attorney General, to

[64] *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements In Support of the Information Sharing Environment* (2005), Section 1.

develop and issue common standards for addressing how terrorism information will be acquired, accessed, shared, and used within the ISE. These standards must maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. This must also be consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities.[65] In response to this direction, the PM-ISE has developed a construct for developing and releasing ISE standards and has identified initial ISE standards addressing two priority functional information sharing business processes. This construct is presented in *Common Terrorism Information Sharing Standards (CTISS)*, *Version 1.0*, which defines processes, standards bodies, and implementation strategies for improving the standardization of information sharing products and activity in the ISE.

6.3.2 Background of IIP Task 1.1 Findings and Observations

In response to IRTPA, Section 1016(e) and the Presidential Memorandum, the Office of the PM-ISE produced the *ISE* IIP to serve as a roadmap for developing the comprehensive implementation plan for the ISE. Task 1.1 of the IIP required a compilation of existing resources within the Federal government, including standards. The PM-ISE observed that strong standards initiatives across the entire ISE community do not exist, and activities to create usable standards will still be multi-year efforts. Furthermore, the PM-ISE noted that uniform Internet web browser standards do not exist, and common information protection standards are not used across the community. With regard to implementation, the PM-ISE observed that there has been little consensus to date regarding the selection of standards and monitoring of their adoption. The IIP tasked the DNI, in coordination with the Secretaries of State, Defense, Homeland Security, and the Attorney General, to develop and issue government-wide common standards. These standards should promote the maximum distribution of and access to terrorism information, while safeguarding such information and protecting sources and methods, and should specify methods for government-wide adoption and implementation of these standards.[66]

Standards have an important role in ensuring consistency of business process and infrastructure development, and they are key decision-making factors when considering future architectures and investments. Standards provide the critical functional and technical bridge between disparate information sources and those related communities of interest responsible for carrying out the counterterrorism mission. While Federal law promotes the use of voluntary consensus standards, terrorism information sharing business process requirements present new and unique challenges that may require a combination of both government-developed standards and voluntary consensus standards.[67] For the ISE, the *functional standards* defined under the following CTISS process document the unique rules, conditions, guidelines and characteristics of

[65] Ibid., Section 2.
[66] Office of the PM-ISE, *The Information Sharing Environment Interim Implementation Plan,* Ibid., Section 3.5.
[67] 15 U.S.C. 272.

business processes, production methods, and actual products supporting terrorism information sharing. These functional standards apply to ISE participants and their infrastructures that will interconnect into the ISE.

6.3.3 Progress to Date

In April of 2006, the PM-ISE established a working group, comprised of standards experts from ISC departments and agencies, to define common standards that support how terrorism information is acquired, accessed, shared, and used. A product of this working group, the *Common Terrorism Information Sharing Standards (CTISS), Version 1.0*, provides the framework for developing and implementing business process-driven ISE functional standards for use universally across all levels of government, the private sector, and foreign partners. These standards also support the domains of intelligence, law enforcement, homeland security, foreign affairs, and defense.

As shown in Figure 6.3-1, the CTISS Framework provides traceability from the domains of terrorism information and information security, through applicable operating concepts and architecture models, down to ISE functional standards for publishing. As shown in the figure, the Framework provides a relational mapping of standards categories, governing standards bodies, and core standards for use across the community. This Framework follows five strategic goals for the CTISS program:

1. Establish a self-governing standards adoption process;
2. Engage foreign and private sector partners;
3. Ensure the process is compliant with statutes, executive orders, and ISE policies;
4. Leverage published commercial standards when appropriate and available; and
5. Define standards that are performance-driven.

The highest level of the Framework identifies the terrorism information domains, or interest areas, for sharing across all levels of government, the private sector, and foreign partners: *intelligence, law enforcement, homeland security, foreign affairs, and defense*. Security domains span the Framework and address security classification designations for information sharing. The standards categories (*Metadata, Data, Exchange Protocols, and Services*) provide key differentiations for existing or newly developed standards. The Metadata standards category describes those standards providing the searchable *characteristics* of information (data descriptions about actual data). The Data standards category focuses on the actual information *content* to be shared. The Exchange Protocols standards category addresses *how* the information is to be shared across systems and networks. Finally, the Services standards category describes the uniform *business processes, common services, and activities* supporting information sharing. Further implementation details for using the CTISS Framework can be found in *CTISS, Version 1.0.*

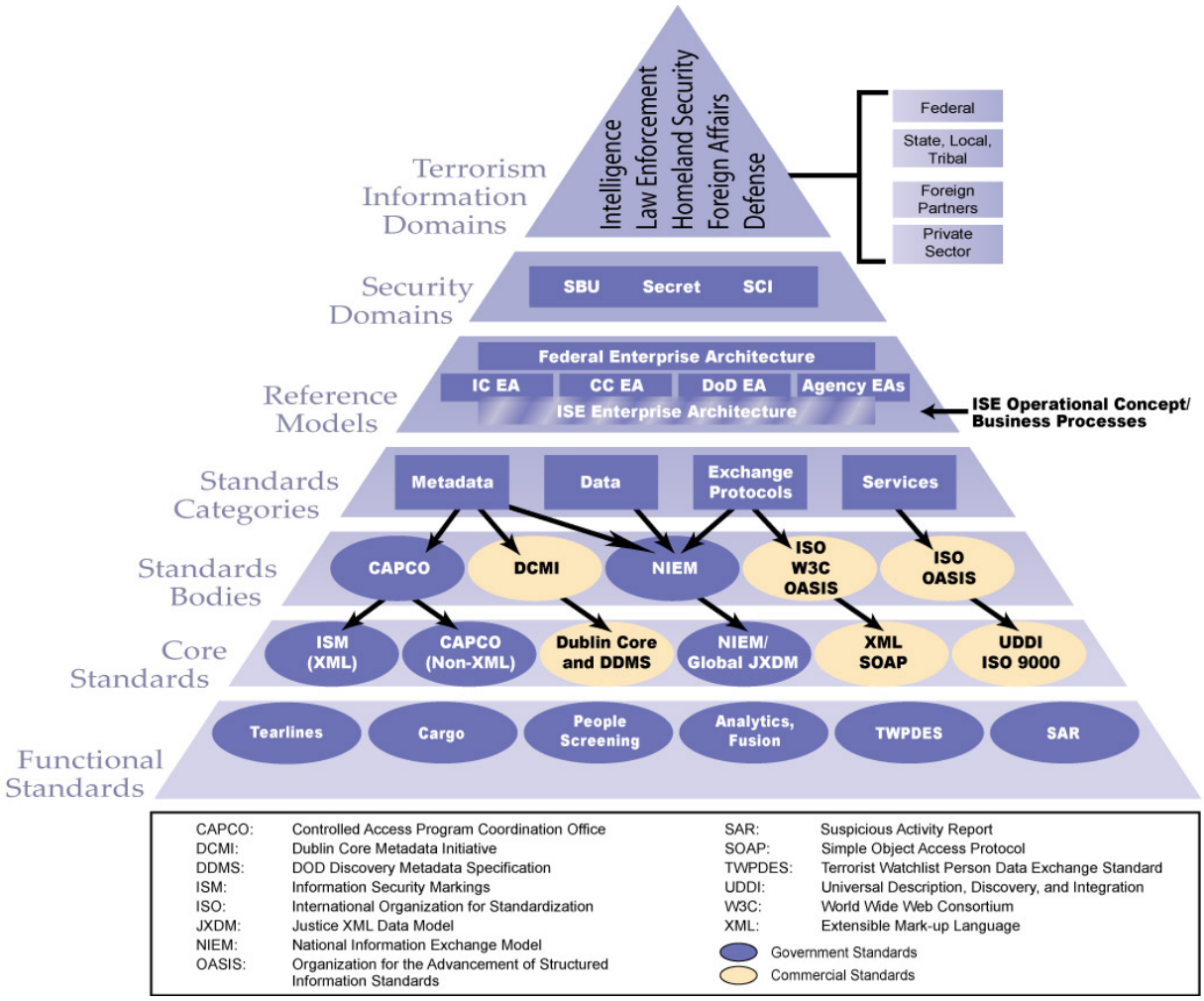


Figure 6.3-1. CTISS Framework

Two functional standards are also documented in *CTISS, Version 1.0* and ready for implementation across the agencies. These standards address priority information sharing business-process issues: tearlines and terrorist watchlists. For future functional standards, the PM-ISE and the ISC will prioritize standards requirements considering such factors as critical need, existing standards maturity, and technical and budgetary feasibility. Other standards not noted, like geospatial, will be incorporated as identified priority business processes that need to be supported. The PM-ISE and the ISC will also review implementation cost impacts on existing and planned investments, including operations, with affected agencies, and document these potential impacts in the recommendations for functional standards implementation. CTISS publishing processes will distribute standards to affected ISE agencies, and the PM-ISE proposes that NIST have the designated role as publishing agent for ISC-approved CTISS functional standards. This designation follows consistently with the role NIST currently has for selecting and publishing standards across Federal government civil systems. However,

current Federal policy does not assign NIST the exclusive role of generating standards for national security systems, and as such the CTISS publishing approach will include coordination with the Offices of the DNI/CIO, the DoD CIO, the NCS Manager, and the CNSS as well. In conjunction with publishing these standards, the PM-ISE and the ISC will also set deadlines and high-level milestones for implementation.

6.3.4 Department and Agency Functional Standards Implementation

Introduction of the CTISS into Federal agency information resource infrastructure and management processes will follow two implementation paths: *investment-driven and priority-driven*. The *investment-driven path* will target new systems (i.e., systems whose design is not finalized) or any system undergoing development, modernization and enhancement. Applicable CTISS functional standards will be published at the time of system design, or CTISS implementations will be scheduled that best meet the mission and functional needs of these affected systems. Timelines for implementation will be synchronized to fiscal year programming and budgeting cycles. Additionally, the CTISS process will introduce functional standards that are compatible for integration into the FEA and national security system EAs. In general, standards affecting architectures *not* designated as national security systems will be coordinated through existing OMB processes. Standards affecting national security systems funded through the National Intelligence Program (NIP) will be coordinated through the ODNI and the CNSS, and standards affecting systems funded through the Military Intelligence Program (MIP) will be coordinated through the Office of the Secretary of Defense. Standards affecting the NCS will be coordinated through the NCS Manager and the NCS COP.

The *priority-driven path* targets those critical business processes along functional areas and associated systems that require adoption within a near-term, fixed time period, potentially without immediate identified funding. For these standards, the PM-ISE and the ISC will set identified priorities and work with agencies to review cost impacts on existing and planned investments, documenting these potential impacts during standards selection. Priority-driven functional standards should be reviewed by agencies with assessments made concerning operational and programmatic cost impacts weighed with the benefits for improving information sharing across the ISE community. Departments and agencies should identify all impacts, to include those affecting operations, as soon as possible so they can determine feasible implementation strategies to minimize impacts while promoting the incorporation of new standards needed in these critical areas.

The PM-ISE will work with the ISC, utilizing the White House policy process, to effectively implement the CTISS. New policy, where appropriate, should clarify that the CTISS will be promulgated uniformly to all Federal information sharing resources to include those designated as national security systems, with appropriate protections of information, and sources and methods uniquely associated with national security systems. This new policy should address the roles of DoD, the DNI, OMB, the PM-ISE, the ISC, the CNSS, the NCS, and Federal departments and agencies in implementing

CTISS. These policies, where appropriate, should expand upon legislation such as the National Technology Transfer and Advancement Act of 1995, the Information Technology Management Reform Act of 1996, the E-Government Act of 2002, the Federal Information Security Management Act, and IRTPA to ensure that the CTISS is implemented uniformly across all Federal systems.

Information sharing standards for non-Federal government agencies will be published as recommendations from the ISC, through the Attorney General and the Secretary of Homeland Security, for use by SLT governments, law enforcement agencies, and the private sector. As the ISE continues to evolve, organizations not in compliance with these standards may find it increasingly difficult to connect to the ISE. However, since these standards are being developed in collaboration with the National Information Exchange Model (NIEM), a joint Federal, SLT, and private sector standards group co-sponsored by DOJ and DHS, standards consideration and adoption actions will reach a wide distribution of SLT and private sector organizations. Fusion centers, and their associated management policies and processes, will be central outreach elements to extend CTISS incorporation out to the State and local levels. Therefore, fusion centers are advised to follow CTISS and provide translations that enable ISE connectivity to those external participating systems not inherently compliant with CTISS.

6.3.5 Implementation Actions

6.3.5.1 Phase 1 Actions

During Phase 1 of ISE implementation:

Action 1.17 The PM-ISE will convene and chair a new working group, the CTISS Working Group (CTISSWG), with representatives from all ISC members, the NCS, NIST, and the CNSS tasked with selecting and issuing information sharing standards, approved through the ISC, and formally published by NIST. The CTISS may include new standards that agencies will introduce to affect on-going investment activities as project schedules and funding permit. Future funded investments incorporating the CTISS will be compatible with the FEA and national security system EAs, and identified in normal agency submittals to the OMB. The CTISSWG will issue CTISS recommendations to the ISC for information sharing standards for non-Federal government agencies. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.18 Departments and agencies will begin to incorporate the CTISS into investment planning, consistent with ISEEA Framework incorporation, with full CTISS incorporation into investments beginning execution in FY 2009. This will include both civil and national security system investments. Agencies will also incorporate the CTISS into information resource lifecycle processes

to include CPIC processes. The CTISS will provide the source of functional standards for information sharing in the FEA's Technical and Data Reference Models. (Planned Completion: Second Quarter, CY 2007)

Action 1.19 The PM-ISE, in consultation with the ISC, will develop *CTISS, Version 2.0* addressing additional processes, including those with foreign partners, and releasing priority functional standards supporting suspicious activity reports (SARs), cargo management and tracking, and general identity management. (Planned Completion: Second Quarter, CY 2007)

6.3.5.2 Phase 2 Actions

During Phase 2 of ISE implementation:

Action 2.13 The PM-ISE and ISC members will work with standards bodies and published standards to expedite efforts to identify the critical gaps in available core standards needed for developing new CTISS functional standards. (Planned Completion: Third Quarter, CY 2007)

Action 2.14 OMB will incorporate new standards from the CTISS into the Technical and Data Reference Models with standards compliance monitored and verified through the Federal Transition Framework and the FEA Program: Enterprise Architecture Assessment Framework. (Planned Completion. (Planned Completion: Third Quarter, CY 2007)

Action 2.15 OMB will publish a new version of the Federal Transition Framework and the FEA Program: EA Assessment Framework incorporating the current CTISS. (Planned Completion: Fourth Quarter, CY 2007)

Action 2.16 OMB will conduct FY 2009 EA reviews to verify incorporation of the CTISS requirements. (Planned Completion: Second Quarter, CY 2008)

Action 2.17 The PM-ISE will work with DOJ, DHS, and other Federal departments and agencies to implement the CTISS into fusion centers to assist them in implementing the CTISS for eventual migration into SLT government infrastructures, where appropriate. Published commercial standards will be leveraged to the maximum extent practical. (Planned Completion: Second Quarter, CY 2008)

Action 2.18 The PM-ISE will work with the Department of Commerce, through NIST, to promote, coordinate, and distribute the CTISS Framework for incorporation by the private sector into new technology and products, where appropriate, supporting terrorism information sharing. (Planned Completion: Third Quarter, CY 2008)

Chapter 7 – Sharing with Partners Outside the Federal Government

7.1 State, Local, and Tribal Governments

7.1.1 Implementing the Framework

The framework depicted in Figure 7.1-1, developed in response to Presidential Guideline 2 establishes a coordinated, collaborative structure through which terrorism information is shared between and among participating Federal, SLT, and private sector organizations to support a variety of different activities, including preventive and protective actions, immediate actionable response, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events.[68]

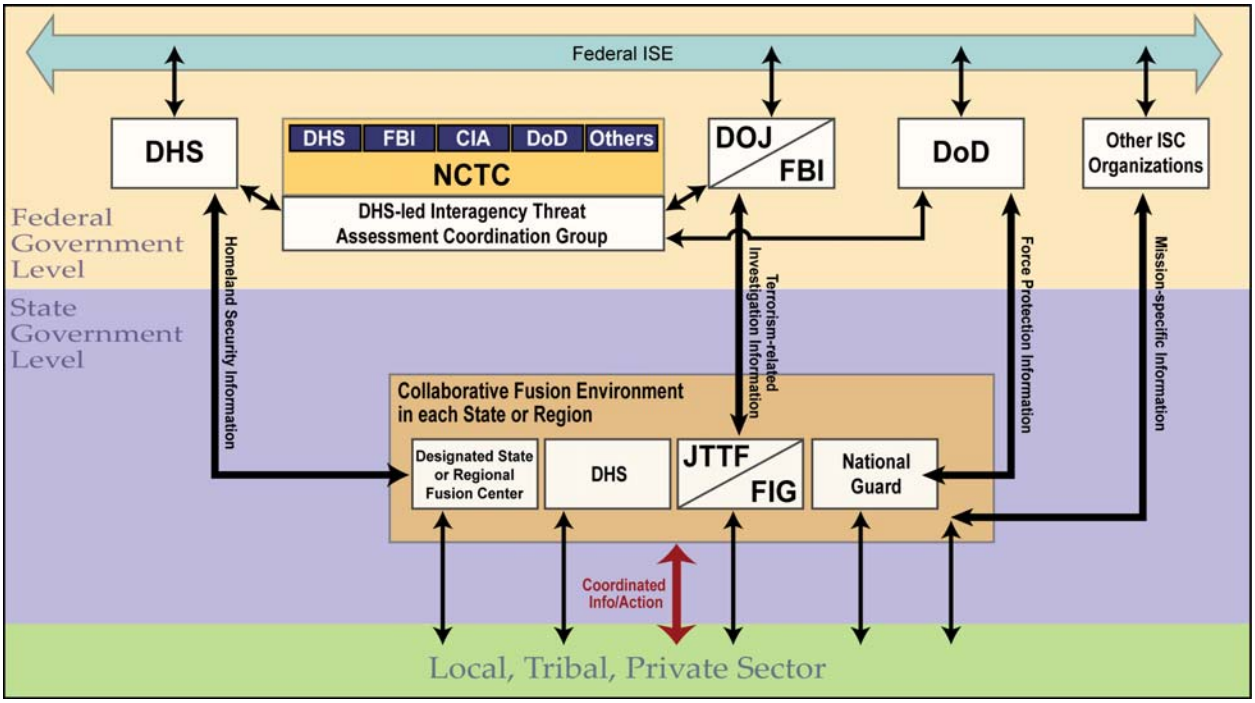


Figure 7.1-1. Approved Guideline 2 Framework

[68] Guideline 2 of the Presidential *Information Sharing Guidelines and Requirements* requires the Attorney General and the Secretary of Homeland Security to submit to the President "a recommended framework to govern the roles and responsibilities of executive departments and agencies pertaining to the acquisition, access, retention, production, use, management, and sharing of homeland security information, law enforcement information, and terrorism information between and among such departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector entities."

