

ISE Profile and Architecture Implementation Strategy

Version 2.0

June 2009



INFORMATION SHARING ENVIRONMENT PROFILE AND ARCHITECTURE IMPLEMENTATION STRATEGY, VERSION 2.0

Prepared by the
Program Manager, Information Sharing Environment

INFORMATION SHARING ENVIRONMENT GUIDANCE (ISE-G)
INFORMATION SHARING ENVIRONMENT (ISE)
PROFILE AND ARCHITECTURE IMPLEMENTATION STRATEGY (PAIS)
VERSION 2.0

1. Authority. The Homeland Security Act of 2002, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Presidential Memorandum dated April 10, 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated December 16, 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); Director of National Intelligence (DNI) memorandum dated May 2, 2007 (Program Manager's Responsibilities); Executive Order 13388; and other applicable provisions of law, regulation, or policy.

2. Purpose. This *ISE PAIS* issuance provides guidance to ISE participants for developing their information sharing segment architecture and trusted repository for information that will be shared in the ISE (ISE Shared Space). A companion document to the *ISE EAF*, this *ISE PAIS* supports efforts to build upon and leverage existing policies, business processes, and technologies in use by Federal, State, local and tribal governments that support information sharing across the ISE community in a manner that fully protects the legal rights of all United States persons. This *ISE PAIS* provides guidance to ISE participants as they seek to implement information sharing capabilities, connect to other ISE participants, expose data, and access ISE data and services.

This *ISE PAIS Version 2.0* supersedes *ISE PAIS Version 1.0* issued May 2008. This newest version of the *ISE PAIS* addresses key requirements of section 1016 of the IRTPA and provides more specific guidance for Federal Chief Information Officers, Chief Technology Officers, Chief Architects, and network managers involved in integrating their information sharing capabilities into the ISE.

3. Applicability. This *ISE PAIS* is applicable to all ISE communities: defense, foreign affairs, homeland security, intelligence, and law enforcement; the Information Sharing Council (ISC) members and their departments and agencies; and departments or agencies that possess or use ISE mission business-related information, operate a system that supports or interfaces to the ISE, or otherwise participate (or expect to participate) in the ISE, as specified in Section 1016(i) of the IRTPA, as amended.

4. References. *ISE Implementation Plan*, November 2006; *ISE Enterprise Architecture Framework (EAF)*, Version 2.0, September 2008; *Initial Privacy and Civil Liberties Analysis for the Information Sharing Environment*, Version 1.0, September 2008; *ISE-AM-300: Common Terrorism Information Standards Program*, 31 October 2007; *Common Terrorism Information Sharing Standards Program Manual*, Version 1.0, October 2007; *National Strategy for*

Information Sharing, October 2007; *ISE Profile and Architecture Implementation Strategy*, Version 1.0, May 2008; National Information Exchange Model, *Concept of Operations*, Version 0.5, 9 January 2007; 28 Code of Federal Regulations (CFR) Part 23; Office of Management and Budget (OMB), *Federal Transition Framework Catalog of Cross Agency Initiatives*, Version 1.0, December 2006; *Presidential Memorandum to Executive Departments and Agencies*, 9 May 2008, (Designation and Sharing of Controlled Unclassified Information); *Nationwide Suspicious Activity Reporting Initiative: Concept of Operations*, Version 1.0, December 2008; *ISE Suspicious Activity Reporting Evaluation Environment Segment Architecture*, December 2008.