This framework draws upon and integrates existing capabilities and systems and acknowledges the roles and responsibilities of DoD, DOJ, DHS, and the DNI, among others, to deter and prevent terrorism and protect the homeland. Because those roles and responsibilities often intersect, the framework establishes a coordinated and collaborative approach to ensure effective, efficient, and non-competing efforts to share terrorism information with SLT governments and the private sector. The framework, recognizing the important missions of statewide and major urban area fusions centers, integrates them as partners in the ISE. Therefore, each is required to meet a certain baseline level of capability and to comply with all applicable privacy laws. The framework also preserves and maintains the roles and responsibilities of participating Federal departments and agencies, and mandates a coordinated and collaborative approach to sharing terrorism information with SLT officials and the private sector. It supports and leverages the success of ongoing initiatives at each level of government and seeks practical solutions to challenges that emerge during ISE implementation. The "To Be" ISE will achieve the following desired outcomes:

1. Improved coordination at the national level for the production and dissemination of terrorism information; and
2. Shared responsibility between Federal and State governments for the timely processing and dissemination of information at every level to meet the needs of all end users.

Chapter 3 describes the Federal, SLT, and private sector components and functions of the ISE. When fully implemented the framework will:

1. Provide a Federal-level interagency capability to facilitate the fusing, validation, deconfliction, and dissemination of terrorism information to SLT authorities and the private sector;
2. Encourage and enhance the collaborative environment at the SLT level by assisting in the development of State and major urban area fusion centers and establish a national, integrated network of these fusion centers;
3. Ensure that Federal organizations operating at the State level put protocols in place to ensure that time sensitive and strategic threat information is effectively shared and used to support a broad array of critical infrastructure protection, prevention, response, and recovery activities;
4. Establish a requirement where designated State and major urban area fusion centers operate at a baseline level of capability as defined by the Global/Homeland Security Advisory Committee Guidelines and in compliance with all applicable Federal laws and policies regarding the protection of information and privacy and other legal rights of individuals;
5. Preserve existing "mission specific" channels of communication for each participating agency to use in fulfilling agency-specific mandates to report terrorism information to SLT governments, with communications designed to

ensure the Federal government delivers coordinated, comprehensive, and useful information to SLT and private sector organizations;

6. Ensure improved interoperable communications between Federal and SLT organizations;
7. Foster an environment in which sharing terrorism information is a complementary rather than a competitive process;
8. Establish a terrorism-information priorities framework to guide the gathering, analysis, and dissemination of law enforcement, public safety, and terrorism information; and
9. Consolidate and standardize the numerous disparate alert, tip, advisory, situational awareness, and warning systems.

This shared-responsibility approach to information sharing builds on our established Federal system to meet the needs of consumers of terrorism information at every level of government. It will enable the rapid exchange of terrorism information within a coordinated environment that reflects organizational realities while overcoming longstanding barriers to information sharing. It will ensure that information produced by Federal organizations within the intelligence, law enforcement, and homeland security communities is fused, validated, deconflicted, and disseminated in a concise and, whenever possible, unclassified format. And it will ensure information developed within the SLT framework is available to appropriate Federal organizations.

7.1.2 Implementation Actions

7.1.2.1 Phase 1 Actions

Action 1.20 Within 30-days of approval of the proposed Guideline 2 framework, the PM-ISE, in consultation with the ISC, will establish a Senior-level Advisory Group—consisting of ISC members or their designees—to ensure accountability, oversight, and governance for the effective operation of the framework. The advisory group will report the results of its oversight to the PM-ISE and the ISC. The advisory group will meet at least once per month during the first year of implementation. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.21 Within seven days of approval of the proposed framework, there will be established an Implementation Team—comprised of representatives from DOD; DOI; DHS; FBI; NCTC; appropriate State, local, tribal, and private sector advocates; and the PM-ISE—to develop an implementation plan for the Interagency Threat Assessment and Coordination Group framework and to ensure its timely execution. The implementation team will develop and

implement plans to notify SLT officials of the ITACG mission and responsibilities. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.22 The ITACG Implementation Team will submit semiannual reports to the PM-ISE that identify successes and shortcomings in implementing and operating the ISE within the Guideline 2 framework and outline steps to refine and improve the framework's operation. (Planned Completion: Ongoing with first report due in the first quarter of CY 2007)

Action 1.23 The PM-ISE will establish a Federal Fusion Center Coordination Group to identify Federal resources to support the development of a network of State-sponsored fusion centers charged to share information at all levels of the ISE and will recommend funding options. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.24 DOJ and DHS will work with Governors or other senior State and local leaders to designate a single fusion center to serve as the statewide or regional hub to interface with the Federal government and through which to coordinate the gathering, processing, analysis, and dissemination of terrorism information. (Planned Completion: First Quarter, CY 2007)

Action 1.25 DOJ and DHS, to the extent possible and practicable, will assume the responsibility for technical assistance and training to support the establishment and operation of these fusion centers. (Planned Completion: First Quarter, CY 2007)

Action 1.26 Appropriate Federal departments and agencies will assess resources and develop and coordinate plans to assign representative personnel to State and local fusion centers. These representatives will work to the extent possible to further integrate—and where appropriate collocate—Federal and State/regional resources. (Planned Completion: First Quarter, CY 2007)

7.1.2.2 Phase 2 Actions

Action 2.19 The DNI will ensure that SLT and private sector ISE participants' needs and priorities for terrorism information are addressed in the Intelligence Community's requirements process. (Planned Completion: Ongoing with first progress report in the third quarter of CY 2007)

Action 2.20 The Guideline 2 Senior-level Advisory Group will ensure each designated State and/or major urban area fusion center achieves a baseline level of capability and complies with all applicable Federal laws and policies regarding the protection of information and privacy and other legal rights of individuals. Semiannual progress

reports will be provided to the PM-ISE and the ISC. (Planned Completion: Ongoing with first progress report in the third quarter of CY 2007)

Action 2.21 Statewide and major area fusion centers will ensure locally generated terrorism information is communicated to the Federal government through appropriate systems identified by Federal officials as part of ISE implementation. (Planned Completion: Ongoing with first progress report in the fourth quarter of CY 2007)

7.2 Private Sector

An effective framework that ensures a two-way flow of timely, actionable threat information between public and private partners is essential in the War on Terror. As described in Section 2.3.3, private sector information represents a crucial element in both understanding the current threat environment and protecting our nation's critical infrastructure from targeted attacks. The private sector owns and operates over eighty percent of the nation's critical infrastructure, and is therefore a primary source and repository for relevant terrorism information.[69] Protecting our nation's interconnected and interdependent infrastructure also requires a robust public-private partnership that provides the private sector with information on incidents, threats, and vulnerabilities, while protecting private sector information in such a way that the private sector is willing to share it with government partners.

Efforts to improve sharing of terrorism information with the private sector are ongoing. These activities are based on the authority provided to the Secretary of Homeland Security by the *Homeland Security Act of 2002* and HSPD-7, which define infrastructure protection responsibilities for DHS, sector-specific agencies, and other departments and agencies. Specifically, HSPD-7 instructs Federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. In addition, the NIPP, released recently by DHS, is the cornerstone document that prescribes a national implementation strategy for HSPD-7 and creates a public-private partnership structure through which to affect that strategy. All of the requirements and tasks identified in these documents require an efficient and effective two-way flow of information between Federal and SLT governments and private sector partners.

The President also created the National Infrastructure Advisory Council (NIAC).[70] The NIAC is charged to improve the cooperation and partnership between the public and private sectors in securing critical infrastructures, and advises the President and Secretary of Homeland Security on policies and strategies that range from risk assessment and management to information sharing, protective strategies, and

[69] The Government Accountability Office estimated that the private sector operates over 80 percent in its report *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, May 8, 2003.

[70] E.O. 13231 (October 16, 2001) as amended by E.O. 13286 (February 28, 2003) and E.O. 13385 (September 29, 2005).

clarification on roles and responsibilities between public and private sectors. In July 2006, the NIAC approved a report and made recommendations to the President on private sector intelligence and information sharing that raised the same issues and reached the same conclusions as those of their State and local government counterparts. As a result, an effective terrorism information sharing framework must continue to:

1. Build a trusted relationship between the Federal, SLT, and private partners to facilitate information sharing. In some cases, establishing such relationships may be difficult because sector-specific agencies may also have a regulatory role;
2. Improve the two-way sharing of terrorism information on incidents, threats, and vulnerabilities. Most critical infrastructure sectors, like their SLT partners, are still concerned with the limited quantity and quality of information and the need for more specific, timely, and actionable information. Likewise, the Federal and SLT governments need to have policies in place that will ensure the protection of private sector vulnerability information that is shared with government partners.
3. Integrate private sector analytic efforts into Federal and SLT processes, as appropriate, for a more complete understanding of our terrorism landscape. The private sector understands its processes, assets, and operations best and can be relied upon to provide the required private sector subject matter expertise.
4. Establish baseline standards to enforce compliance with all applicable privacy laws as they pertain to information sharing with the private sector.

The sharing framework developed in response to Presidential Guideline 2 now provides the strong foundation from which Government agencies at all levels can effectively and efficiently share information with the private sector. That said, this framework, while an essential step in the right direction, will not by itself ensure that all private sector terrorism information sharing needs are fully addressed.

In recognition of the importance of private sector involvement in the ISE, the ISC established a standing Private Sector Subcommittee whose coordination mechanism will primarily be based on the NIPP sector partnership structure.[71] Co-chaired by DOJ and DHS, this subcommittee will provide a forum to ensure that implementation actions related to the SLT and private-sector framework are completed and address private-sector issues. Specifically, during Phases 1 and 2 of ISE implementation:

[71] The subcommittee is comprised of persons and entities outside the Federal government who provide the ISC with expert advice and guidance in accordance with Section 1016(g)(3) of IRTPA.

Action 1.27 The Private Sector Subcommittee will produce a plan that implements elements of the framework as it affects the private sector. This plan must be consistent with statutes and Presidential direction and ensure that information and privacy and legal rights are adequately protected. (Planned Completion: Second Quarter, CY 2007)

Action 2.22 The PM-ISE, in consultation with the ISC, will review the private sector sharing plan developed in Phase 1 and identify priorities for implementation. In addition, some of the recommendations are likely to entail issues requiring executive-level decisions or legislative changes. (Planned Completion: Fourth Quarter, CY 2007)

7.3 Foreign Partners

Strong and effective cooperation with our foreign partners is a vital component of the global war on terrorism. Sharing of terrorism information between Federal departments and agencies and foreign partners and allies is therefore essential, and policies and procedures to facilitate this information access and exchange must be established.

DOS established the Foreign Government Information Sharing Working Group in November 2005 to meet Presidential Guideline 4 requirements by providing recommendations for appropriate legislative, administrative, and policy changes to improve the sharing of terrorism information with foreign partners and allies, except for those activities conducted pursuant to sections 102A(k), 104A(f), and 119(f)(1)(E) of the National Security Act of 1947.[72] The recommendations address bi-directional sharing of information with foreign governments, i.e., facilitating appropriate dissemination and protection of U.S. information given to foreign partners and also protecting information provided to the United States by foreign partners, while still allowing for maximum dissemination, when appropriate. The working group also recommended that the President issue a memorandum that provides specific steps that departments and agencies should take to develop an appropriate internal and international framework for information sharing with foreign partners.

The implementation of the foreign government information sharing recommendations will occur over Phases 1 and 2 of the overall ISE development. Federal departments and agencies will begin implementing the Presidential Guideline 4 Working Group's recommendations once they are approved by the President in the following priority areas:

[72] Presidential Guideline 4 excluded from the working group's consideration and recommendations those activities conducted pursuant to Sections 102A(k), 104A(f), and 119(f)(1)(E) of the National Security Act of 1947.

1. Ensuring proper handling and protections of U.S. and foreign government classified, sensitive, and other restricted information;
2. Ensuring that sharing with foreign partners and allies does not compromise privacy protections and is in accordance with requirements for sharing U.S. person information;
3. Facilitating appropriate and timely sharing of terrorism information between the United States and foreign partners;
4. Ensuring that agencies have necessary information regarding foreign government domestic regimes and practices; and
5. Developing an appropriate international framework to facilitate information sharing while affording necessary protections.

To implement these priorities, the following actions are recommended for Phase 1:

Action 1.28 The Foreign Government Information Sharing Working Group, with coordination and assistance from the PM-ISE, will develop recommendations on Privacy Act systems of records notices and routine uses for the Guideline 5 Working Group. (Planned Completion: First Quarter, CY 2007)

Action 1.29 The Foreign Government Information Sharing Working Group, with coordination and assistance from the PM-ISE, will develop a checklist of issues that need to be taken into account in negotiating international agreements, including privacy protections and possible review procedures. (Planned Completion: Second Quarter, CY 2007)

Action 1.30 Federal departments and agencies, with coordination and assistance from the PM-ISE, will encourage bilateral and multilateral efforts whenever feasible and appropriate to develop “best practices” on terrorism information sharing (e.g., protocols on what to do if there is a “hit”). (Planned Completion: Ongoing with a first progress report in the second quarter of CY 2007)

The following actions are also recommended for Phase 2:

Action 2.23 Federal departments and agencies, with coordination and assistance from the PM-ISE, will ensure that all agencies issue internal procedures to expedite disclosure decisions, including clear written procedures on declassification and release of terrorism information to foreign governments. (Planned Completion: Second Quarter, CY 2008)

Action 2.24 Federal departments and agencies, with coordination and assistance from the PM-ISE, will ensure that agency Privacy Act systems of records notices and routine uses provide for terrorism information sharing with foreign partners. (Planned Completion: Second Quarter, CY 2008)

Action 2.25 The ISC will develop appropriate common standards or protocols for electronic handling of foreign government information within the ISE to ensure that any necessary foreign government requirements are respected. (Planned Completion: Third Quarter, CY 2008)

Action 2.26 Federal departments and agencies, with coordination and assistance from the PM-ISE, will encourage appropriate international standardization of technological and substantive marking and handling standards. (Planned Completion: Ongoing with a first progress report in the second quarter of CY 2008)

Action 2.27 Federal departments and agencies, with coordination and assistance from the PM-ISE, will consider impact on U.S. persons when negotiating international arrangements that involve sharing information with foreign governments. (Planned Completion: Ongoing with a first progress report in the second quarter of CY 2008)

Action 2.28 Federal departments and agencies, with coordination and assistance from the PM-ISE, will consider possible interaction with provisions of existing agreements when negotiating new international agreements (e.g., inconsistent promises, "most favorable" treatment). (Planned Completion: Ongoing with a first progress report in the second quarter of CY 2008)

Action 2.29 Federal departments and agencies, with coordination and assistance from the PM-ISE, will ensure "foreign disclosure officers" or comparable approaches are adopted by all government agencies to make and expedite disclosure decisions and provide resources to support disclosure decisions (e.g., training, information, automation tools). (Planned Completion: Fourth Quarter, CY 2008)

Action 2.30 Federal departments and agencies engaged in developing terrorism information sharing agreements and best practices and protocols, with coordination and assistance from the PM-ISE, will make both the registry and the text of all such agreements, as well as the texts of any best practices and protocols, available to other departments and agencies, including to the extent feasible, in electronic form, as part of the ISE. (Planned Completion: Fourth Quarter, CY 2008)

Action 2.31 The PM-ISE will work closely with the ISC to ensure effective and efficient implementation of the Foreign Government Information Sharing Working Group recommendations. (Planned Completion: Second Quarter, CY 2009)

Action 2.32 Federal departments and agencies, with coordination and assistance from the PM-ISE, will ensure agency authorities permit the full range of requirements for information sharing with foreign partners. (Planned Completion: Second Quarter, CY 2009)

PART III

Major Challenges

This page intentionally blank.

Chapter 8 – Promoting a Culture of Information Sharing

8.1 Promoting a Culture of Information Sharing

In accordance with Section 1016 of IRTPA, Requirement 2 of the Information Sharing Guidelines and Requirements directed heads of executive departments and agencies to work to promote a culture of information sharing by:

1. Assigning personnel and dedicating resources to terrorism information sharing;
2. Reducing disincentives to such sharing; and
3. Holding their senior managers and officials accountable for improved and increased sharing of such information.[73]

In order to implement an effective, widespread culture of information sharing, balanced with a need for security and the protection of privacy and civil liberties, Federal departments and agencies are working to complete the Presidentially-directed actions as described below.

First, ISC member departments and agencies designated an accountable senior official to provide direct, agency-wide oversight authority for the planning, development, and implementation of all aspects of the ISE including policy, technology, budget, and management. In order to cultivate and promote the information sharing culture within their respective agencies, these senior officials:

1. Provide accountability and oversight for terrorism information sharing within their departments or agencies;
2. Work with the PM-ISE, in consultation with the ISC, to develop high-level information sharing performance measures for the department or agency to be assessed no less than semiannually; and
3. Provide, through the department or agency head, an annual report to the DNI on best practices for and remaining barriers to optimal terrorism information sharing.

At the same time information sharing responsibilities will permeate all levels of government, from chief executives to entry-level analysts.

Second, Federal departments and agencies are developing guidelines, providing training and incentives, and holding personnel accountable for the improved and increased sharing of terrorism information (see Section 8.2).

[73] *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements In Support of the Information Sharing Environment* (2005), Section 3.

Third, on an ongoing basis, Federal departments and agencies will bring to the attention of the Attorney General and DNI any restriction contained in a rule, regulation, executive order, or directive that significantly impedes the sharing of terrorism information and that such department or agency head believes is not required by applicable laws or to protect privacy and civil liberties. The Attorney General and DNI will review such restrictions and, if appropriate, jointly submit any recommendations for changes to such restrictions to the Assistant to the President for Homeland Security and Counterterrorism (APHS-CT), the Assistant to the President for National Security Affairs (APNSA), and the Director of OMB for further review.

The success of an overarching information sharing culture will depend heavily on the establishment and maintenance of clear policy, authority, and guidance for the sharing of terrorism information and widespread application of training and incentives to share. In Phase 1 of the ISE development, departments and agencies will consider implementing incentives that may include:

1. Monetary and non-monetary awards;
2. Recognition within the department/agency of an office or an individual who developed an improved information-sharing practice;
3. Inclusion in internal newsletters of information sharing accomplishments and the tangible end benefits that resulted;
4. Development of awareness materials;
5. Establishment of an annual Federal award for the agency or work unit that best fostered the culture of information sharing; and
6. Sharing "best practices" regarding effective ways to educate and motivate their personnel, perhaps through the PM-ISE website.

8.2 ISE Training Plan

As discussed in Section 8.1, training is a crucial component of an improved culture of information sharing. The ISE training plan will be implemented through a "core" training program across all departments and agencies, combined with department/agency-specific training. Collectively, these training elements will allow ISE participants to meet the ISE's goals outlined in Chapter 1.

8.2.1 "Core" Training

"Core" refers to common goals that must be the same across Federal departments and agencies and should extend to SLT governments. This training module will draw from laws, regulations, and policies, including executive orders, Presidential directives, and Presidential memoranda, enabling all personnel in Federal departments and agencies participating in the ISE to:

1. Understand definitions of "information sharing environment" and "terrorism information";
2. Be familiar with the legal basis for information sharing and the roles of the PM-ISE and the ISC;
3. Be familiar with the *Guidelines To Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment* (see Chapter 9);
4. Understand the authorities and regulations that pertain to the IC, Federal law enforcement agencies, military and diplomatic communities, SLT governments, and private organizations that collect or receive terrorism information;
5. Be familiar with efforts to integrate SLT governments and private sector information into the ISE;
6. Understand and promote the culture of information sharing;
7. Understand the requirement for collecting and handling terrorism information inside the United States;
8. Be familiar with the format of and distribution controls for tear-lines derived from intelligence reporting and with the concept of "write-for-release";
9. Upon final approval of the standards for SBU information:
    a. Understand the definition of SBU and of similar controls;
    b. Know what should be SBU; and
    c. Know how SBU information may be used, shared, secured, transmitted, and released; and
10. Be familiar with information assurance and computer security standards and protocols to implement the ISE.

Due to its extensive background in training development and vast experience with distance learning, DOS' Foreign Service Institute (FSI) has agreed to develop the core training module, which will serve as a common educational baseline for the ISE. This module will be jointly funded through the PM-ISE's office with additional voluntary contributions from departments and agencies. Together with a working group of ISC training representatives, the PM-ISE will review the training module and ensure implementation across the ISE.

All Federal department and agency personnel who are charged with sharing terrorism information, or supporting such sharing, will be required to take the core training. This includes but is not limited to: intelligence discipline and Federal law enforcement personnel and managers involved in collection, analysis, tasking, production, exploitation, and distribution of terrorism information, as well as information assurance

and technology specialists, and members of Congressional liaison, public affairs, policy, and budget staffs.

8.2.2 Department and Agency Specific Training

In addition to the core training, departments and agencies will develop tailored training programs based on their unique business processes, missions, program, and policy needs. This specific training should enable personnel in Federal departments and agencies participating in the ISE to:

1. Know the department or agency's role in the ISE;
2. Apply information sharing authorities and responsibilities pertaining to his/her department or agency and position;
3. Understand Federal roles and responsibilities with regard to information sharing with SLT governments and the private sector;
4. Know how to share information via the ISE, according to the department or agency's role and authorities;
5. Be able to properly mark information contributed to the ISE to convey the currency and reliability of the information and redistribution requirements;
6. Know the information sharing tools available;
7. Know the department or agency's procedures for user access to information sharing tools such as EDS (White/Yellow/Blue/Green Pages) and responsibility for updating this information, NCTC resources, and Terrorist Screening Center (TSC) data;
8. Know the roles and responsibilities of other ISE participants;
9. Understand how to request terrorism information via the ISE;
10. Know where to find points of contact that can answer questions regarding the ISE;
11. Be familiar with incentives for information sharing and the requirement to include a performance evaluation element in annual performance appraisal reviews; and
12. Know the department or agency's procedures for handling "protected information."[74]

[74] The *Guidelines To Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment* apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the Intelligence Community, protected information includes information about "United States persons" as defined in E.O. 12333. Protected information may also include other information that the Federal government expressly determines by Executive Order, international agreement, or other similar instrument should be covered by the Guidelines. See Chapter 9.

8.3 Implementation Actions

During Phase 1 of ISE implementation:

Action 1.31 The DOS FSI, supported by the working group of ISC training representatives, will develop the core training module that will serve as the common educational baseline for the ISE. (Planned Completion: Second Quarter, CY 2007)

Action 1.32 The PM-ISE, in consultation with the ISC, will review departmental incentives for sharing of terrorism information and will measure their effectiveness. (Planned Completion: Second Quarter, CY 2007)

During Phase 2 of ISE implementation:

Action 2.33 All Federal departments and agencies responsible for terrorism information sharing will develop tailored training programs based on their unique business processes, missions, program, and policy needs. (Planned Completion: Fourth Quarter, CY 2007)

Action 2.34 DOJ, DHS, and FBI, in coordination with the ISC SLT Subcommittee and with guidance from the ISC training working group, will develop information sharing training guidelines for SLT governments. The guidelines will include the core training goals used by the departments and agencies represented on the ISC, as well as training specific to SLT and private sector operating environments and officers. (Planned Completion: Fourth Quarter, CY 2007)

Action 2.35 All Federal departments and agencies will provide the PM-ISE with a copy of their agency-specific training modules, as well as a count of the number and career categories of personnel who have received training on the ISE for inclusion in the President's report on ISE performance. This information will continue to be submitted on an annual basis. (Planned Completion: Second Quarter, CY 2008)

Action 2.36 Federal departments and agencies will train newly hired personnel within six months of entrance on duty. Each executive department and agency will also include information sharing in performance appraisal reviews as appropriate. (Planned Completion: Fourth Quarter, CY 2008)

Action 2.37 Federal departments and agencies will recommend modifications to internal policies, as appropriate, to accommodate the ISE training, incentive, and accountability requirements, including each will review its procedures for disciplining personnel who fail to adhere

to security procedures regarding the handling and distribution of classified and controlled information. (Planned Completion: Fourth Quarter, CY 2008)

Chapter 9 – Protecting Information Privacy and Civil Liberties in the ISE

9.1 Background

IRTPA requires that the ISE incorporate protections for individuals' privacy and civil liberties.[75] IRTPA also requires the President to issue guidelines that protect privacy and civil liberties in the development and use of the ISE.[76] Accordingly, in December 2005, the President issued guidelines that, among other things, directed the Attorney General and the DNI, in coordination with the heads of executive departments and agencies that possess or use intelligence or terrorism information, to:

1. Conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans; and
2. Develop guidelines to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information.[77]

The Attorney General and the DNI completed the review, developed guidelines, and forwarded them to the President through the Director of OMB and the APHS-CT and APNSA. The final recommendations of the Attorney General and the DNI—*Guidelines To Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment*—are summarized in the next Section.

9.2 ISE Information Privacy Guidelines

The Guidelines describe the means by which Federal departments and agencies participating in the ISE will protect privacy and civil liberties in the development and operation of the ISE. Key features include:

[75] IRTPA, Section 1016(b)(2)(H).
[76] IRTPA, Section 1016(d)(2)(A).
[77] *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements In Support of the Information Sharing Environment* (2005), Section (2)(e).

1. Compliance with laws. The Guidelines state that all agencies shall, without exception, comply with the Constitution and all applicable laws and executive orders relating to protected information.[78]
2. Process-based approach. The Guidelines require each agency to implement an ongoing process for identifying and assessing the laws, executive orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE.
3. Specification of purpose. The Guidelines state that "protected information" should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information.[79]
4. Consistent with the criteria set forth in the guidelines, each agency is also required to:
    a. Identify its data holdings that contain protected information to be shared through the ISE, ensure protected information has been reviewed pursuant to the Guidelines, and establish mechanisms that allow ISE participants to determine the nature of the protected information so that such participants can handle the information in accordance with applicable legal requirements;
    b. Implement data quality procedures;
    c. Use appropriate security measures to safeguard information;
    d. Implement procedures to hold personnel accountable for violations of policies, provide training to personnel, and enable effective reviews and audits to verify compliance with the Guidelines;
    e. Establish redress procedures consistent with the agency's legal authorities and mission requirements to address complaints from persons regarding protected information about them that is under the agency's control;
    f. Implement guidelines via training, business process changes, and system designs; and
    g. Facilitate appropriate public awareness of the Guidelines.

[78] The Privacy Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the Intelligence Community, protected information includes information about "United States persons" as defined in E.O. 12333. Protected information may also include other information that the Federal government expressly determines by Executive Order, international agreement, or other similar instrument should be covered by the Guidelines.

[79] These terms are defined in Section 13 of the Privacy Guidelines, and are also included in Appendix 4 of this plan.

5. Governance Structure:
    a. Makes clear that each agency's senior official with overall agency-wide responsibility for information privacy issues shall directly oversee the agency's implementation of and compliance with these guidelines;[80]
    b. Requires each agency to designate an ISE Privacy Official;
    c. Directs the PM-ISE to establish an ISE Privacy Guidelines Committee consisting of ISC members' ISE Privacy Officials to work in consultation with the PCLOB; and
    d. Requires each agency to prepare an ISE Privacy Protection Policy setting forth the implementation of the Guidelines.

Consistent with standards and procedures that may be issued to govern participation in the ISE by SLT governments and private sector organizations, each agency shall work with the PM-ISE to ensure that non-Federal organizations seeking to access the agency's protected information through the ISE have implemented appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the Guidelines.

9.3 Implementation Actions

During Phase 1 of ISE implementation:

Action 1.33 Each agency will ensure that one or more ISE Privacy Officials are designated in accordance with paragraph 12.a of the privacy guidelines. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.34 The PM-ISE will establish and designate a chair for the ISE Privacy Guidelines Committee. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.35 The PM-ISE, in consultation with the ISE Privacy Guidelines Committee and the ISC, will establish a process for ensuring that non-Federal organizations participating in the ISE implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the Guidelines. (Planned Completion: First Quarter, CY 2007)

Action 1.36 The ISE Privacy Guidelines Committee will provide an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections, to be included in the President's first

[80] As designated by statute, Executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005.

annual ISE performance report. (Planned Completion: Second Quarter, CY 2007)

During Phase 2 of ISE implementation:

Action 2.38 The ISE Privacy Guidelines Committee will provide an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections, to be included in the President's annual ISE performance report. (Planned Completion: Second Quarter, CY 2008 and 2009)

Chapter 10 – Terrorism Information Handling

10.1 Classified Terrorism Information

The handling of classified national security information is governed primarily by Executive Order 12958 and its implementing directives. According to the 9/11 and WMD Commissions, the sharing of terrorism information suffers from cumbersome and outdated information classification and personnel security policies and practices. Two ongoing initiatives address these limitations and promote the modification and reciprocity of security practices: simplification of personnel clearance processes, and the adoption of community-wide certification and accreditation policies and standards.

10.1.1 Personnel Security Practices

In response to Section 3001 of IRTPA, a number of initiatives are underway to streamline and simplify personnel security practices across the Federal government. E.O. 13381, *Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information,* as amended, assigns to OMB responsibility for the government-wide initiative to make clearance processes uniform, centralized, efficient, timely, and reciprocal. Among the initiatives underway: the Office of Personnel Management is charged with developing and operating a government-wide security clearance database; government-wide standards for reciprocal recognition of clearances are under development; and the ODNI has initiated reviews at Federal departments and agencies to assess clearance adjudication practices and make recommendations to speed processes and further enhance reciprocity. The ISE must leverage these government-wide initiatives, as they are important elements for its successful implementation. The PM-ISE and ISC should regularly monitor progress of ISE participants in meeting the goals established in IRTPA Section 3001 as part of the ISE implementation process.

10.1.2 Certification and Accreditation (C&A) Practices

Inconsistent C&A policies and standards across individual departments and agencies, as well as communities, impede the speed and agility of today's ISE, and could inhibit the development of the future ISE. In one effort to address this weakness, the IC is currently working with the defense community, as well as representatives from industry and academia, to overhaul outdated and non-scalable C&A processes. Reducing the time needed to certify and accredit systems, and promoting the reciprocity of C&A decisions, is central to this overhaul. Available and interoperable technical solutions that will enable the future ISE rely upon the development and implementation of enterprise, or community-wide, C&A policies and standards rather than those created locally for specific departments and agencies.

10.1.3 Implementation Actions

Actions relating to the handling of terrorism information address: modifications to personnel security practices, and the adoption of community-wide C&A policies and standards.

10.1.3.1 Phase 2 Actions

Phase 2 will include the following three implementation actions:

Action 2.39 The PM-ISE, in consultation with the ISC, and OMB and the ODNI, will monitor existing performance measures and assess progress against the security clearance processing requirements of IRTPA Section 3001. (Planned Completion: Second Quarter, CY 2009)

Action 2.40 On an ongoing basis, the PM-ISE, in consultation with the ISC, will support Information Security Oversight Office (ISOO) efforts to facilitate compliance with E.O. 12958, as amended, and its implementing directives. (Planned Completion: Ongoing)

Action 2.41 On an ongoing basis, the PM-ISE, in consultation with the ISC, will work closely with ODNI-led efforts to overhaul current C&A policies and standards for the Intelligence Community and will evaluate the applicability of these policies and standards to the broader ISE. (Planned Completion: Ongoing)

10.2 Sensitive But Unclassified Information

Because the ISE crosses three security domains, it must support access to and handling of both classified and unclassified information. Wherever possible, classified terrorism information should be made available in unclassified versions to assure the widest distribution while still protecting sensitive sources and methods. However, the growing and non-standardized inventory of SBU designations and markings is a serious impediment to information sharing among agencies, between levels of government, and, as appropriate, with the private sector.[81] Elimination of this impediment is essential to ensure that the future ISE promotes and enhances the effective and efficient acquisition, access, retention, production, use, management, and sharing of unclassified information while also ensuring its appropriate and consistent safeguarding.

In his December 16, 2005 memorandum, the President provided direction to Federal departments and agencies on the standardization of procedures for handling SBU information. Specifically, Presidential Guideline 3 called on the Secretary of Homeland

[81] According to GAO report (GAO-06-385) *Information Sharing: The Federal Government Needs to Establish Policies and Processes For Sharing Terrorism-Related and Sensitive But Unclassified (SBU) Information* (GAO: Washington, DC, 2006), Federal agencies use at least 56 different sensitive but unclassified designations (16 of which belong to one agency) to protect sensitive information.

Security and the Attorney General—in coordination with the Secretaries of State, Defense, and Energy, and the DNI—to submit to the President for approval recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information.[82]

These recommendations must include three elements:

- Recommendations for government-wide policies and procedures to standardize SBU procedures;
- Recommendations, as appropriate, for legislative, policy, regulatory, and administrative changes; and
- An assessment—by each department and agency participating in the SBU procedures review process—of the costs and budgetary considerations for all proposed changes to marking conventions, handling caveats, and other procedures pertaining to SBU information.

Efforts to formulate the required recommendations began immediately upon issuance of the Presidential Guidelines. It now continues under the auspices of a Coordinating Committee, chaired by the PM-ISE with HSC oversight, and composed of representatives from the departments of State, Defense, Justice, Transportation, Energy, and Homeland Security; ODNI; NSC; and OMB. These efforts have involved, and will continue to involve, consultation as appropriate with representatives from other affected departments and agencies, the ISOO, the Controlled Access Program Coordination Office (CAPCO), the ISC, and its State, Local, and Tribal and Private Sector Subcommittees.

The Coordinating Committee will:

- Clearly articulate the "Case for Action" as part of a general framework document that completes the requirements for Guideline 3;
- Develop and adhere to a schedule that provides for completion of work by January 2007;
- Maintain an explicit focus on homeland security information, law enforcement information, and terrorism information; and
- Ensure all recommendations identify any effect on existing statutes and regulations or ongoing legislative and regulatory activities.

[82] *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements In Support of the Information Sharing Environment* (2005), Section (2)(c)(ii).

10.2.1 Specific Implementation Action

Action 1.37 The Guideline 3 Coordinating Committee will complete its work and submit recommendations for SBU standardization through the White House policy process to the APHS-CT and the APNSA. (Planned Completion: First Quarter, CY 2007)

Chapter 11 – ISE Enabling Activities

11.1 ISE Performance Management

Performance management is the process of managing and assessing an organization's progress toward its strategic goals. Successfully used, the process and resulting information provide a foundation for guiding budget and resource allocation decisions; focusing employee endeavors as well as incentive and training programs; proposing organizational restructuring as appropriate; and recognizing program gaps and areas for further development.

Performance management across the ISE requires a collaborative effort between the PM-ISE, ISC, and the ISE participants. The ISE is an integrating environment focused on the counterterrorism mission shared by its member organizations with the recognition that each department and agency has its own unique structure and responsibilities. As envisioned, ISE performance management will reflect this two-tiered structure by including ISE-wide goals and measures to evaluate the performance of cross-cutting ISE activities, while integrating the performance goals, measures, and targets specific to individual departments and agencies. As such, the ISE Performance Management Program should complement and enhance—not replace or subsume—departmental or agency performance management efforts.