5. Definitions.

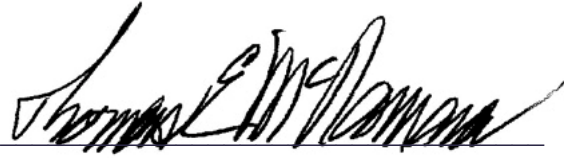
- a. Federal Segment Architecture Methodology (FSAM) - a step-by-step process for developing and using segment architectures that was developed by distilling proven best practices from across Federal agencies.
- b. ISE Enterprise Architecture Framework (EAF) - presents a logical structure of ISE business processes, information flows, and relationships, services, and high-level data packet descriptions and exchange relationships.
- c. ISE Implementation Agent - refers to an organization responsible for providing infrastructure and services in the ISE Core Segment.
- d. ISE participant - any Federal, State, local, or tribal government organization, private sector entity, or foreign government organization (to include employees) that participates in the ISE.
- e. ISE Profile and Architecture Implementation Strategy (PAIS) - a guide for ISE participants that describes what each should do to connect to the ISE, expose data to the ISE, build their ISE Shared Space, and access data and services provided by the ISE.
- f. ISE Shared Space - standardizes terrorism information, as defined through the Common Terrorism Information Sharing Standards (CTISS) and is made available by one ISE participant to others, as appropriate. Additionally, ISE participants may create or use an ISE Shared Space to make their services and data accessible, as appropriate, to other ISE participants.
- g. Segment Architecture - the business-driven approach of logically documenting the set of business and information requirements, outcomes, and constraints that lay the foundation for building executable operational solutions (or systems) that meet or exceed mission performance goals for a particular line of business (e.g., Information Sharing) and are derived from a concept of operations.
- h. Solution Architecture - the structured, technical documents, derived from Segment Architectures, which are scoped to describe the particular functions or processes to be implemented; identify methods for achieving operational outcomes; and define specific IT assets, applications, and components for procurement and implementation. Solution Architectures do not specifically identify vendors or specific vendor items as these are generally identified in subsequent specification documents and/or procurement orders.

6. Guidance. This *ISE PAIS* is established to assist in coordinating activities and development of individual ISE participants' enterprise and Information Sharing Segment Architectures to drive the planning and management of those businesses and information resources that define the nationwide ISE capability. This *ISE PAIS* provides greater detail than the *Federal Enterprise Architecture Framework (FEAF)*, but does not address details at the operational level, which is appropriate for individual departments and agencies to include in enterprise architectures, and especially Information Sharing Segment Architectures.

7. Responsibilities.

- a. The Program Manager, Information Sharing Environment (PM-ISE), in consultation with the Information Sharing Council (ISC), shall:
 - 1) Work with ISE participants, through the ISC Chief Architects' Roundtable, to publish, maintain, administer, and manage use of the *ISE PAIS*; and
 - 2) Monitor the implementation and use of the *ISE PAIS* and subsequent updates in alignment with Federal Enterprise Architecture (FEA) assessment guidance.
- b. Each ISE participant shall:
 - 1) Incorporate *ISE PAIS* attributes into their information systems to interface with the ISE, and any subsequent implementation guidance of it into budget activities associated with relevant current (operational) mission specific programs, systems, or initiatives (e.g., operations and maintenance {O&M} or enhancements);
 - 2) Incorporate the *ISE PAIS* and any subsequent implementation guidance into budget activities associated with future or new development efforts for relevant mission-specific systems or initiatives (e.g., development, modernization, or enhancement {DME});
 - 3) Incorporate the *ISE PAIS* attributes into agencies transition planning strategy for enterprise architectures or Information Sharing Segment Architectures development and implementation;
 - 4) Abide by ISE performance goals and strategies while implementing the *ISE PAIS*; and
 - 5) Abide by ISE privacy and civil liberties policies while implementing the *ISE PAIS*.

8. Effective Date and Expiration. This ISE Guidance is effective immediately and will remain in effect until superseded or cancelled.

A handwritten signature in black ink, appearing to read "Thomas E. McNamara", written over a horizontal line.

Thomas E. McNamara
Program Manager for the
Information Sharing Environment

Date: June 24, 2009

Attachment(s):

ISE PAIS Version 2.0

INFORMATION SHARING ENVIRONMENT PROFILE AND ARCHITECTURE IMPLEMENTATION STRATEGY, VERSION 2.0

**Prepared by the
Program Manager, Information Sharing Environment**

June 2009



This page intentionally blank.

TABLE OF CONTENTS

List of Figures	v
List of Tables	vi
Executive Summary	vii
Chapter 1 – Introduction	1
1.1 Purpose and Scope	1
1.2 Supporting Architecture Concepts	1
1.3 Testing and Evaluation	4
1.4 Privacy and Civil Liberties.....	5
Chapter 2 – ISE Architecture Implementation Considerations	7
2.1 Information Security and Assurance (ISA).....	7
2.2 Risk Management Framework (RMF).....	8
2.3 ISE Trust Relationships	11
2.4 Systems Validation and Testing for the ISE.....	13
2.5 Training.....	14
Chapter 3 – ISE Architecture Implementation Life Cycle.....	15
3.1 Introduction	15
3.2 Federal Segment Architecture Methodology.....	15
3.3 FSAM and ISE Architecture Implementation Life Cycle Alignment.....	17
Chapter 4 – ISE Shared Spaces Development and Implementation	29
4.1 Overview.....	29
4.2 System/Software Development Life Cycle	30
4.3 ISE Shared Space Requirements	32
4.4 ISE Shared Space Security	36
4.5 Hardware/Software Configuration	38
4.6 Software Development.....	41
4.7 System Integration and Testing	42
4.8 Other Implementation Considerations.....	42
Chapter 5 – Case Study: Washington, DC Metropolitan Police Department (MPD) ISE Shared Space.....	45
5.1 Overview.....	45
5.2 DC MPD’s Alert Management System	46
5.3 Data Analysis and Migration Process	46
5.4 MPD’s Implementation of ISE Shared Space	46
5.5 Project Results.....	53
5.6 Future Considerations.....	54
Appendix A – Architecture and Infrastructure Committee Letter	A-1
Appendix B – Acronyms	B-1
Appendix C – Bibliography	C-1
Appendix D – Glossary	D-1
Appendix E – ISE Business Processes	E-1

Appendix F – ISE Shared Spaces F-1
Appendix G – ISE Shared Space Information Security and Assurance
(ISA) Considerations G-1

LIST OF FIGURES

Figure 2-1.	ISE EAF Implementer's View	8
Figure 2-2.	The ISE Risk Management Framework (RMF)	9
Figure 2-3.	Building Trust Relationships through Security Due Diligence and Reciprocity	12
Figure 3-1.	FSAM Methodology	16
Figure 3-2.	ISE Architecture Implementation Life Cycle	17
Figure 4-1.	Conceptual ISE Shared Space implementation	35
Figure 5-1.	Detailed Component Layout	47
Figure 5-2.	Example: ISE Shared Space Server Database Entity Relationship Diagram.....	50
Figure 5-3.	High Level Network Diagram	53
Figure G-1.	ISE Core Security Operations Center Monitoring	G-1
Figure G-2.	ISE Shared Space Logical Diagram	G-3
Figure G-3.	ISE Shared Space Inner Security Boundary Logical Diagram	G-8
Figure G-4.	ISE Shared Space Outer Security Boundary Logical Diagram	G-10

LIST OF TABLES

Table ES-1. ISE Architecture Program Documentation	viii
Table 1-1. Levels of Architecture	4
Table 2-1. ICD 503 Purpose	11
Table 2-2. ISA Five Elements of Trust	13
Table 4-1. ISE Shared Space Hardware Requirements.....	38
Table 5-1. Hardware Specifications	47

Executive Summary

Section 1016 of the *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004*¹ 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.” Executive Order (EO) 13388, issued on October 25, 2005,² requires that “to the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies: (a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America; (ii) the interchange of terrorism information among agencies; (iii) the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities; and (iv) the protection of the ability of agencies to acquire additional such information; and (b) protect the freedom, information privacy, and other legal rights of Americans.”

On December 16, 2005, the President issued a Memorandum for the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment that included requirements to *develop a common framework for the sharing of information* between and among Executive departments and agencies and State, local, and tribal (SLT) governments; law enforcement agencies; and the private sector and *define common standards* for the way information is acquired, accessed, shared, and used within the ISE.³

To comply with this legislative and Presidential direction, the ISE architectural approach builds upon processes affecting existing systems throughout the ISE, addresses terrorism-related information sharing across multiple levels of security and protection levels, and incorporates mechanisms for protecting privacy and civil liberties. The Program Manager, Information Sharing Environment (PM-ISE) introduced the ISE Architecture and Common Terrorism Information Sharing Standards (CTISS) programs,

¹ Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law No. 108-458 (December 17, 2004). Section 1016 of IRTPA was amended on August 3, 2007 by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Public Law No. 110-53. This version of the *ISE Profile and Architecture Implementation Strategy (ISE PAIS)* does not address the additional authorities and requirements set forth in P.L. 110-53; these will be addressed in future versions of the *ISE Enterprise Architecture Framework (ISE EAF)* and the *ISE PAIS*. The new law expands the scope of the ISE to include homeland security information and weapons of mass destruction information and sets forth additional ISE attributes. It also codifies many of the recommendations developed in response to the President’s information sharing guidelines, such as the creation of the Interagency Threat Assessment and Coordination Group and the development of a national network of State and major urban area fusion centers.