11.1.1 Progress to Date

In January 2006, the PM-ISE conducted an informal survey of ISE participants regarding terrorism information sharing goals and measures currently incorporated into their annual performance plans. In general, departments and agencies addressed information sharing issues within the context of each agency's own counterterrorism, WMD, or homeland security production or business lines and had not yet begun to address information sharing as an enterprise-wide strategic goal.

In late March 2006, the PM-ISE developed an action plan establishing a framework for all subsequent ISE performance management activities, which included:

1. An overview of the ISE performance management process;
2. A description of terminology to be used; and
3. A description of how ISE performance management will relate to OMB's initiatives for the President's Management Agenda (PMA) and to performance management activities of individual departments and agencies.

Since the IIP in January 2006 and the action plan (the response to IIP Task 10.1) in March 2006, a number of milestones that affect the approach to performance management have been realized. Achievements include progress on the ODNI's *National Intelligence Strategy* (NIS), the NCTC's substantive work to develop the *National Implementation Plan*, development of a strategy for communications and interaction between the Federal government and the SLT governments, and agreement on strategic goals for the ISE.

It is important that the ISE Performance Management Program capitalize on progress already made by individual ISE participants. Therefore, Phase 1 of the Performance Management Program will be dedicated to the following goals:

1. Developing overarching ISE performance measures;
2. Providing guidance to departments and agencies to assist in formulating agency-specific goals and measures;
3. Providing training, incentives, and mechanisms for accountability for improved and increased sharing of terrorism information;
4. Documenting progress made toward implementing the ISE during 2006 and 2007;
5. Working with ISE participants to reach a common understanding regarding ISE Performance Management Plan roles and responsibilities, as well as expectations for the ISE Performance Management Report; and
6. Implementing and refining the ISE Performance Management Plan.

11.1.2 Next Steps

With the overarching ISE strategic goals agreed to in Section 1.5, the next step is to develop the measures. As noted above, it is important to capture and capitalize on the progress already made by individual ISE members. Many programs and procedures already in place and functioning can often be replicated, expanded, or adapted to meet the larger ISE's goals.

In measuring progress against the strategic goals set for the ISE (see Section 1.5), in Phase 1 the PM-ISE will focus on:

1. Discovery of readily adaptable systems, policies, and procedures;
2. Establishment or improvement of qualitative feedback mechanisms between SLT governments and the Federal government;
3. Protection of privacy and civil liberties;
4. Establishing a mechanism to produce a uniform Federal message to SLTs, private sector, and foreign partners;

5. Core ISE training for all Federal personnel, available to SLT and private sector partners as applicable;
6. Incorporation of information sharing as a specific strategic goal in Federal strategies; and
7. Increasing the amount of data and the likelihood of finding relevant data through EDS.

The performance management deadlines set by IRTPA are not aligned with the Federal government performance management cycle. As a result, the following are recommended actions in Phase 1:

Action 1.38 To align timelines, the PM-ISE will work with ISC members and other partners to establish cut-off dates for the yearly ISE performance management reports. (Planned Completion: First Quarter, CY 2007)

Action 1.39 Federal departments and agencies will use their information sharing and terrorism-related FY06 goals, measures, and outcomes as input to the ISE Performance Management Report. (Planned Completion: Second Quarter, CY 2007)

Federal performance management cycles revolve around the PMA. Performance management plans for the 2006-2007 PMA cycle are well underway, if not already completed, in most agencies. However, since the majority of changes and improvements required to meet IRTPA goals are related to policy and procedure, there is still adequate time to ensure that the ISE is fully addressed in Federal performance plans for FY07. The PM-ISE's overarching goals for the ISE are broadly designed to encompass efforts underway or about to be implemented across Federal departments and agencies, SLT governments, and the private sector. The following are recommended actions:

Action 1.40 Federal departments and agencies will reflect ISE goals in their individual performance management plans. (Planned Completion: First Quarter, CY 2007)

Action 1.41 Federal departments and agencies will specify support to the ISE as part of their strategic plans and performance management efforts for the 2006-2007 cycle. (Planned Completion: Second Quarter, CY 2007)

Action 1.42 Federal departments and agencies will work with the PM-ISE to develop specific ISE-wide program outcome goals and measures (performance measures and threshold values), as appropriate, for the goals listed in Section 1.5. (Planned Completion: Second Quarter, CY 2007)

Action 1.43 Federal departments and agencies will provide their mid-year reviews of goals and measures to the PM-ISE (mid-year reviews are required by the Information Sharing Guidelines and Requirements). (Planned Completion: Second Quarter, CY 2007)

Significant sections of the NIP and the NIS contain major policy, procedure, and structural efforts intended to improve terrorism and related information sharing throughout the Federal government and with SLT and private sector organizations. Therefore, the PM-ISE will review interdependencies among the ISE, NIS, and NIP goals and measures.

Action 1.44 The PM-ISE, in coordination with the ODNI, will illustrate interdependencies through a "crosswalk" of the ISE, NIS, and NIP goals and measures. The "crosswalk" will be completed by or before December 2006. (Planned Completion: Fourth Quarter, CY 2006)

In the normal course of strategic management, a Federal department or agency would perform a cost-benefit analysis on any new infrastructure, program, or system it was considering creating or adjusting to ensure the new effort would meet that agency's mission needs. The requirement to build the ISE, however, is already codified in both public law and Federal policy. Performing a cost-benefit analysis of structures needed to advance the ISE would be an unnecessary additional step. Once the policy, procedural, and IT structure of the ISE is in place, cost-benefit analyses to determine the best course for improving the ISE will be examined. The PM-ISE, the ISC, and OMB will work together to determine the correct course of action on a case-by-case basis.

11.1.3 Performance Management Report

The annual ISE Performance Management Report is due from the President to Congress on a yearly basis. Following the framework outlined in this plan, Federal departments and agencies may expect a call for input into the annual Performance Management Report no later than 60 days before the PMA-prescribed deadline.

11.1.4 State, Local, Tribal, and Private Sector Performance Management

The Guideline 2 framework establishes a collaborative structure through which terrorism information will be shared between and among participating Federal, State, Local, Tribal, and private sector partners. The framework also defines a process for developing and establishing performance measures to assess progress in improving information sharing among these participants.

Action 1.45 The PM-ISE and ISC members will develop performance objectives and measures, in cooperation with SLT and Private Sector

Subcommittees, to address progress against the Guideline 2 framework. (Planned Completion: Second Quarter, CY 2007)

11.2 ISE Planning, Programming, and Budgeting

The transformation of the current ISE into one that better facilitates, coordinates, and expedites protected access to terrorism information across ISE participants requires the dedication of specific funds and resources. While existing systems and capabilities will be drawn upon to build the proposed ISE, the implementation of many of the initiatives outlined in IRTPA and the Information Sharing Guidelines and Requirements will require the reprioritization of resources to support these activities. Specific funding estimates, strategies, and proposals will need to be assessed, prioritized, cross-walked, and carefully integrated to formulate an overarching budget plan that can achieve the two-phased implementation approach presented in this plan.

The intelligence, law enforcement, defense, homeland security, and foreign affairs communities that will utilize the ISE are funded through several different mechanisms. As a result, ISE-related budget proposals and recommendations will be integrated with the various timelines and requirements associated with these funding mechanisms to impact future Federal budget cycles.

While certain execution year FY07 budget adjustments may be proposed to redirect resources to priority projects or activities, the bulk of Phase 2 activities will be expected to impact Federal departments' and agencies' FY08 and subsequent budget cycles.

11.2.1 Progress to Date

The PM-ISE, with support from OMB, has reached out to ISC departments and agencies to identify their FY06 and FY07 expenditures and planned investments for the programs, systems, and architectures that support terrorism information sharing. The information obtained from these efforts is being reviewed and analyzed by the PM-ISE and OMB, in combination with the working inventory of existing resources to identify overall ISE assets and investments, highlight redundant or overlapping investments and activities across agencies, and identify resource gaps for which focused investments could have significant impact for quick solutions and longer-term ISE operability.

The results of an initial review of the information were used to assist the PM-ISE and OMB in the development of FY08 cross-cutting terrorism information sharing budget guidance to agencies, which has been provided to ISC departments and agencies. The PM-ISE and OMB have also announced their intent to conduct ISE program reviews covering departments' and agencies' planned investment on programs and projects supporting terrorism information sharing. As Presidential direction becomes available, and further definition regarding the roles and requirements of individual ISE participants solidify, Federal departments and agencies will develop budget estimates to address the implementation of the initiatives outlined in IRTPA and the Information Sharing

Guidelines and Requirements. These estimates will address costs associated with, but not limited to:

1. Departmental assessments of privacy policies and procedures regarding the retention of protected information, the modification of such procedures, and the cataloging of agency holdings;
2. Architecture development, assessments, and alignment with the ISE Enterprise Architecture Framework;
3. Recommendations for common standards implementation, including impacts on existing and planned investments at affected departments and agencies;
4. Implementation of information assurance/security programs to provide user identity, access, auditing, protection, integrity, and availability related to terrorism information;
5. Development or modification of systems, programs, and procedures for foreign disclosure officers to make and expedite sharing decisions and to release classified information to foreign governments;
6. Creation of a national network of fusion centers and development of an Interagency Threat Assessment and Coordination Group at the NCTC to specifically address SLT and private sector needs;
7. Development and implementation of mechanisms to provide liability and anti-trust protections to the private sector for sharing information in good faith;
8. System modification; purchase of security products; and reproduction and distribution of materials associated with new SBU policies, markings, and handling procedures;
9. Training requirements and materials associated with changes in Federal government SBU designations, privacy, foreign government sharing, standards, and other information sharing activities;
10. Hardware interfaces and software upgrades to existing networks and databases that will be accessible by SBU mobile devices, and potential procurement of the additional end devices;
11. Hosting and interconnectivity of the EDS to respective agency databases; and
12. Implementation of new policies and procedures at the Federal, State, local, and tribal government levels.

As with the recommendations derived from the analysis of the Budget Data Request (BDR) and working inventory of existing resources, budget estimates concerning the implementation of IRTPA and the Presidential Information Sharing Guidelines and Requirements actions will be carefully reviewed by the PM-ISE and OMB—in consultation with the ISC—to determine how best to address and prioritize specific

recommendations in FY08 and subsequent budget cycles for the duration of the Office of the PM-ISE and any governance structure identified thereafter for this purpose. These recommendations will take into account potential impact on department- and agency-specific mission areas, and each proposed investment's alignment with and contribution to ISE goals and requirements.

11.2.2 Next Steps

A plan for gathering information from SLT organizations on their current ISE-related resources, investment plans, and budgetary requirements to identify potential resource gaps will be developed and prioritized based on input provided by the ISC SLT Subcommittee. The plan will examine how existing grant processes can be leveraged to recommend priorities for funding as it relates to SLT ISE-related requirements identified through an overall gap analysis and, eventually, to facilitate the adoption of ISE-related policies, processes, and standards. Fusion centers are an integral part of the SLT framework, and resource issues associated with these centers are addressed specifically in Chapter 7. The PM-ISE will work through the NIPP framework to determine the appropriate mechanism to address private-sector resources, investment plans, and requirements.

During the FY08 budget cycle, the PM-ISE will review the ISE investment strategy and begin planning for subsequent budget cycles. The following are recommended actions for Phase 1:

Action 1.46 The PM-ISE will support OMB, which will provide Federal departments and agencies with budget guidance for FY 2008. (Completed: Third Quarter, CY 2006)

Action 1.47 The PM-ISE will work with OMB during the fall budget process to review Federal departments' and agencies' investments with ISE priorities and OMB will provide additional budget guidance to departments and agencies, as appropriate. (Planned Completion: Fourth Quarter, CY 2006)

Action 1.48 The PM-ISE, with support from OMB and the ISC, will begin planning for subsequent budget cycles. (Planned Completion: First Quarter, CY 2007)

This page intentionally blank.

PART IV

Conclusions and Recommendations

This page intentionally blank.

Chapter 12 – Managing ISE Implementation

12.1 Managing ISE Policy, Business Processes, and Technology

Transforming the ISE requires the integration of critical policies, business processes, and technology components. A robust set of ISE policies will lay the foundation for the future ISE. Business processes will be developed based on this essential policy foundation. The combination of ISE policy and business processes will drive the necessary technology solutions.

12.1.1 ISE Policy and Business Process Management

IRTPA directs the President to "determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE."[83] Presidential Requirement 1(c) directs the DNI to "direct the PM, in consultation with the ISC, to develop, in a manner consistent with applicable law, the policies, procedures … needed to create the ISE," which "shall be reviewed through the interagency policy coordination process, and shall be submitted … by the DNI to the President for approval through the APHS-CT and the APNSA."[84] The PM-ISE has a broad, government-wide, responsibility to "plan for, oversee the implementation of, and manage the ISE," but lacks the specific authorities to issue policies, standards, business processes, and procedures to implement changes directly.[85] In Chapter 14, the PM-ISE seeks to rectify this situation by recommending that the President delegate to the PM-ISE government-wide authority to issue procedures, guidelines, functional standards, and instructions for the management, development, and operation of the ISE.

12.1.2 ISE Technology Management

Departments and agencies align information resources to support their missions. The sharing of terrorism information is a vital part of these missions. For the ISE to succeed, terrorism information sharing and interoperability with the ISE need to be integral attributes of departments' and agencies' overall information resource planning and enterprise architectures. The PM-ISE will work with the ISC and the CIOs of the ODNI, DoD, and other principal ISE stakeholders to communicate ISE requirements that may impact information resource planning. This will allow CIOs to appropriately integrate ISE requirements into their established information resource planning processes.

---

[83] IRTPA Section 1016(b)(1)(C).

[84] *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements In Support of the Information Sharing Environment* (December 16, 2005), Requirement 1(c).

[85] IRTPA Section 1016(f)(2)(A).

12.2 ISE Technical Project Management

This Section describes the project management construct for the technical implementation of the ISE. It also discusses the interface between the technical implementation and the policy and business process bodies when impediments to implementation are identified. This construct addresses only the set of common capabilities to support ISE mission users—not the ISE's required participant-specific project management activities. However, as described in Section 4.2.3, the ISC is responsible for ensuring coordination among the Federal departments and agencies participating in the ISE and can, therefore, influence appropriate project management activities and coordination within specific agencies.

12.2.1 Overall Roles and Responsibilities

Feedback and involvement from mission users and IT managers are necessary to ensure that ISE solutions add value to the counterterrorism mission. Individual ISE implementation efforts to meet specified capability requirements must be coordinated across all participating departments and agencies. The approach that will be followed is modeled on the one used to implement EDS and is tailored to manage the additional complexity of the ISE. The primary players are the PM-ISE, ISC, ITIA, and teams that support mission validation and implementation coordination. These are each discussed in detail below. The PM-ISE, in consultation with the ISC, provides overall direction. Each ITIA is responsible for management of focused implementation efforts within the constraints of the applicable, specified ISE requirements and PM-ISE direction.

Consistent with direction from IRTPA to leverage existing resources, this project management structure uses IT governance structures and technical capabilities of participating organizations. Because most existing policy and technical coordination between participating agencies focuses on supporting internal requirements, interagency bodies must be created to support process and technical coordination specifically focused on the ISE.

Accordingly, and as depicted in Figure 12.2-1, two types of teams will support the implementation of specific ISE capabilities or clusters of capabilities: Mission Validation Teams (MVT) will provide feedback and a basis for adjustments to capability requirements; and one or more Implementation Coordination Teams (ICT) will ensure that the detailed implementation strategies are viable. There may be multiple MVTs and ICTs clustered around functional capabilities or network security domains. The ITIA representative will chair the ICTs and will use that forum to issue guidance and direction to the participating departments and agencies. To ensure that mission requirements are being addressed, the ICTs will periodically recommend to the PM-ISE that a MVT should be formed to make an assessment from a user perspective.