² Executive Order 13388—Further Strengthening the Sharing of Terrorism Information to Protect Americans, found at Internet site <http://www.ise.gov/docs/guidance/eo13388.pdf>.

³ Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment (Washington: White House, 2005), Section 1, found at Internet site http://www.ise.gov/docs/Memo_on_Guidelines_and_Rqmts_in_Support_of_the_ISE.pdf.

cross-community, institutional approaches for helping ISE participants⁴ adjust, plan, install, and operate current and future information resources that form the infrastructure fabric of the ISE. A business process-driven *ISE Enterprise Architecture Framework (EAF)* and this companion document, the *ISE Profile and Architecture Implementation Strategy (PAIS)*, are designed to be used to implement the ISE across Federal information resources,⁵ consistent with Office of Management and Budget (OMB) Federal Enterprise Architecture (FEA) Framework guidelines. Furthermore, this approach defines recommended approaches for connecting information resources of SLT governments, the private sector, and foreign partners, and integrates the diverse landscape of existing policies and management processes across the Federal Government. A fully functional ISE requires the development of information sharing relationships and the transformation of culture and institutions supported by the construction, integration, and sustained operations of terrorism-related information sharing systems, processes, services, and other resources across the Nation.

Document Organization

This *ISE PAIS* is a companion document to the *ISE EAF* and provides implementation guidance for ISE participants. As Table ES-1 outlines, this *ISE PAIS* is one of three documents that define the architecture program of the ISE.

Table ES-1. ISE Architecture Program Documentation

Title	Description
ISE Enterprise Architecture Framework	A high-level description of the components, structure, and unifying characteristics of the ISE to include the four partitions: Business, Data, Application & Service, and Technical.
ISE Profile and Architecture Implementation Strategy	A guide for ISE participants that describes what each should do to connect to the ISE, expose data to the ISE, build their ISE Shared Space, and access data and services provided by the ISE.
ISE Drivers and Requirements Specification	A high-level specification of the ISE requirements. Requirements are allocated to components of the <i>ISE EAF</i> including an ISE participant's ISE Shared Space, ISE Core Transport, ISE Core Services, and ISE Portal.

Chapter 1 – Introduction

The introduction describes high-level background information for this document. It defines the purpose and scope of this document. It also outlines supporting ISE-consistent architectural concepts.

⁴ An ISE participant refers to any Federal, State, local, or tribal government organization; private sector entity; or foreign government organization (to include employees) that participates in the ISE.

⁵ 44 U.S.C. 3502(6) defines information resources as "information and related resources, such as personnel, equipment, funds, and information technology."

Chapter 2 – ISE Architecture Implementation Considerations

This chapter provides descriptions of program management considerations required to develop and implement the ISE. These tools and approaches include information security and assurance, risk management, trust, systems validation and testing, and training.

Chapter 3 – ISE Architecture Implementation Life Cycle

This chapter provides a detailed description of the iterative architectural process used to develop and implement the ISE architecture, and an overview of OMB's Federal Segment Architecture Methodology (FSAM), an approach leveraged by the ISE to harmonize and integrate nationwide information resources to support information sharing. It outlines, in detail, the activities and anticipated inputs and outputs/outcomes at each stage of the ISE architecture development process. It also delineates the correlation and linkages of the ISE architecture development process to FSAM.

Chapter 4 – ISE Shared Spaces Development and Implementation

This chapter provides a detailed description of the types of hardware and software required to develop and implement an ISE Shared Space.

Chapter 5 – Case Study: Washington, DC Metropolitan Police Department (MPD) ISE Shared Space

This chapter provides a case study of the ISE Shared Space implementation at Washington, DC Metropolitan Police Department in preparation for the 2009 Presidential Inauguration.

Appendix A – Architecture and Infrastructure Committee Letter

This appendix is the letter from the Architecture and Infrastructure Committee (AIC) approving the *ISE PAIS, Version 1.0* document as a valid Profile and Architecture Implementation Strategy for the ISE. *ISE PAIS, Version 2.0* is consistent with and complements *ISE PAIS Version 1.0*.