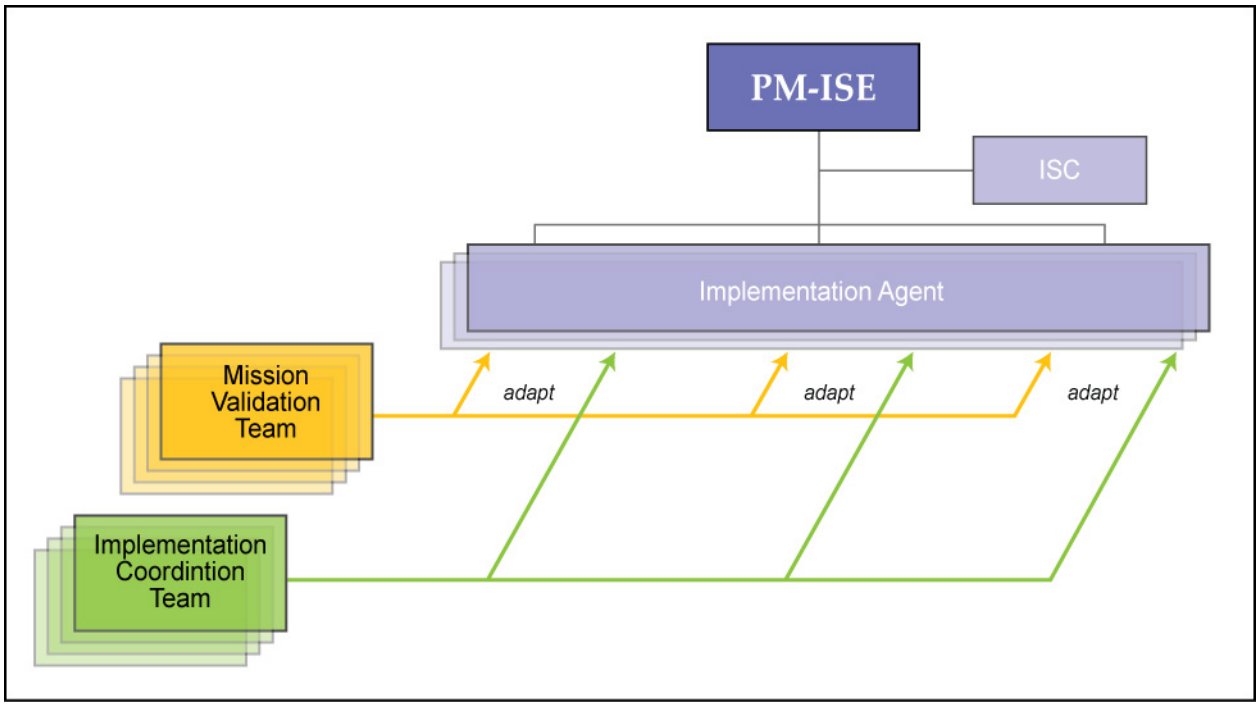


Figure 12.2-1. ISE Technical Project Management

12.3 Monitoring ISE Implementation

In addition to playing an essential role in integrating critical policies, business processes, and technology components, the PM-ISE will employ the tools needed to monitor ISE implementation progress, make mid-course adjustments as required, and elevate important issues to the senior levels when they cannot be resolved by the PM-ISE. In carrying out these responsibilities, the PM-ISE will operate in accordance with the governance structure described in Chapter 4. To ensure that this plan is executed properly, the PM-ISE will employ a number of specific management tools, including the following:

1. **ISC Subcommittees and Working Groups:** Interagency working groups are an effective mechanism for analyzing complex issues by experts and recommending solutions. All subcommittees and working groups formed to address terrorism information sharing issues must operate within the ISE governance structure. Accordingly, all working groups assigned to address actions identified in this plan will be established by and will report to the PM-ISE and the ISC. This approach will employ the ISE governance structure more effectively by focusing attention on a set of priorities, allowing more streamlined coordination, and providing a single management chain for addressing issues.
2. **Prioritization:** While all the actions identified in this plan are important, they cannot all be performed simultaneously. The Implementation Plan's two-

phase approach already provides one level of prioritization, but the ISE must dynamically respond to changing conditions and regularly review and adjust priorities as needed. Therefore, in consultation with the ISC, the PM-ISE will regularly review all implementation actions and adjust ISE priorities as required.

3. **ISE Performance Reviews:** Consistent with Presidential Requirement 2, departments and agencies will work with the PM-ISE to develop performance goals and measures that assess their capabilities in terrorism information sharing. At least semi-annually, the PM-ISE and the ISC will formally review progress in achieving the specific targets and performance goals for the ISE, and make adjustments as required.
4. **Operational Exercises:** While performance measures and milestones are *necessary* tools for managing the ISE, they are not *sufficient*. Periodic evaluation of ISE performance in an operational environment is also required. The PM-ISE will work with the departments and agencies responsible for conducting counterterrorism and homeland security exercises to ensure that information sharing capabilities are exercised and evaluated. Lessons learned through these exercises will be used to adjust ISE actions and priorities. As ISE operations mature in Phase 2 of ISE implementation, the PM-ISE will explore the use of modeling and simulation of ISE capabilities as a technique for determining ISE capabilities against operational scenarios.
5. **Evaluation Environments:** To identify new requirements, performance elements, capabilities, and standards, ISE implementation must be grounded in practical applications. Chapter 3 described the use of Federal and State evaluation environments as one mechanism for testing implementation approaches and extracting lessons learned that could be applied across the ISE.[86]

[86] Office of the PM-ISE, *Information Sharing Environment Interim Implementation Plan,* January 2006, Section 3.2.2.

Chapter 13 – ISE Expansion and Future Management Structure

13.1 Introduction

Section 1016(e) of IRTPA requires the President to submit to Congress a report containing an Implementation Plan that includes the recommendations of the PM-ISE, in consultation with the ISC:

1. Regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information (IRTPA Section 1016(e), Requirement 9); and
2. For a future management structure for the ISE, including whether the position of the PM should continue to remain in existence (IRTPA, Section 1016(e) Requirement 11).

The PM-ISE recommendations are provided below.

13.2 Expansion of ISE beyond Terrorism Information

As described in Chapter 1, IRTPA specifically defines the ISE as "an approach that facilitates the sharing of terrorism information." Accordingly, the IRTPA definition of terrorism information forms the foundation for the ISE described in this plan. Recognizing that it will be nearly impossible to predict exactly which types of information, insight, or expertise will be required to detect, prevent, prepare for, respond to, and mitigate the effects of a terrorist attack, the counterterrorism community requires a flexible, adaptable ISE that enables the sharing not only of "terrorism information," but also of "homeland security information" and certain law enforcement information. The definition of "terrorism information" is similar to and overlaps in part with the definitions of "homeland security information" and "law enforcement information."[87] All three types of information are necessary to the national effort to combat terrorism. While such overlapping terminology in legislation is not unique, it has been a significant complicating factor in the delineation of roles, missions, and responsibilities in carrying out the counterterrorism mission—a factor often referred to as the "lanes in the road."

Both Guidelines 2 and 3 of the Presidential Information Sharing Guidelines and Requirements recognized the above-mentioned overlap in definitions, and in the case of Guideline 2, the Presidential memorandum directed that a recommended framework be submitted to the President "to govern the roles and responsibilities of executive

[87] *Homeland Security Act of 2002* (Public Law 107-296), § 892(f)(1), which is now codified as 6 U.S.C. §§ 101 *et seq*. There is no statutory or universally accepted definition of the term "law enforcement information" but for purposes of the ISE only, "'law enforcement information' means any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission..."

departments and agencies pertaining to the acquisition, access, retention, production, use, management, and sharing of **homeland security information, law enforcement information, and terrorism information"** between and among federal departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector entities." Guideline 3 in turn directed that the recommendations for standardizing procedures for marking and handling SBU information should eventually apply to these same three types of information. This broadening of the ISE's scope will enable the ISE to accomplish its national security objectives.

Consequently, the PM-ISE recommends:

1. Pursuant to this Implementation Plan, and consistent with Guidelines 2 and 3, the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA section 1016(a)(4), as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland. Such additional information includes intelligence information.
2. The PM-ISE recommends deferring a decision to further expand the ISE to include additional intelligence information until policies, business practices, and systems are sufficiently mature to evaluate the impact of including such additional information, and revisiting the topic in the first annual ISE Performance Report (see Recommendation 3 below).

Should this recommendation be sustained, the actions described in this plan should be executed so they may accommodate a possible future expansion if such a decision is made. Furthermore, the PM, in consultation with the ISC, should reconsider this recommendation in June 2007, and each June thereafter, in conjunction with the development of the annual ISE Performance Report.

13.3 Future ISE Management Structure

The initial period of standing up the ISE will require substantial oversight and management, and it is now clear that this period will be longer than the two years originally allotted by IRTPA. Therefore, the PM-ISE recommends continuation of the PM-ISE and ISC for the three years covered by this plan to ensure its full implementation and to provide a fully operational ISE. Once up and running, the ISE may require less than the current PM-ISE effort to sustain it.

In several important areas—budget, performance management, standards, and enterprise architecture—implementing the actions defined in this plan will require a concerted and coordinated effort over the next three years, through June 2009. The unique position of the PM-ISE allows him/her to serve as an objective, honest broker for the ISE, focused exclusively on the national goal of improving terrorism information

sharing and collaboration. The PM-ISE can render objective views, help drive consensus, and align multiple activities into a functioning ISE.

Furthermore, the ISC provides a useful forum for Federal departments and agencies, which carry out the actual work of ISE implementation, to advise the PM-ISE on priorities and resources and also assist in the development of departmental policies and procedures that affect ISE participants. The ISC has a significant role to play in ISE implementation through Phases 1 and 2 of this plan. As with the prior recommendation, however, the PM, in consultation with the ISC, should reconsider this recommendation in June 2007, and each June thereafter, in conjunction with the development of the annual ISE Performance Report.

This page intentionally blank.

Chapter 14 – Additional PM Recommendations and Summary of Actions

14.1 Additional PM Recommendations

14.1.1 Synchronize ISE Performance Report with ISE Implementation Phases

IRTPA, Section 1016(h)(1) requires that "[n]ot later than two years after the date of the enactment … and annually thereafter, the President shall submit to Congress a report on the state of the ISE and of information sharing across the Federal Government." In accordance with that schedule, the first ISE performance report would be due in December 2006. This plan describes a two-phase ISE implementation approach with the first phase ending in June 2007. The PM believes that the performance reporting cycle and the phases of the implementation process should be synchronized so that the performance report accurately reflects the status of the action for each implementation phase. Providing the first report in June 2007 will allow the initial evaluation of performance to be made on the basis of Phase 1 of this Plan—a natural point for reflection as Phase 2 begins. Moreover, adopting the June date for subsequent reports places ISE activities in alignment with the Federal Planning, Programming, and Budgeting process, thus better supporting the development of department and agency performance measures, initial assessments of Departmental programs under the Program Assessment Rating Tool (PART), and the development of department and agency budgets. Consequently, the PM recommends that the President request that the first ISE Performance Report be submitted at the end of June 2007—rather than December 2006—and at the end of June every year thereafter.

14.1.2 Delegation of Authority

As discussed in Chapter 12, the ISE requires the integration of critical policies, business processes, and technology components. Although IRTPA identifies the PM as "responsible for information sharing across the Federal Government," neither IRTPA nor Executive Order 13388 specifically empowers any official below the President to issue the procedures, guidelines, functional standards, and instructions necessary for managing and overseeing ISE implementation.[88]

Accordingly, the need to grant the PM-ISE government-wide authority to issue procedures, guidelines, functional standards, and instructions for the management, development, and operation of the ISE, and options for doing so, should be considered. Such issuances would need to be consistent with the policies and directives issued by

[88] IRTPA, Section 1016(f)(1); In Guideline 1, however, the President did delegate to "the DNI, in coordination with the Secretaries of State, Defense, and Homeland Security, and the Attorney General," the authority to "issue …common standards" for the ISE. See *Information Sharing Guidelines and Requirements*, paragraph 2.a.

the President, the DNI, the Director of OMB, and other heads of departments and agencies having the authority to issue ISE policies and directives. Such issuance authority would not change or abrogate the authorities of the heads of such Federal departments and agencies, and all issuances would be coordinated through the ISE governance process described in Section 4.2 of this Implementation Plan. The delegation could be made consistent with the Presidential memorandum of June 2, 2005, and be through the DNI to the PM-ISE.

14.2 Summary of ISE Implementation Actions

This Implementation Plan sets forth operational details and implementation actions to create the ISE in Phase 1 (present to June 2007) and Phase 2 (June 2007 to June 2009). These actions map to the six strategic goals listed in Chapter 1:

1. Facilitate the establishment of a trusted partnership among all levels of government, the private sector, and foreign partners.
2. Promote an information sharing culture among ISE partners by facilitating the improved sharing of timely, validated, protected, and actionable terrorism information supported by extensive education, training, and awareness programs for ISE participants.
3. To the maximum extent possible, function in a decentralized, distributed, and coordinated manner.
4. Develop and deploy incrementally, leveraging existing information sharing capabilities while also creating new core functions and services.
5. Enable the Federal government to speak with one voice on terrorism-related matters, and to promote more rapid and effective interchange and coordination among Federal departments and agencies and State, local, and tribal governments, the private sector, and foreign partners, thus ensuring effective multi-directional sharing of information.
6. Ensure sharing procedures and policies protect information privacy and civil liberties.

Tables 14.2-1 and 14.2-2 summarize the actions for Phases 1 and 2 respectively.

Table 14.2-1. Phase 1 Implementation Actions

Action Number	Action	Reference	Alignment to ISE Goal(s)
ISE Operational Capabilities			
Action 1.1	The PM-ISE and ISC members will identify the alerts and notifications to be available to Federal and non-Federal ISE participants and the enabling policies and business processes necessary to implement the alert and notification capability. (Planned Completion: First Quarter, Calendar Year (CY) 2007)	43	2, 4, 5
Action 1.2	The PM-ISE and ISC members will identify existing technologies, capabilities, and programs (e.g., HSPD-12 and Federal Information Processing Standard [FIPS] 201) that provide easier user access, but still support identity management through audits, authentication, and access controls. The ISC will assess the technologies and pilot programs to determine whether or not the technologies support its user base and are suitable for ISE adoption. (Planned Completion: Second Quarter, CY 2007)	44	2, 4
Action 1.3	The PM-ISE and ISC members will determine what ISE-wide identity management capabilities are practical and develop a detailed set of requirements and Project Plan for implementation of such capabilities in a time frame consistent with technology maturity and available budgetary resources. (Planned Completion: Second Quarter, CY 2007)	45	2, 4
Action 1.4	The PM-ISE and ISC members will investigate existing or emerging capabilities that discover data and information within the Federal government and industry. The initial implementation of enterprise search will apply a search engine to index both structured and unstructured data. This activity will include the evaluation of several ongoing pilot programs using technologies that integrate data across heterogeneous networks and data stores to enhance the "findability" of relevant information and the interoperability of data and information. (Planned Completion: Second Quarter, CY 2007)	46	2, 4
Action 1.5	The PM-ISE and the ISC will work with the CDMO to establish a process to ensure that cross-domain solutions developed through this office meet the needs of ISE participants. (Planned Completion: First Quarter, CY 2007)	50	1, 2, 3, 4, 5
Action 1.6	The PM-ISE and ISC members will identify existing collaborative tools that are used and operational in the counterterrorism or other analytic or investigative communities and review the feasibility of adopting common tools for use across the ISE. (Planned Completion: First Quarter, CY 2007)	51	1, 2, 3, 4,
Action 1.7	The PM-ISE and ISC members will develop requirements to implement new and emerging collaborative technologies. (Planned Completion: Second Quarter, CY 2007)	51	1, 2, 3, 4
Action 1.8	The PM-ISE and the ISC members will implement EDS Blue, Yellow, and Green Pages in the SCI, Secret, and SBU security domains. (Planned Completion: Second Quarter, CY 2007)	53	1, 2, 3, 4
Action 1.9	The PM-ISE and the ISC members will implement EDS White Pages in the SCI and Secret security domains. (Planned Completion: Second Quarter, CY 2007)	53	1, 2, 3, 4

Action Number	Action	Reference	Alignment to ISE Goal(s)
Architecture and Standards			
Action 1.10	The PM-ISE, in consultation with the ISC, will publish a preliminary version of the ISEEA Framework Document providing the models with major portions of the ISE and their attributes. (Planned Completion: Fourth Quarter, CY 2006)	61	3,4
Action 1.11	OMB, in the FEA Business Reference Model (BRM), will include "Information Sharing" as a new government sub-function, BRM code 143, with the "Information and Technology Management" Line of Business, BRM code 404. (Planned Completion: Fourth Quarter, CY 2006)	61	3,4
Action 1.12	The PM-ISE will work with NSA, NIST, the DNI/CIO, and the CNSS on incorporating network security and information assurance policies and practices for the ISEEA Framework and associated functional standards. (Planned Completion: First Quarter, CY 2007)	62	3,4
Action 1.13	The PM-ISE, in consultation with the ISC, will publish a fully documented ISEEA Framework Document and an FEA-ISE Profile. The development process will be worked in collaboration with the OMB, department and agency CIOs, and ISC members. (Planned Completion: First Quarter, CY 2007)	62	3, 4
Action 1.14	The PM-ISE, in consultation with the ISC, will develop a configuration management process for the control and management of updates to the ISEEA Framework Document and FEA-ISE Profile. (Planned Completion: Fourth Quarter, CY 2006)	62	3, 4
Action 1.15	OMB, in the FEA Reference Models, will add the ISEEA Framework and the FEA-ISE Profile as compliance requirements in the Federal Transition Framework, a catalog of cross-agency initiatives, and the FEA Program: Enterprise Architecture Assessment Framework, the maturity assessment guide for Federal EAs. (Planned Completion: First Quarter, CY 2007)	62	3, 4
Action 1.16	DHS will work with the PM-ISE to review existing policies and procedures for ascertaining relevant and effective approaches to migrate the ISEEA Framework models and attributes into the private sector. (Planned Completion: Second Quarter, CY 2007)	62	1, 3, 4, 5
Action 1.17	The PM-ISE will convene and chair a new working group, the CTISS Working Group (CTISSWG), with representatives from all ISC members, the NCS, NIST, and the CNSS tasked with selecting and issuing information sharing standards, approved through the ISC, and formally published by NIST. The CTISS may include new standards that agencies will introduce to affect on-going investment activities as project schedules and funding permit. Future funded investments incorporating the CTISS will be compatible with the FEA and national security system EAs, and identified in normal agency submittals to the OMB. The CTISSWG will issue CTISS recommendations to the ISC for information sharing standards for non-Federal government agencies. (Planned Completion: Fourth Quarter, CY 2006)	68	3, 4