Appendix B – Acronyms

This appendix provides an explanation of the acronyms used in this document.

Appendix C – Bibliography

This appendix provides a list of the major sources referenced in this document.

Appendix D – Glossary

This appendix provides definitions for certain specialized terms used in this document.

Appendix E – ISE Business Processes

This appendix provides descriptions for business process terms used in this document.

Appendix F – ISE Shared Spaces

This appendix provides a synopsis of ISE Shared Spaces and ISE Core development.

Appendix G – ISE Shared Space Information Security and Assurance (ISA) Considerations

This appendix outlines the ISA implementation details for ISE Shared Spaces and ISE Core development.

Chapter 1 – Introduction

1.1 Purpose and Scope

This *ISE PAIS* helps guide planning and implementation of ISE participants' enterprise architectures (EAs), segment architectures, solution architectures, and systems that follow key activities of the OMB Capital Planning and Investment Control (CPIC) process.⁶ Both Federal and non-Federal ISE participants can use this *ISE PAIS* to develop their related information resource capital planning and investment processes by identifying and incorporating ISE standards into those information technology (IT) systems that will interface with the ISE. Moreover, this *ISE PAIS* provides guidance to ISE participants and ISE Implementation Agents⁷ for developing and implementing information resources that support a successful and operational ISE.

This *ISE PAIS* recognizes and leverages the *ISE EAF* as an approved and accepted framework for structuring and describing information sharing services, systems, and processes required for an organization to participate in the ISE. The *ISE EAF* provides the overarching framework (i.e., the “what”) and the methodology (i.e., the “how”) towards implementation. This *ISE PAIS* provides implementation details to build information sharing systems and participate in the ISE. This *ISE PAIS* illustrates specific implementation details needed and provides a discrete operational example of an ISE Shared Space development. Establishing trust (to include proper application of information assurance [IA] and cyber security principles) is critical in the implementation of a protected and trusted ISE. This *ISE PAIS* includes guidance for incorporating a common risk management framework, trustworthiness, governance, and information system(s) security concepts (including considerations for security and protecting privacy and civil liberties) into ISE participants' and ISE Implementation Agents' EAs.

1.2 Supporting Architecture Concepts

To capitalize on the critical inter-organizational processes associated with the ISE Architecture program and the CTISS program efforts, the PM-ISE, Federal departments and agencies, and SLT organizations developed the following key documents leveraged to produce this *ISE PAIS*: *ISE PAIS, Version 1.0*, *ISE EAF, Version 2.0*, and *ISE-SAR Evaluation Environment (EE) Segment Architecture, Version 1.0*.⁸ This *ISE PAIS* cuts across the interrelated FEA reference models providing guidance to Federal departments and agencies for use in implementing the ISE. This *ISE PAIS* is not only

⁶ Aligning to the OMB CPIC process is a proven best practice that not only helps Federal Government departments and agencies plan, invest, and integrate IT resources but also demonstrates to non-Federal government organizations the extensibility of the *ISE PAIS* to support both environments.

⁷ An ISE Implementation Agent refers to an organization responsible for providing infrastructure and services in the ISE Core Segment as defined in the *ISE EAF*.

⁸ The *ISE-SAR Evaluation Environment (EE) Segment Architecture, Version 1.0* can be found at <http://www.ise.gov/pages/sar-initiative.html>.

based on the *ISE EAF*, but it also includes guidance and requirements derived from the National Strategy for Information Sharing (NSIS), October 2007.⁹

1.2.1 ISE Enterprise Architecture Framework

The *ISE EAF* meets three objectives: (1) provides a comprehensive, strategic description of the overall ISE architecture; (2) establishes an architectural framework for implementing ISE capabilities; and (3) identifies key architectural decisions that have been made or must be made. The impact of the *ISE EAF* resulted in many Federal departments and agencies incorporating *ISE EAF* fundamental principles into existing enterprise architecture or transition strategies to help improve and institutionalize information sharing across the ISE.