Action Number	Action	Reference	Alignment to ISE Goal(s)
Action 1.18	Departments and agencies will begin to incorporate the CTISS into investment planning, consistent with ISEEA Framework incorporation, with full CTISS incorporation into investments beginning execution in FY 2009. This will include both civil and national security system investments. Agencies will also incorporate the CTISS into information resource lifecycle processes to include CPIC processes. The CTISS will provide the source of functional standards for information sharing in the FEA's Technical and Data Reference Models. (Planned Completion: Second Quarter, CY 2007)	68	3, 4
Action 1.19	The PM-ISE, in consultation with the ISC, will develop CTISS, Version 2.0 addressing additional processes, including those with foreign partners, and releasing priority functional standards supporting suspicious activity reports (SARs), cargo management and tracking, and general identity management. (Planned Completion: Second Quarter, CY 2007)	69	3, 4, 5
Sharing with Partners Outside the Federal Government			
Action 1.20	Within 30-days of approval of the proposed Guideline 2 framework, the PM-ISE, in consultation with the ISC, will establish a Senior-level Advisory Group—consisting of ISC members or their designees—to ensure accountability, oversight, and governance for the effective operation of the framework. The advisory group will report the results of its oversight to the PM-ISE and the ISC. The advisory group will meet at least once per month during the first year of implementation. (Planned Completion: Fourth Quarter, CY 2006)	73	1, 3, 5
Action 1.21	Within seven days of approval of the proposed framework, there will be established an Implementation Team—comprised of representatives from DOD; DOI; DHS; FBI; NCTC; appropriate State, local, tribal, and private sector advocates; and the PM-ISE—to develop an implementation plan for the Interagency Threat Assessment and Coordination Group framework and to ensure its timely execution. The implementation team will develop and implement plans to notify SLT officials of the ITACG mission and responsibilities. (Planned Completion: Fourth Quarter, CY 2006)	73	1, 3, 5
Action 1.22	The ITACG Implementation Team will submit semiannual reports to the PM-ISE that identify successes and shortcomings in implementing and operating the ISE within the Guideline 2 framework and outline steps to refine and improve the framework's operation. (Planned Completion: Ongoing with first report due in the first quarter of CY 2007)	74	1, 3, 5
Action 1.23	The PM-ISE will establish a Federal Fusion Center Coordination Group to identify Federal resources to support the development of a network of State-sponsored fusion centers charged to share information at all levels of the ISE and will recommend funding options. (Planned Completion: Fourth Quarter, CY 2006)	74	1, 3, 5
Action 1.24	DOJ and DHS will work with Governors or other senior State and local leaders to designate a single fusion center to serve as the statewide or regional hub to interface with the Federal government and through which to coordinate the gathering, processing, analysis, and dissemination of terrorism information. (Planned Completion: First Quarter, CY 2007)	74	1, 3, 5

Action Number	Action	Reference	Alignment to ISE Goal(s)
Action 1.25	DOJ and DHS, to the extent possible and practicable, will assume the responsibility for technical assistance and training to support the establishment and operation of these fusion centers. (Planned Completion: First Quarter, CY 2007)	74	1, 2, 3, 5
Action 1.26	Appropriate Federal departments and agencies will assess resources and develop and coordinate plans to assign representative personnel to State and local fusion centers. These representatives will work to the extent possible to further integrate—and where appropriate collocate—Federal and State/regional resources. (Planned Completion: First Quarter, CY 2007)	74	1, 3, 5
Action 1.27	The Private Sector Subcommittee will produce a plan that implements elements of the framework as it affects the private sector. This plan must be consistent with statutes and Presidential direction and ensure that information and privacy and legal rights are adequately protected. (Planned Completion: Second Quarter, CY 2007)	77	1, 3, 5, 6
Action 1.28	The Foreign Government Information Sharing Working Group, with coordination and assistance from the PM-ISE, will develop recommendations on Privacy Act systems of records notices and routine uses for the Guideline 5 Working Group. (Planned Completion: Fist Quarter, CY 2007)	78	1, 2, 5, 6
Action 1.29	The Foreign Government Information Sharing Working Group, with coordination and assistance from the PM-ISE, will develop a checklist of issues that need to be taken into account in negotiating international agreements, including privacy protections and possible review procedures. (Planned Completion: Second Quarter, CY 2007)	78	1, 2, 5, 6
Action 1.30	Federal departments and agencies, with coordination and assistance from the PM-ISE, will encourage bilateral and multilateral efforts whenever feasible and appropriate to develop "best practices" on terrorism information sharing (e.g., protocols on what to do if there is a "hit"). (Planned Completion: Ongoing with a first progress report in the second quarter of CY 2007)	78	1, 2, 5
Promoting a Culture of Information Sharing			
Action 1.31	The DOS FSI, supported by the working group of ISC training representatives, will develop the core training module that will serve as the common educational baseline for the ISE. (Planned Completion: Second Quarter, CY 2007)	87	2
Action 1.32	The PM-ISE, in consultation with the ISC, will review departmental incentives for sharing of terrorism information and will measure their effectiveness. (Planned Completion: Second Quarter, CY 2007)	87	2
Protecting Information Privacy and Civil Liberties in the ISE			
Action 1.33	Each agency will ensure that one or more ISE Privacy Officials are designated in accordance with paragraph 12.a of the privacy guidelines. (Planned Completion: Fourth Quarter, CY 2006)	91	6
Action 1.34	The PM-ISE will establish and designate a chair for the ISE Privacy Guidelines Committee. (Planned Completion: Fourth Quarter, CY 2006)	91	6

Action Number	Action	Reference	Alignment to ISE Goal(s)
Action 1.35	The PM-ISE, in consultation with the ISE Privacy Guidelines Committee and the ISC, will establish a process for ensuring that non-Federal organizations participating in the ISE implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the Guidelines. (Planned Completion: First Quarter, CY 2007)	91	5, 6
Action 1.36	The ISE Privacy Guidelines Committee will provide an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections, to be included in the President's first annual ISE performance report. (Planned Completion: Second Quarter, CY 2007)	91	6
Improved Terrorism Information Handling			
Action 1.37	The Guideline 3 Coordinating Committee will complete its work and submit recommendations for SBU standardization through the White House policy process to the APHS-CT and the APNSA. (Planned Completion: First Quarter, CY 2007)	96	1, 2, 3, 5
ISE Enabling Activities			
Action 1.38	To align timelines, the PM-ISE will work with ISC members and other partners to establish cut-off dates for the yearly ISE performance management reports. (Planned Completion: First Quarter, CY 2007)	99	4
Action 1.39	Federal departments and agencies will use their information sharing and terrorism-related FY06 goals, measures, and outcomes as input to the ISE Performance Management Report. (Planned Completion: Second Quarter, CY 2007)	99	4
Action 1.40	Federal departments and agencies will reflect ISE goals in their individual performance management plans. (Planned Completion: First Quarter, CY 2007)	99	4
Action 1.41	Federal departments and agencies will specify support to the ISE as part of their strategic plans and performance management efforts for the 2006-2007 cycle. (Planned Completion: Second Quarter, CY 2007)	99	4
Action 1.42	Federal departments and agencies will work with the PM-ISE to develop specific ISE-wide program outcome goals and measures (performance measures and threshold values), as appropriate, for the goals listed in Section 1.5. (Planned Completion: Second Quarter, CY 2007)	99	4
Action 1.43	Federal departments and agencies will provide their mid-year reviews of goals and measures to the PM-ISE (mid-year reviews are required by the Information Sharing Guidelines and Requirements). (Planned Completion: Second Quarter, CY 2007)	100	4
Action 1.44	The PM-ISE, in coordination with the ODNI, will illustrate interdependencies through a "crosswalk" of the ISE, NIS, and NIP goals and measures. The "crosswalk" will be completed by or before December 2006. (Planned Completion: Fourth Quarter, CY 2006)	100	4
Action 1.45	The PM-ISE and ISC members will develop performance objectives and measures, in cooperation with SLT and Private Sector Subcommittees, to address progress against the Guideline 2 framework. (Planned Completion: Second Quarter, CY 2007)	100	4, 5

Action Number	Action	Reference	Alignment to ISE Goal(s)
Action 1.46	The PM-ISE will support OMB, which will provide Federal departments and agencies with budget guidance for FY 2008. (Completed: Third Quarter, CY 2006)	103	4
Action 1.47	The PM-ISE will work with OMB during the fall budget process to review Federal departments' and agencies' investments with ISE priorities and OMB will provide additional budget guidance to departments and agencies, as appropriate. (Planned Completion: Fourth Quarter, CY 2006)	103	4
Action 1.48	The PM-ISE, with support from OMB and the ISC, will begin planning for subsequent budget cycles. (Planned Completion: First Quarter, CY 2007)	103	4

Table 14.2-2. Phase 2 Implementation Actions

Action Number	Action	Reference	Alignment to ISE Goal(s)
ISE Operational Capabilities			
Action 2.1	The PM-ISE and ISC members will identify the subscription and delivery technologies required to deliver the alert and notification capability, and develop a detailed set of requirements and Project Plan for implementing alert and notification requirements. (Planned Completion: Third Quarter, CY 2007)	43	2, 4, 5
Action 2.2	The PM-ISE and ISC members will develop a detailed project plan for implementing the enterprise search technologies selected in Phase 1. (Planned Completion: Third Quarter, CY 2007)	46	2, 4
Action 2.3	The DNI CIO and the CIOs of DoD, DHS, DOJ, and the Department of State (DOS) will work with the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the Committee on National Security Systems (CNSS) to develop a common IT security framework for the ISE as described in Section 5.5.2. DOJ and DHS will ensure that this framework addresses the requirements of SLT CIOs. The results of this effort will be presented to the PM-ISE and ISC for incorporation into ISE implementation priorities. (Planned Completion: The PM-ISE and ISC members will develop a detailed project plan for implementing the technologies selected in Phase 1. (Planned Completion: Third Quarter, CY 2007)	50	1,2,3,4,5
Action 2.4	Federal departments and agencies will implement the common IT security framework developed in Phase 2 across the ISE. (Planned Completion: Third Quarter, CY 2008)	50	1, 2, 3, 4, 5
Action 2.5	Federal departments and agencies will deploy CDSs developed by the CDMO across the ISE to provide two-way cross-domain transfers of terrorism information with minimal human review. (Planned Completion: Third Quarter, CY 2008)	51	1, 2, 3, 4, 5
Action 2.6	For Sections 5.2, 5.3, 5.4, 5.6, and 5.7, the PM-ISE and ISC will review the status in all areas and reassess Phase 2 Actions. (Planned Completion: Ongoing with a first progress check to occur by First Quarter, CY 2008)	53	1, 2, 3, 4, 5
Architecture and Standards			
Action 2.7	Departments and agencies will introduce the ISEEA Framework and the FEA-ISE Profile into their EA planning affecting investments beginning execution in FY 2008. Agencies that have been identified to provide ISE Core services and transport components will include these into their planning. The DNI CIO and the DoD CIO will introduce the ISEEA Framework and FEA-ISE Profile elements into their EAs affecting national security investments beginning execution in FY 2008. Agencies will also incorporate ISEEA Framework attributes in their information resource lifecycle processes, to include capital planning and investment control (CPIC) processes. The Common Terrorism Information Sharing Standards (discussed in section 6.3) will provide the source of functional standards for information sharing in the FEA's Technical and Data Reference Models. (Planned Completion: Fourth Quarter, CY 2007)	62	3, 4

Action Number	Action	Reference	Alignment to ISE Goal(s)
Action 2.8	The PM-ISE, working with the NCS Manager, will coordinate and monitor the incorporation of the ISEEA Framework and the FEA-ISE Profile into the NCS and the CCEA planning affecting investments beginning execution in FY 2008. (Planned Completion: Fourth Quarter, CY 2007)	63	3, 4
Action 2.9	OMB will publish a new version of the Federal Transition Framework and the FEA Program: EA Assessment Framework incorporating the ISEEA Framework and the FEA-ISE Profile. (Planned Completion: Fourth Quarter, CY 2007)	63	3, 4
Action 2.10	OMB will conduct FY 2009 EA reviews, including those affecting national security systems, and ensure these reviews demonstrate incorporation of the ISEEA Framework and the FEA-ISE Profile across Federal agencies. (Planned Completion: Second Quarter, CY 2008)	63	3, 4
Action 2.11	The PM-ISE will work with DHS to promote, coordinate, and distribute the ISEEA Framework for incorporation by the private sector into new technology and products supporting terrorism information sharing. Consistent with the National Infrastructure Protection Plan, these efforts will incorporate requirements and actions specified in Sector-Specific Plans. (Planned Completion: Third Quarter, CY 2008)	63	3, 4, 5
Action 2.12	The PM-ISE will work with DOJ, DHS, and other Federal agencies to coordinate and implement the ISEEA Framework and FEA-ISE Profile elements into the fusion centers initially as translation infrastructures to SLT governments. As SLT government infrastructures transform to integrate more directly with the ISEEA Framework, the requirement for continuing to operate and maintain translation infrastructures will be reduced. (Planned Completion: Fourth Quarter, CY 2008)	63	1, 3, 4, 5
Action 2.13	The PM-ISE and ISC members will work with standards bodies and published standards to expedite efforts to identify the critical gaps in available core standards needed for developing new CTISS functional standards. (Planned Completion: Third Quarter, CY 2007)	69	3,4
Action 2.14	OMB will incorporate new standards from the CTISS into the Technical and Data Reference Models with standards compliance monitored and verified through the Federal Transition Framework and the FEA Program: Enterprise Architecture Assessment Framework. (Planned Completion. (Planned Completion: Third Quarter, CY 2007)	69	3, 4
Action 2.15	OMB will publish a new version of the Federal Transition Framework and the FEA Program: EA Assessment Framework incorporating the current CTISS. (Planned Completion: Fourth Quarter, CY 2007)	69	3, 4
Action 2.16	OMB will conduct FY 2009 EA reviews to verify incorporation of the CTISS requirements. (Planned Completion: Second Quarter, CY 2008)	69	1, 3, 4, 5
Action 2.17	The PM-ISE will work with DOJ, DHS, and other Federal departments and agencies to implement the CTISS into fusion centers to assist them in implementing the CTISS for eventual migration into SLT government infrastructures, where appropriate. Published commercial standards will be leveraged to the maximum extent practical. (Planned Completion: Second Quarter, CY 2008)	69	1, 3, 4, 5

Action Number	Action	Reference	Alignment to ISE Goal(s)
Action 2.18	The PM-ISE will work with the Department of Commerce, through NIST, to promote, coordinate, and distribute the CTISS Framework for incorporation by the private sector into new technology and products, where appropriate, supporting terrorism information sharing. (Planned Completion: Third Quarter, CY 2008)	70	1, 3, 4
Sharing with Partners Outside the Federal Government			
Action 2.19	The DNI will ensure that SLT and private sector ISE participants' needs and priorities for terrorism information are addressed in the Intelligence Community's requirements process. (Planned Completion: Ongoing with first progress report in the third quarter of CY 2007)	74	1, 3, 5
Action 2.20	The Guideline 2 Senior-level Advisory Group will ensure each designated State and/or major urban area fusion center achieves a baseline level of capability and complies with all applicable Federal laws and policies regarding the protection of information and privacy and other legal rights of individuals. Semiannual progress reports will be provided to the PM-ISE and the ISC. (Planned Completion: Ongoing with first progress report in the third quarter of CY 2007)	74	1, 3, 5, 6
Action 2.21	Statewide and major area fusion centers will ensure locally generated terrorism information is communicated to the Federal government through appropriate systems identified by Federal officials as part of ISE implementation. (Planned Completion: Ongoing with first progress report in the fourth quarter of CY 2007)	75	1, 2, 3, 5
Action 2.22	The PM-ISE, in consultation with the ISC, will review the private sector sharing plan developed in Phase 1 and identify priorities for implementation. In addition, some of the recommendations are likely to entail issues requiring executive-level decisions or legislative changes. (Planned Completion: Fourth Quarter, CY 2007)	77	1, 3, 5, 6
Action 2.23	Federal departments and agencies, with coordination and assistance from the PM-ISE, will ensure that all agencies issue internal procedures to expedite disclosure decisions, including clear written procedures on declassification and release of terrorism information to foreign governments. (Planned Completion: Second Quarter, CY 2008)	78	1, 2, 5
Action 2.24	Federal departments and agencies, with coordination and assistance from the PM-ISE, will ensure that agency Privacy Act systems of records notices and routine uses provide for terrorism information sharing with foreign partners. (Planned Completion: Second Quarter, CY 2008)	79	1, 2, 5, 6
Action 2.25	The ISC will develop appropriate common standards or protocols for electronic handling of foreign government information within the ISE to ensure that any necessary foreign government requirements are respected. (Planned Completion: Third Quarter, CY 2008)	79	1, 2, 5
Action 2.26	Federal departments and agencies, with coordination and assistance from the PM-ISE, will encourage appropriate international standardization of technological and substantive marking and handling standards. (Planned Completion: Ongoing with a first progress report in the second quarter of CY 2008)	79	1, 2, 5

Action Number	Action	Reference	Alignment to ISE Goal(s)
Action 2.27	Federal departments and agencies, with coordination and assistance from the PM-ISE, will consider impact on U.S. persons when negotiating international arrangements that involve sharing information with foreign governments. (Planned Completion: Ongoing with a first progress report in the second quarter of CY 2008)	79	1, 2, 5, 6
Action 2.28	Federal departments and agencies, with coordination and assistance from the PM-ISE, will consider possible interaction with provisions of existing agreements when negotiating new international agreements (e.g., inconsistent promises, "most favorable" treatment). (Planned Completion: Ongoing with a first progress report in the second quarter of CY 2008)	79	1, 2
Action 2.29	Federal departments and agencies, with coordination and assistance from the PM-ISE, will ensure "foreign disclosure officers" or comparable approaches are adopted by all government agencies to make and expedite disclosure decisions and provide resources to support disclosure decisions (e.g., training, information, automation tools). (Planned Completion: Fourth Quarter, CY 2008)	79	1, 2, 5
Action 2.30	Federal departments and agencies engaged in developing terrorism information sharing agreements and best practices and protocols, with coordination and assistance from the PM-ISE, will make both the registry and the text of all such agreements, as well as the texts of any best practices and protocols, available to other departments and agencies, including to the extent feasible, in electronic form, as part of the ISE. (Planned Completion: Fourth Quarter, CY 2008)	79	1, 2, 5
Action 2.31	The PM-ISE will work closely with the ISC to ensure effective and efficient implementation of the Foreign Government Information Sharing Working Group recommendations. (Planned Completion: Second Quarter, CY 2009)	80	1, 2, 5
Action 2.32	Federal departments and agencies, with coordination and assistance from the PM-ISE, will ensure agency authorities permit the full range of requirements for information sharing with foreign partners. (Planned Completion: Second Quarter, CY 2009)	80	1, 2, 5
Promoting a Culture of Information Sharing			
Action 2.33	All Federal departments and agencies responsible for terrorism information sharing will develop tailored training programs based on their unique business processes, missions, program, and policy needs. (Planned Completion: Fourth Quarter, CY 2007)	87	2
Action 2.34	DOJ, DHS, and FBI, in coordination with the ISC SLT Subcommittee and with guidance from the ISC training working group, will develop information sharing training guidelines for SLT governments. The guidelines will include the core training goals used by the departments and agencies represented on the ISC, as well as training specific to SLT and private sector operating environments and officers. (Planned Completion: Fourth Quarter, CY 2007)	87	2, 5
Action 2.35	All Federal departments and agencies will provide the PM-ISE with a copy of their agency-specific training modules, as well as a count of the number and career categories of personnel who have received training on the ISE for inclusion in the President's report on ISE performance. This information will continue to be submitted on an annual basis. (Planned Completion: Second Quarter, CY 2008)	87	2

Action Number	Action	Reference	Alignment to ISE Goal(s)
Action 2.36	Federal departments and agencies will train newly hired personnel within six months of entrance on duty. Each executive department and agency will also include information sharing in performance appraisal reviews as appropriate. (Planned Completion: Fourth Quarter, CY 2008)	87	2
Action 2.37	Federal departments and agencies will recommend modifications to internal policies, as appropriate, to accommodate the ISE training, incentive, and accountability requirements, including each will review its procedures for disciplining personnel who fail to adhere to security procedures regarding the handling and distribution of classified and controlled information. (Planned Completion: Fourth Quarter, CY 2008)	87	2
Protecting Privacy and Civil Liberties in the ISE			
Action 2.38	The ISE Privacy Guidelines Committee will provide an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections, to be included in the President's annual ISE performance report. (Planned Completion: Second Quarter, CY 2008 and 2009)	92	6
Improved Terrorism Information Handling			
Action 2.39	The PM-ISE, in consultation with the ISC, and OMB and the ODNI, will monitor existing performance measures and assess progress against the security clearance processing requirements of IRTPA Section 3001. (Planned Completion: Second Quarter, CY 2009)	94	2, 5
Action 2.40	On an ongoing basis, the PM-ISE, in consultation with the ISC, will support Information Security Oversight Office (ISOO) efforts to facilitate compliance with E.O. 12958, as amended, and its implementing directives. (Planned Completion: Ongoing)	94	2
Action 2.41	On an ongoing basis, the PM-ISE, in consultation with the ISC, will work closely with ODNI-led efforts to overhaul current C&A policies and standards for the Intelligence Community and will evaluate the applicability of these policies and standards to the broader ISE. (Planned Completion: Ongoing)	94	2

This page intentionally blank.

APPENDICES

This page intentionally blank.

Appendix 1 – IRTPA Requirements Compliance

IRTPA Requirement (Section 1016(e))		References
1	A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.	Chapters 1, 3, 5, and 6
2	A description of the impact on enterprise architectures of participating agencies.	Chapter 6
3	A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.	Chapter 11
4	A project plan for designing, testing, integrating, deploying, and operating the ISE.	Chapters 4 and 12
5	The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized. (Note: Subsection (b)(1)(C) states that, in the establishment of the ISE, the President shall, "determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.")	Chapters 5, 6, 7, 8, 10, and 12
6	Objective, system wide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.	Chapter 11
7	A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.	Chapter 10
8	A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.	Chapters 2 and 9
9	The recommendations of the Program Manager, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information.	Chapter 13
10	A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with – (a) the authority of the Director of National Intelligence under this title, and the amendments made by this title, to set standards for information sharing throughout the Intelligence Community; and (b) the authority of the Secretary of Homeland Security and the Attorney General and the roles of the Department of Homeland Security and the Attorney General, in coordinating with State, local, and tribal officials and the private sector.	Chapters 2, 3, and 12
11	The recommendations of the program manager, in consultation with the ISC, for a future management structure or the ISE, including whether the position of program manager should continue to remain in existence.	Chapter 13

This page intentionally blank.

Appendix 2 – Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004

SEC. 1016. INFORMATION SHARING.

(a) **DEFINITIONS.--**In this section:

(1) **INFORMATION SHARING COUNCIL.**--The term "Information Sharing Council'' means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection (g).

(2) **INFORMATION SHARING ENVIRONMENT; ISE.**--The terms "information sharing environment'' and "ISE'' mean an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section.

(3) **PROGRAM MANAGER.**--The term "program manager'' means the program manager designated under subsection (f).

(4) **TERRORISM INFORMATION.**--The term "terrorism information'' means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to--

(A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

(B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

(C) communications of or by such groups or individuals; or

(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

(b) **INFORMATION SHARING ENVIRONMENT.**--

(1) **ESTABLISHMENT.**--The President shall--

(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

(2) **ATTRIBUTES.**--The President shall, through the structures described in subparagraphs (B) and (C) of paragraph (1), ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that--

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations, and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties; and

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.

(c) **PRELIMINARY REPORT.**--Not later than 180 days after the date of the enactment of this Act, the program manager shall, in consultation with the Information Sharing Council--

(1) submit to the President and Congress a description of the technological, legal, and policy issues presented by the creation of the ISE, and the way in which these issues will be addressed;

(2) establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information; and

(3) conduct a review of relevant current Federal agency capabilities, databases, and systems for sharing information.

(d) **GUIDELINES AND REQUIREMENTS.**--As soon as possible, but in no event later than 270 days after the date of the enactment of this Act, the President shall--

(1) leverage all ongoing efforts consistent with establishing the ISE and issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;

(2) in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, issue guidelines that--

(A) protect privacy and civil liberties in the development and use of the ISE; and

(B) shall be made public, unless nondisclosure is clearly necessary to protect national security; and

(3) require the heads of Federal departments and agencies to promote a culture of information sharing by--

(A) reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval, consistent with applicable laws and regulations; and

(B) providing affirmative incentives for information sharing.

(e) **IMPLEMENTATION PLAN REPORT.**--Not later than one year after the date of the enactment of this Act, the President shall, with the assistance of the program manager, submit to Congress a report containing an implementation plan for the ISE. The report shall include the following:

(1) A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.

(2) A description of the impact on enterprise architectures of participating agencies.

(3) A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.

(4) A project plan for designing, testing, integrating, deploying, and operating the ISE.

(5) The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized.

(6) Objective, systemwide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.

(7) A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.

(8) A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.

(9) The recommendations of the program manager, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information.

(10) A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with--

(A) the authority of the Director of National Intelligence under this title, and the amendments made by this title, to set standards for information sharing throughout the Intelligence Community; and

(B) the authority of the Secretary of Homeland Security and the Attorney General, and the role of the Department of Homeland Security and the Attorney General, in coordinating with State, local, and tribal officials and the private sector.

(11) The recommendations of the program manager, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of program manager should continue to remain in existence.

(f) **PROGRAM MANAGER.**--

(1) **DESIGNATION.**--Not later than 120 days after the date of the enactment of this Act, with notification to Congress, the President shall designate an individual as the program manager responsible for information sharing across the Federal Government. The individual designated as the program manager shall serve as program manager during the two-year period beginning on the date of designation

under this paragraph unless sooner removed from service and replaced by the President (at the President's sole discretion). The program manager shall have and exercise government wide authority.

(2) **DUTIES AND RESPONSIBILITIES.**--

(A) **IN GENERAL.**--The program manager shall, in consultation with the Information Sharing Council--

(i) plan for and oversee the implementation of, and manage, the ISE;

(ii) assist in the development of policies, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the ISE; and

(iii) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency, and policy compliance; and regularly report the findings to Congress.

(B) **CONTENT OF POLICIES, PROCEDURES, GUIDELINES, RULES, AND STANDARDS.**--The policies, procedures, guidelines, rules, and standards under subparagraph (A)(ii) shall--

(i) take into account the varying missions and security requirements of agencies participating in the ISE;

(ii) address development, implementation, and oversight of technical standards and requirements;

(iii) take into account ongoing and planned efforts that support development, implementation and management of the ISE;

(iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community and the law enforcement community;

(v) address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments;

(vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

(vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and

(viii) ensure the protection of privacy and civil liberties.

(g) **INFORMATION SHARING COUNCIL.**--

(1) **ESTABLISHMENT.**--There is established an Information Sharing Council that shall assist the President and the program manager in their duties under this section. The Information Sharing Council shall serve during the two-year period beginning on the date of the initial designation of the program manager by the President under subsection (f)(1), unless sooner removed from service and replaced by the President (at the sole discretion of the President) with a successor body.

(2) **SPECIFIC DUTIES.**--In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall--

(A) advise the President and the program manager in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE;

(B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the ISE;

(C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the redirection of existing resources to support the ISE;

(D) identify gaps, if any, between existing technologies, programs, and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment;

(E) recommend solutions to address any gaps identified under subparagraph (D);

(F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments; and

(G) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.

(3) **CONSULTATION.**--In performing its duties, the Information Sharing Council shall consider input from persons and organizations outside the Federal Government having significant experience and expertise in policy, technical matters, and operational matters relating to the ISE.

(4) **INAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.**--The Information Sharing Council shall not be subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App.).

(h) **PERFORMANCE MANAGEMENT REPORTS.**--

(1) **IN GENERAL.**--Not later than two years after the date of the enactment of this Act, and annually thereafter, the President shall submit to Congress a report on the state of the ISE and of information sharing across the Federal Government.

(2) **CONTENT.**--Each report under this subsection shall include--

(A) a progress report on the extent to which the ISE has been implemented, including how the ISE has fared on the performance measures and whether the performance goals set in the preceding year have been met;

(B) objective system-wide performance goals for the following year;

(C) an accounting of how much was spent on the ISE in the preceding year;

(D) actions taken to ensure that procurement of and investments in systems and technology are consistent with the implementation plan for the ISE;

(E) the extent to which all terrorism watch lists are available for combined searching in real time through the ISE and whether there are consistent standards for placing individuals on, and removing individuals from, the watch lists, including the availability of processes for correcting errors;

(F) the extent to which State, tribal, and local officials are participating in the ISE;

(G) the extent to which private sector data, including information from owners and operators of critical infrastructure, is incorporated in the ISE, and the extent to which individuals and organizations outside the government are receiving information through the ISE;

(H) the measures taken by the Federal government to ensure the accuracy of information in the ISE, in particular the accuracy of information about individuals;

(I) an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections; and

(J) an assessment of the security protections used in the ISE.

(i) **AGENCY RESPONSIBILITIES.**--The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall--

(1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (f);

(2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;

(3) ensure full department or agency cooperation in the development of the ISE to implement governmentwide information sharing; and

(4) submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

(j) **AUTHORIZATION OF APPROPRIATIONS.**--There is authorized to be appropriated to carry out this section $20,000,000 for each of fiscal years 2005 and 2006.

Appendix 3 – Presidential Memorandum of December 16, 2005

SUBJECT: Guidelines and Requirements in Support of the Information Sharing Environment

Ensuring the appropriate access to, and the sharing, integration, and use of, information by Federal, State, local, and tribal agencies with counterterrorism responsibilities, and, as appropriate, private sector organizations, while protecting the information privacy and other legal rights of Americans, remains a high priority for the United States and a necessity for winning the war on terror. Consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108 458) (IRTPA), my Administration is working to create an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information (as defined in Executive Order 13388 of October 25, 2005).

Section 1016 of IRTPA supplements section 892 of the Homeland Security Act of 2002 (Public Law 107 296), Executive Order 13311 of July 29, 2003, and other Presidential guidance, which address various aspects of information access. On April 15, 2005, consistent with section 1016(f) of IRTPA, I designated the program manager (PM) responsible for information sharing across the Federal Government. On June 2, 2005, my memorandum entitled "Strengthening Information Sharing, Access, and Integration - Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment" directed that the PM and his office be part of the Office of the Director of National Intelligence (DNI), and that the DNI exercise authority, direction, and control over the PM and ensure that the PM carries out his responsibilities under IRTPA. On October 25, 2005, I issued Executive Order 13388 to facilitate the work of the PM and the expeditious establishment of the ISE and restructure the Information Sharing Council (ISC), which provides advice concerning and assists in the establishment, implementation, and maintenance of the ISE.

On June 2, 2005, I also established the Information Sharing Policy Coordination Committee (ISPCC), which is chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC), and which has the responsibilities set forth in section D of Homeland Security Presidential Directive 1 and other relevant presidential guidance with respect to information sharing. The ISPCC is the main day-to-day forum for interagency coordination of information sharing policy, including the resolution of issues raised by the PM, and provides policy analysis and recommendations for consideration by the more senior committees of the HSC and NSC systems and ensures timely responses.

Section 1016(d) of IRTPA calls for leveraging all ongoing efforts consistent with establishing the ISE, the issuance of guidelines for acquiring, accessing, sharing, and using information in support of the ISE and for protecting privacy and civil liberties in the development of the ISE, and the promotion of a culture of information sharing.

Consistent with the Constitution and the laws of the United States, including section 103 of the National Security Act of 1947, as amended, and sections 1016 and 1018 of IRTPA, I hereby direct as follows:

1. Leveraging Ongoing Information Sharing Efforts in the Development of the ISE. The ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively "resources") used for the sharing and integration of and access to terrorism information, and shall leverage those resources to the maximum extent practicable, with the objective of establishing a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information.

a. The DNI shall direct the PM to conduct and complete, within 90 days after the date of this memorandum, in consultation with the ISC, a comprehensive evaluation of existing resources pertaining to terrorism information sharing employed by individual or multiple executive departments and agencies. Such evaluation shall assess such resources for their utility and integrative potential in furtherance of the establishment of the ISE and shall identify any unnecessary redundancies.

b. To ensure that the ISE supports the needs of executive departments and agencies with counterterrorism responsibilities, and consistent with section 1021 of IRTPA, the DNI shall direct the PM, jointly with the Director of the National Counterterrorism Center (NCTC), and in coordination with the heads of relevant executive departments and agencies, to review and identify the respective missions, roles, and responsibilities of such executive departments and agencies, both as producers and users of terrorism information, relating to the acquisition, access, retention, production, use, management, and sharing of terrorism information. The findings shall be reviewed through the interagency policy coordination process, and any recommendations for the further definition, reconciliation, or alteration of such missions, roles, and responsibilities shall be submitted, within 180 days after the date of this memorandum, by the DNI to the President for approval through the Assistant to the President for Homeland Security and Counterterrorism (APHS-CT) and the Assistant to the President for National Security Affairs (APNSA). This effort shall be coordinated as appropriate with the tasks assigned under the Guidelines set forth in section 2 of this memorandum.

c. Upon the submission of findings as directed in the preceding paragraph (1(b)), the DNI shall direct the PM, in consultation with the ISC, to develop, in a manner consistent with applicable law, the policies, procedures, and architectures needed to create the ISE, which shall support the counterterrorism missions, roles, and responsibilities of executive departments and agencies. These policies, procedures, and architectures shall be reviewed through the interagency policy coordination process, and shall be submitted, within 180 days after the

submission of findings as directed in the preceding paragraph (1(b)), by the DNI to the President for approval through the APHS-CT and the APNSA.

2. Information Sharing Guidelines. Consistent with section 1016(d) of IRTPA, I hereby issue the following guidelines and related requirements, the implementation of which shall be conducted in consultation with, and with support from, the PM as directed by the DNI:

a. Guideline 1 - Define Common Standards for How Information is Acquired, Accessed, Shared, and Used Within the ISE

The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities.

Consistent with Executive Order 13388 and IRTPA, the DNI, in coordination with the Secretaries of State, Defense, and Homeland Security, and the Attorney General, shall develop and issue, within 90 days after the date of this memorandum, common standards (i) for preparing terrorism information for maximum distribution and access, (ii) to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE while safeguarding such information and protecting sources and methods from unauthorized use or disclosure, (iii) for implementing legal requirements relating to the handling of specific types of information, and (iv) that include the appropriate method for the Government-wide adoption and implementation of such standards. Such standards shall accommodate and reflect the sharing of terrorism information, as appropriate, with State, local, and tribal governments, law enforcement agencies, and the private sector. Within 90 days after the issuance of such standards, the Secretary of Homeland Security and the Attorney General shall jointly disseminate such standards for use by State, local, and tribal governments, law enforcement agencies, and the private sector, on a mandatory basis where possible and a voluntary basis where not. The DNI may amend the common standards from time to time as appropriate through the same process by which the DNI issued them.

b. Guideline 2 - Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector

Recognizing that the war on terror must be a national effort, State, local, and tribal governments, law enforcement agencies, and the private sector must have the opportunity to participate as full partners in the ISE, to the extent consistent with applicable laws and executive orders and directives, the protection of

national security, and the protection of the information privacy rights and other legal rights of Americans.

Within 180 days after the date of this memorandum, the Secretary of Homeland Security and the Attorney General, in consultation with the Secretaries of State, Defense, and Health and Human Services, and the DNI, and consistent with the findings of the counterterrorism missions, roles, and responsibilities review under section 1 of this memorandum, shall:

(i) perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing with State, local, and tribal governments, law enforcement agencies, and the private sector; and

(ii) submit to the President for approval, through the APHS-CT and the APNSA, a recommended framework to govern the roles and responsibilities of executive departments and agencies pertaining to the acquisition, access, retention, production, use, management, and sharing of homeland security information, law enforcement information, and terrorism information between and among such departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector organizations.

c. Guideline 3 - Standardize Procedures for Sensitive But Unclassified Information

To promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, procedures and standards for designating, marking, and handling SBU information (collectively "SBU procedures") must be standardized across the Federal Government. SBU procedures must promote appropriate and consistent safeguarding of the information and must be appropriately shared with, and accommodate and reflect the imperative for timely and accurate dissemination of terrorism information to, State, local, and tribal governments, law enforcement agencies, and private sector entities. This effort must be consistent with Executive Orders 13311 and 13388, section 892 of the Homeland Security Act of 2002, section 1016 of IRTPA, section 102A of the National Security Act of 1947, the Freedom of Information Act, the Privacy Act of 1974, and other applicable laws and executive orders and directives.

(i) Within 90 days after the date of this memorandum, each executive department and agency will conduct an inventory of its SBU procedures, determine the underlying authority for each entry in the inventory, and provide an assessment of the effectiveness of its existing SBU procedures. The results of each inventory shall be reported to the DNI, who shall provide the compiled results to the Secretary of Homeland Security and the Attorney General.