The PM-ISE released to heads of departments and agencies the newest version of the *ISE EAF* on October 21, 2008. The *ISE EAF, Version 2.0* builds on the foundation established in *ISE EAF, Version 1.0* to provide more specificity and granularity for ISE mission business processes and information flows. This newest version of the *ISE EAF* was developed through a collaborative process involving members from the Information Sharing Council (ISC), and provides additional structured descriptions of the ISE's associated business processes, information flows and relationships, services, and high-level data packet descriptions. New additions in *ISE EAF, Version 2.0* include

- Greater granularity to support the mission business processes for
 - Suspicious Activity Reporting (SAR);
 - Identification and Screening (Terrorist Watchlist (TWL) components);
 - Alerts, Warnings, and Notifications (AWN).
- The roles and responsibilities of the ISE Implementation Agents for implementation within the ISE Core;
- ISE Shared Spaces components discussion;
- An ISE Identity and Access Management (IdAM) Framework;
- A cross mapping of ISE mission business processes to the FEA Business Reference Model (BRM) sub function.¹⁰

The *ISE EAF* continues to assist in coordinating activities and development of individual ISE participant enterprise and information sharing segment architectures (ISSA),¹¹

⁹ National Strategy for Information Sharing, October 2007 is available at <http://www.ise.gov>.

¹⁰ ISE participants' ability to align department-level investment planning and budget activities to common ISE business processes affords departments and agencies the opportunity to reuse common practices, avoid additional developmental/implementation cost, and leverage common services used in support of the ISE.

¹¹ As noted in the *ISE EAF*, in each ISE participant's Information Sharing Segment Architecture (ISSA), common ISE attributes, services, standards, and other ISE tools are apparent and allow for opportunities to reuse (promoting cost savings) and leverage services within the Federal community. ISSAs would include data assets, applications, and services that facilitate information sharing. Additionally, each ISE participant segment will include the software and hardware that provide the interface to the ISE Core segment.

associated CPIC processes and the management of those business processes and information resources that define the nationwide ISE capability. The applicable types of information that traverse the ISE include, but are not limited to, terrorism information,¹² homeland security information,¹³ and law enforcement information.¹⁴ To integrate and operate within the ISE, ISE participants should (1) incorporate *ISE EAF* attributes into their information systems to interface with the ISE, and any subsequent implementation guidance into budget activities associated with relevant current (operational) mission-specific programs, systems, or initiatives (e.g., Operations and Maintenance [O&M] or enhancements); (2) incorporate the *ISE EAF* and any subsequent implementation guidance into budget activities associated with future or new development efforts for relevant mission-specific systems or initiatives (e.g., Development, Modernization, or Enhancement [DME]); and (3) incorporate the *ISE EAF* attributes into ISE participants' transition planning strategies for enterprise architecture or ISSA development and implementation.

Table 1-1 depicts the hierarchical relationships among the various levels of architectures used within individual agencies and organizations across the ISE that are influenced by the *ISE EAF* and this *ISE PAIS*. Consistent with OMB guidance for Federal departments and agencies, frameworks and profiles, enterprise, segment,¹⁵ and solution architectures¹⁶ provide different perspectives and levels of detail for

¹² The term "terrorism information" means "all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to (i) 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; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals." [IRTPA, Section 1016(a)(5), as amended.]

¹³ For the purposes of the ISE, the term "homeland security information" means 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)).]








¹⁴ For the purposes of the ISE, law enforcement information addresses 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.]

¹⁵ Segment Architecture refers to the business-driven approach of logically documenting the set of business and information requirements, outcomes, and constraints that lay the foundation for building executable operational solutions (or systems) that meet or exceed mission performance goals for a particular line of business and are derived from a concept of operations.

¹⁶ Solution Architecture refers to the structured, technical documents, derived from Segment Architectures, that are scoped to describe the particular functions or processes that will be implemented; identify methods for achieving operational outcomes; and define specific IT assets, applications, and components for procurement and implementation. Solution Architectures do not specifically identify vendors or specific vendor items as these are generally identified in subsequent specification documents and/or procurement orders.

agencies and organizations in their enterprise architecture planning. At the highest level, frameworks provide logical structures for classifying and organizing complex enterprise architecture information and, specifically, the Federal Enterprise Architecture Framework (FEAF), leveraged for defining the ISE architecture, provides “a structure for organizing Federal resources and for describing and managing Federal Enterprise Architecture activities.”¹⁷ The *ISE EAF*, in turn, presents a logical structure of ISE business processes, information flows and relationships, services, and high-level data packet descriptions and exchange relationships.