(ii) Within 90 days after receiving the compiled results of the inventories required under the preceding paragraph (i), the Secretary of Homeland Security and the Attorney General, in coordination with the Secretaries of State, Defense, and Energy, and the DNI, shall submit to the President for approval recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information in the manner described in paragraph (iv) below.

(iii) Within 1 year after the date of this memorandum, the DNI, in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, Homeland Security, Health and Human Services, and the Attorney General, and in consultation with all other heads of relevant executive departments and agencies, shall submit to the President for approval recommendations for the standardization of SBU procedures for all types of information not addressed by the preceding paragraph (ii) in the manner described in paragraph (iv) below.

(iv) All recommendations required to be submitted to the President under this Guideline shall be submitted through the Director of the Office of Management and Budget (OMB), the APHS-CT, and the APNSA, as a report that contains the following:

(A) Recommendations for government-wide policies and procedures to standardize SBU procedures;

(B) Recommendations, as appropriate, for legislative, policy, regulatory, and administrative changes; and

(C) An assessment by each department and agency participating in the SBU procedures review process of the costs and budgetary considerations for all proposed changes to marking conventions, handling caveats, and other procedures pertaining to SBU information.

(v) Upon the approval by the President of the recommendations submitted under this Guideline, heads of executive departments and agencies shall ensure on an ongoing basis that such recommendations are fully implemented in such department or agency, as applicable. The DNI shall direct the PM to support executive departments and agencies in such implementation, as well as in the development of relevant guidance and training programs for the standardized SBU procedures.

d. Guideline 4 - Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners

The ISE must support and facilitate appropriate terrorism information sharing between executive departments and agencies and foreign partners and allies. To that end, policies and procedures to facilitate such informational access and

exchange, including those relating to the handling of information received from foreign governments, must be established consistent with applicable laws and executive orders and directives.

Within 180 days after the date of this memorandum, the Secretary of State, in coordination with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, the Attorney General, and the DNI, shall review existing authorities and submit to the President for approval, through the APHS-CT and the APNSA, recommendations for appropriate legislative, administrative, and policy changes to facilitate the sharing of terrorism information with foreign partners and allies, except for those activities conducted pursuant to sections 102A(k), 104A(f), and 119(f)(1)(E) of the National Security Act of 1947.

e. Guideline 5 - Protect the Information Privacy Rights and Other Legal Rights of Americans

As recognized in Executive Order 13353 of August 27, 2004, the Federal Government has a solemn obligation, and must continue fully, to protect the legal rights of all Americans in the effective performance of national security and homeland security functions. Accordingly, in the development and use of the ISE, the information privacy rights and other legal rights of Americans must be protected.

(i) Within 180 days after the date of this memorandum, the Attorney General and the DNI, in coordination with the heads of executive departments and agencies that possess or use intelligence or terrorism information, shall (A) conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans, (B) develop guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information, and (C) submit such guidelines to the President for approval through the Director of OMB, the APHS-CT, and the APNSA. Such guidelines shall not be inconsistent with Executive Order 12333 and guidance issued pursuant to that order.

(ii) Each head of an executive department or agency that possesses or uses intelligence or terrorism information shall ensure on an ongoing basis that (A) appropriate personnel, structures, training, and technologies are in place to ensure that terrorism information is shared in a manner that protects the information privacy and other legal rights of Americans, and (B) upon approval by the President of the guidelines developed under the preceding subsection (i), such guidelines are fully implemented in such department or agency.

3. Promoting a Culture of Information Sharing. Heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information.

Accordingly, each head of an executive department or agency that possesses or uses intelligence or terrorism information shall:

a. within 90 days after the date of this memorandum, designate a senior official who possesses knowledge of the operational and policy aspects of information sharing to (i) provide accountability and oversight for terrorism information sharing within such department and agency, (ii) work with the PM, in consultation with the ISC, to develop high level information sharing performance measures for the department or agency to be assessed no less than semiannually, and (iii) provide, through the department or agency head, an annual report to the DNI on best practices of and remaining barriers to optimal terrorism information sharing;

b. within 180 days after the date of this memorandum, develop and issue guidelines, provide training and incentives, and hold relevant personnel accountable for the improved and increased sharing of terrorism information. Such guidelines and training shall seek to reduce obstructions to sharing, consistent with applicable laws and regulations. Accountability efforts shall include the requirement to add a performance evaluation element on information sharing to employees' annual Performance Appraisal Review, as appropriate, and shall focus on the sharing of information that supports the mission of the recipient of the information; and

c. bring to the attention of the Attorney General and the DNI, on an ongoing basis, any restriction contained in a rule, regulation, executive order or directive that significantly impedes the sharing of terrorism information and that such department or agency head believes is not required by applicable laws or to protect the information privacy rights and other legal rights of Americans. The Attorney General and the DNI shall review such restriction and jointly submit any recommendations for changes to such restriction to the APHS-CT and the APNSA for further review.

4. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide assistance and information to the DNI and the PM in the implementation of this memorandum.

5. This memorandum:

a. shall be implemented in a manner consistent with applicable laws, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;

b. shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;

c. shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

d. is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.

GEORGE W. BUSH

Appendix 4 – Definitions

Agency	The term "agency" has the meaning set forth for the term "executive agency" in section 105 of title 5, United States Code (*i.e.*, an Executive department, a Government corporation, and an independent establishment), together with the Department of Homeland Security, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office. [E.O. 13388 Section (6)(a) and 5 U.S.C. 105]
Communities of Interest	"Communities of Interest" (COI) are defined in the *National Information Exchange Model (NIEM) CONOPS*, October 2004, as a collaborative group of users who require a shared vocabulary to exchange information in pursuit of common goals, interests, and business objectives.
Controlled Unclassified Information (CUI)	As used in this plan, Controlled Unclassified Information (CUI) is defined as categories of unclassified information that require controls that protect it from public release, both to safeguard the civil liberties and legal rights of U.S. citizens, and to deny information advantage to those who threaten the security of the nation.
Enabling Technology	As used in this plan, the term "enabling technology" refers to any technological capability used to support ISE policies or business processes. [Chapter 5]
Enterprise Architecture	A strategic information asset base, which defines the mission, the information necessary to perform the mission and the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. [Endorsed definition from the Federal CIO Council]
Enterprise Search	As used in this plan, the term "enterprise search" is defined as the act of searching content to discover data, information, and knowledge wherever it exists. [Chapter 5]
Federal Enterprise Architecture	A business-driven framework that defines and aligns Federal business functions and supporting technology using a set of 5 common models (performance, business, services, data, and technology).
Foreign Partners	As used in this plan, the term "foreign partners" refers to non-U.S. government organizations that participate in the ISE. The term "foreign governments" is a general term that includes

	foreign governments and their sub-components, such as individual ministries or foreign provincial or local authorities. While this Plan focuses in particular on foreign governments, however, the same conclusions and recommendations may generally be applicable to other foreign information sharing partners. Such foreign partners include, for example, regional inter-governmental organizations such as the European Union (EU), international organizations composed of governments such as the United Nations (UN) and the International Criminal Police Organization (INTERPOL), certain other entities with recognized comparable international status and certain foreign private entities such as port operators, foreign airlines, and other logistics providers. [Foreign Government Information Sharing Working Group Report]
Fusion Center	A center established by State and local governments designed to coordinate the gathering, analysis, and dissemination of law enforcement, public-safety, and terrorism information. [*Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*]
Homeland Security Information	Any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act. [Section 892(f)(1) of the Homeland Security Act (6 U.S.C. 482(f)(1))]
Information Sharing Council (ISC)	The term ‘‘Information Sharing Council’’ (ISC) means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection 1016(g) of the IRTPA. [Extracted from IRTPA 1016(a)(1)] E.O. 13388, which superseded E.O. 13356, established the Information Sharing Council.
Information Sharing Environment (ISE)	The terms ‘‘information sharing environment’’ and ‘‘ISE’’ mean an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section [1016]. [IRTPA 1016(a)(2)] The ISE is to provide and facilitate the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. [Extracted from IRTPA 1016(b)(2)] To the greatest extent practicable, the ISE is to provide the

	functional equivalent of, or otherwise support, a decentralized, distributed, and coordinated environment that— (A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector; (B) ensures direct and continuous online electronic access to information; (C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations, and operations; (D) builds upon existing systems capabilities currently in use across the Government; (E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security; (F) facilitates the sharing of information at and across all levels of security; (G) provides directory services, or the functional equivalent, for locating people and information; (H) incorporates protections for individuals' privacy and civil liberties; and (I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls. [Extracted from IRTPA 1016(b)(2)]
ISE Participant	The term "ISE participant" is defined as any Federal, State, local, or tribal government organization; private sector entity; or foreign government organization that participates in the ISE. [Chapter 1]
Law Enforcement Information	For the purposes of the ISE only, any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification,

	detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance. [Extracted from the Recommendations for Presidential Guideline 2]
Local Government	The term “local government” means-- (A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity. [Homeland Security Act of 2002, 6 U.S.C. 101]
Outcome Measures	Outcomes describe the intended result of carrying out a program or activity. They define an event or condition that is external to the program or activity and that is of direct importance to the intended beneficiaries and/or the public. For a tornado warning system, outcomes could be the number of lives saved and property damage averted. While performance measures must distinguish between outcomes and outputs, there must be a reasonable connection between them, with outputs supporting (i.e., leading to) outcomes in a logical fashion. [OMB A-11]
Private Sector Partners	As used in this plan, the term “private sector partners” includes vendors, owners, and operators of products and infrastructures participating in the ISE.
Program Manager	The term ‘‘program manager’’ means the program manager designated under subsection 1016(f) of the IRTPA, who is responsible for information sharing across the Federal Government and shall, in consultation with the Information Sharing Council, plan for and oversee the implementation of, and manage, the ISE. [Extracted from IRTPA 1016(a)(3) and 1016(f)]
Security Domains	As used in this plan, the term “Security Domains” refers to three security levels—Sensitive Compartmented Information (SCI), Secret, and Sensitive but Unclassified (SBU)—across which the ISE must operate.

State	The term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. [Homeland Security Act of 2002, 6 U.S.C. 101]
Terrorism Information	The term “terrorism information” means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to— (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals. [IRTPA 1016(a)(4)]
United States	The term “United States”, when used in a geographical sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States, and any waters within the jurisdiction of the United States. [Homeland Security Act of 2002, 6 U.S.C. 101]

This page intentionally blank.

Appendix 5 – Acronyms

APHS-CT	Assistant to the President for Homeland Security and Counterterrorism
APNSA	Assistant to the President for National Security Affairs
BDR	Budget Data Request
BRM	Business Reference Model
C&A	Certification and Accreditation
CAPCO	Controlled Access Program Coordination Office
CCEA	Continuity Communications Enterprise Architecture
CDMO	Cross Domain Management Office
CDS	Cross Domain Solution
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CONOPS	Concept of Operations
COP	Committee of Principals
CPIC	Capital Planning and Investment Control
CTISS	Common Terrorism Information Sharing Standards
CTISSWG	Common Terrorism Information Sharing Standards Working Group
CUI	Controlled Unclassified Information
CY	Calendar Year
DCMI	Dublin Core Metadata Initiative
DDMS	DoD Discovery Metadata Specification
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOC	Department of Commerce
DOD	Department of Defense
DODEA	Department of Defense Enterprise Architecture
DOJ	Department of Justice
DOS	Department of State

EA	Enterprise Architecture
EDS	Electronic Directory Services
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FIG	Field Intelligence Group
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
FSI	Foreign Service Institute
FY	Fiscal Year
GAO	Government Accountability Office
GIG	Global Information Grid
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICEA	Intelligence Community Enterprise Architecture
ICT	Implementation Coordination Team
IIP	Interim Implementation Plan
IOC	Initial Operating Capability
IP	Implementation Plan
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISAC	Information Sharing and Analysis Center
ISC	Information Sharing Council
ISE	Information Sharing Environment
ISEEA	Information Sharing Environment Enterprise Architecture
ISEEAWG	Information Sharing Environment Enterprise Architecture Working Group
ISM	Information Security Markings
ISO	International Organization for Standardization

ISOO	Information Security Oversight Office
ISPCC	Information Sharing Policy Coordination Committee
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
ITIA	Information Technology Implementation Agent
JTTF	Joint Terrorism Task Force
JXDM	Justice XML Data Model
MIP	Military Intelligence Program
MVT	Mission Validation Team
NCS	National Communications System
NCTC	National Counterterrorism Center
NIAC	National Infrastructure Advisory Council
NIEM	National Information Exchange Model
NIP	National Implementation Plan
NIP	National Intelligence Program
NIPP	National Infrastructure Protection Plan
NIS	National Intelligence Strategy
NIST	National Institute of Standards and Technology
NOL	National Counterterrorism Center Online
NSA	National Security Agency
NSC	National Security Council
NS/EP	National Security and Emergency Preparedness
NSPD	National Security Presidential Directive
OASIS	Organization for the Advancement of Structured Information Standards
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PART	Program Assessment Rating Tool
PCC	Policy Coordination Committee
PCLOB	Privacy and Civil Liberties Oversight Board
PM	Program Manager

PMA	President's Management Agenda
RAIS PCC	Records Access and Information Security Policy Coordination Committee
SAR	Suspicious Activity Report
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SLT	State/local/tribal
SOAP	Simple Object Access Protocol
TSC	Terrorist Screening Center
TTIC	Terrorist Threat Integration Center
TWPDES	Terrorist Watchlist Person Data Exchange Standard
UDDI	Universal Description, Discovery, and Integration
U.S.C.	United States Code
WMD	Weapons of Mass Destruction
W3C	World Wide Web Consortium
XML	Extensible Mark-Up Language

Appendix 6 – ISC Membership

Program Manager for the Information Sharing Environment (Chair)

Central Intelligence Agency

Department of Commerce

Department of Defense – Joint Chiefs of Staff

Department of Defense – Office of the Secretary of Defense

Department of Energy

Department of Health and Human Services

Department of Homeland Security

Department of the Interior

Department of Justice

Department of State

Department of Transportation

Department of the Treasury

Director of National Intelligence

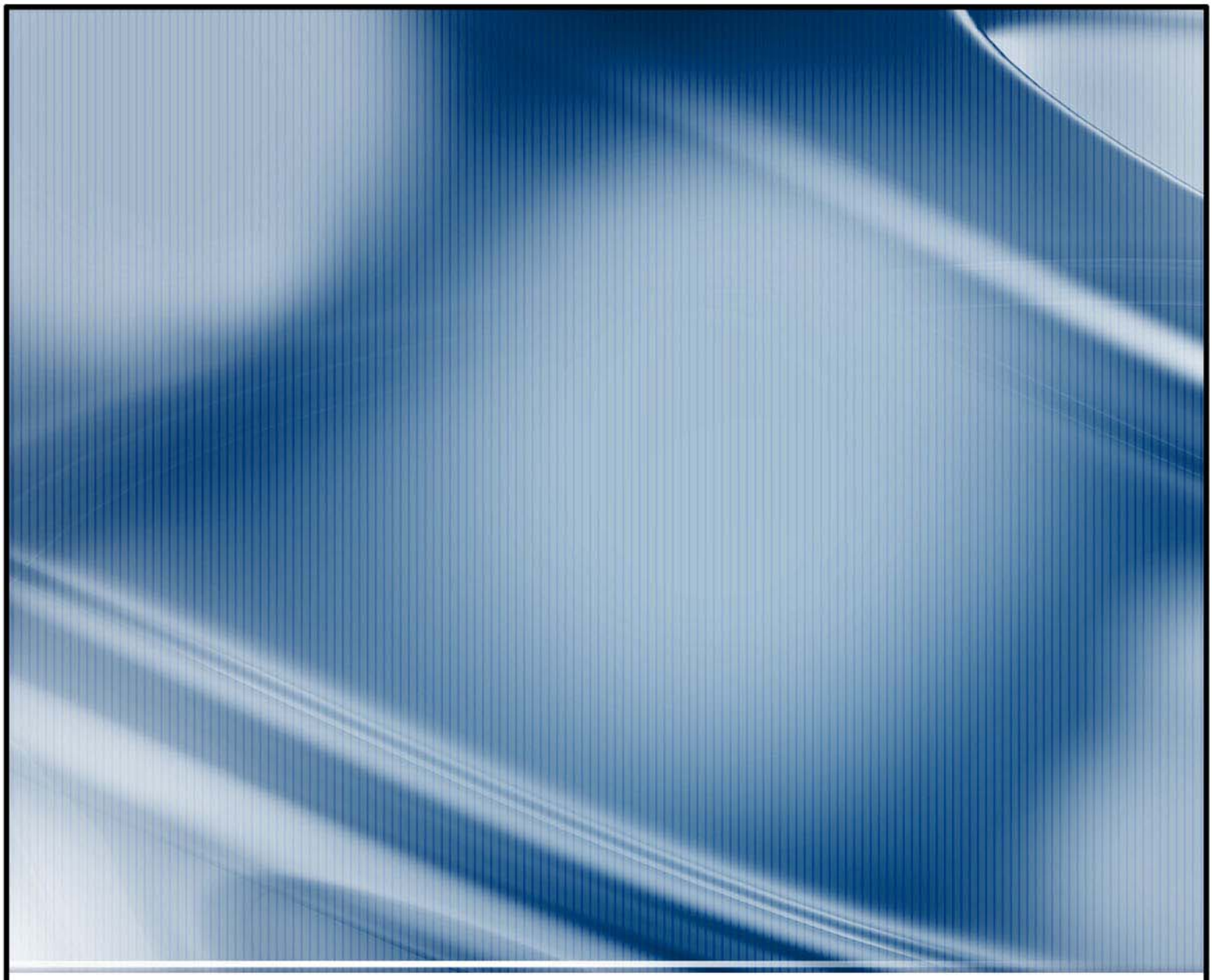
Federal Bureau of Investigation

National Counterterrorism Center

Office of Management and Budget

This page intentionally blank.

This page intentionally blank.



Office of the Director of National Intelligence
Attention: Program Manager, Information Sharing Environment
Washington, D.C. 20511

(202) 331-2490

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