Table 1-1. Levels of Architecture

AUDIENCE	LEVEL	SCOPE	DETAIL	IMPACT	
ISE Stakeholders		ISE	Low	Nationwide Strategic Outcomes	The <i>ISE EAF</i> provides descriptions of ISE business processes, information flows and relationships, services, and high level data packet descriptions and exchange relationships. The <i>ISE PAIS</i> outlines what each ISE participant must do to connect to and expose data to the ISE, and access data and services provided by the ISE.
 All Stakeholders		Agency/ Organization	Low	Strategic Outcomes	Describes the current and future state of the organization, and lays out a plan for transitioning from the current state to the desired future state.
 Business Owners		Line of Business	Medium	Business Outcomes	Detailed result-orientated architecture (baseline and target) and a transition strategy for a portion or segment of the enterprise.
 Users and Developers		Function/ Process	High	Operational Outcomes	An architecture for an individual IT system that is part of a segment.

1.3 Testing and Evaluation

Testing and evaluation is another key element of the *ISE PAIS*. For each security domain (Top Secret/Sensitive Compartmented Information (TS/SCI), Secret/Collateral, Controlled Unclassified Information/Sensitive But Unclassified (CU/SBU)) in the ISE, an environment for testing, integrating, and managing ISE components is required to ensure that they are interoperable to the extent intended and compliant with ISE standards and requirements. Compliance with security, including privacy and Section

¹⁷ Chief Information Officer (CIO) Council, *Federal Enterprise Architecture Framework, Version 1.1*, (CIO Council: Washington, DC, 1999), C-6, found at Internet site <http://www.cio.gov/Documents/fedarch1.pdf>.

508 of the Rehabilitation Act of 1973¹⁸ requirements, are also vital for a successful evaluation in addition to functional, operational, and performance requirements for enabling associated business processes. The environment(s) will support controlled testing, integration, security assessment, and authorization to operate within the ISE; configuration management; and verification of procedures. Facilities to capture and analyze implementation test data will support various levels of testing. ISE participants will evaluate compliance with ISE common standards, as documented in the CTISS.

1.4 Privacy and Civil Liberties

Consistent with the NSIS and Presidential Guideline 5, Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004, and Section 1 of EO 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, the ISE Privacy Guidelines provide the foundation for sharing information in the ISE in a manner that protects privacy, civil rights, and civil liberties. The guidelines support the dual imperatives of sharing terrorism information and protecting privacy and civil liberties by establishing uniform procedures to implement required protection in unique legal and mission environments. In addition, the privacy guidelines establish an ISE privacy governance structure for compliance, conflict resolution and continuous development of privacy and civil liberties guidance.¹⁹

The privacy guidelines build on a set of core principles that all ISE participants will follow. These principles require specific, uniform action across these entities and reflect basic privacy and civil liberties protections and best practices. They require ISE participants to: identify any privacy-protected information to be shared; enable other ISE participants to determine the nature of the information (e.g., whether it contains information about U.S. persons); assess and document applicable legal and policy rules and restrictions that establish security, accountability, and audit mechanisms; implement data authenticity and integrity and, where appropriate, redress procedures; identify an ISE Privacy Official to ensure compliance with the guidelines; document privacy and civil liberties protections in an ISE privacy policy; and facilitate public awareness of these protections as appropriate.²⁰

Successful implementation of the guidelines requires a governance structure both to monitor compliance and to iterate guideline modifications as appropriate. The guidelines require all ISE participants to designate a senior ISE Privacy Official to directly oversee

¹⁸ Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

¹⁹ PM-ISE, Guidelines to ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment, found at Internet site

<http://www.ise.gov/docs/privacy/privacyguidelines20061204.pdf>.

²⁰ PM-ISE, Ibid.

implementation of the guidelines. The guidelines also provide for an ISE Privacy Guidelines Committee (PGC), consisting of ISE Privacy Officials, to ensure consistency and standardization (where feasible) in implementation as well as to share best practices and resolve inter-agency issues.

The ISE Privacy Guidelines ensure that Federal agencies and the PM-ISE will work with non-Federal entities (SLT governments, the private sector, and foreign partners) to ensure that such entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the guidelines.²¹

²¹ PM-ISE, Ibid.

Chapter 2 – ISE Architecture Implementation Considerations

Federal, State, local, tribal governments, and foreign and private partners will participate in the ISE if they are assured that the systems they are connecting to, requesting information from and providing information to, are secure. This section discusses documents and associated standards for consideration during architecture implementation, specifically

- Information Security and Assurance (ISA)
- Risk Management Framework (RMF)
- ISE Trust Relationships
- Systems Validation and Testing for the ISE, and
- Training

ISE participants must have confidence that the information shared by ISE participants is reliable and secure. Risk management ensures that applicable security guidelines and controls are in place for sharing ISE participant information. Implementing trust relationships also ensures information is properly secured and shared only with appropriate ISE participants.

This section also discusses the appropriate level of systems validation and testing recommended to ensure that all hardware and software, whether commercial off-the-shelf (COTS), custom developed or proprietary, are certified ensuring security across the enterprise.

Adequate training is suggested. Managers should design and implement training programs so that all ISE participants can be confident that information and assets shared within the ISE are safeguarded at the appropriate security and classification levels.

2.1 Information Security and Assurance (ISA)

The secure, accurate, and timely sharing of terrorism information among Federal, State, local, and tribal governments as well as foreign partners and private sector entities is a fundamental tenet of the ISE. Information Sharing Environment Guidance (ISE-G-106) Technical Standard – Information Assurance, Version 1.0, issued October 2008 – identifies technical standards for providing information assurance (IA) services within the ISE Core. These technical standards constitute voluntary consensus standards for planning, implementing, and providing ISE Core infrastructure, and developing ISE Shared Spaces. ISE participants should ensure alignment to these technical standards for developing and interfacing their ISE Shared Space to the ISE Core and providing system connectivity. Information assurance standards are identified for use within the ISE Core, and include the implementing authoritative organization.

ISA²² supports both this fundamental tenet and the protection of privacy and civil liberties. From the Implementer's View in Figure 2-1, ISA is an integral part of the overall ISE architecture and critical for enhancing the cyber security posture of the ISE.

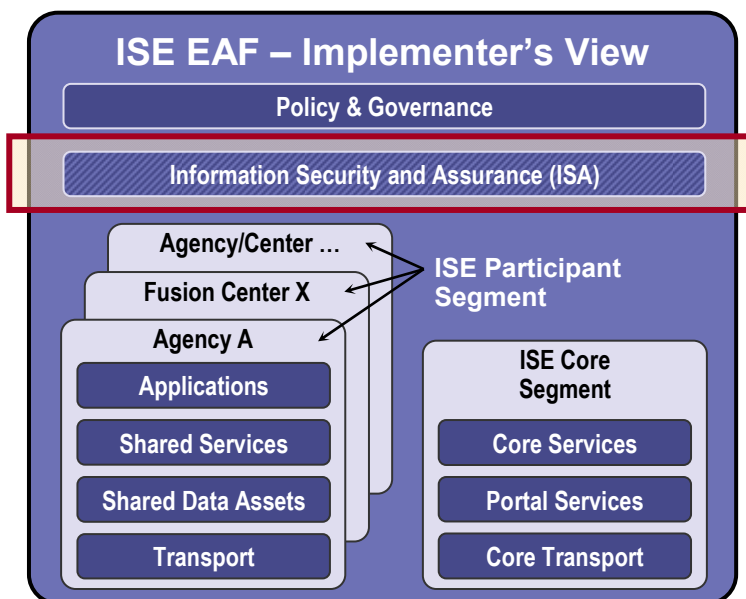


Figure 2-1. ISE EAF Implementer's View

2.2 Risk Management Framework (RMF)

The steps for implementing the RMF are described in the ISA Chapter of the *ISE EAF* and in National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-39²³. Figure 2-2 depicts the RMF cycle illustrating the specific activities in the ISE/NIST RMF security standards and guidelines. Following Figure 2-2 are the implementation details for each step in this cycle.

²² Information Security and Assurance is defined in Chapter 4 of the *ISE Enterprise Architecture Framework, Version 2.0*, November 2008, found at Internet site <http://www.ise.gov>.

²³ All of the NIST documents, both the Special Publications and Federal Information Processing Standards that are listed in this section, are published by NIST and can be found at <http://www.csrc.nist.gov/publications/PubsSPs.html>.

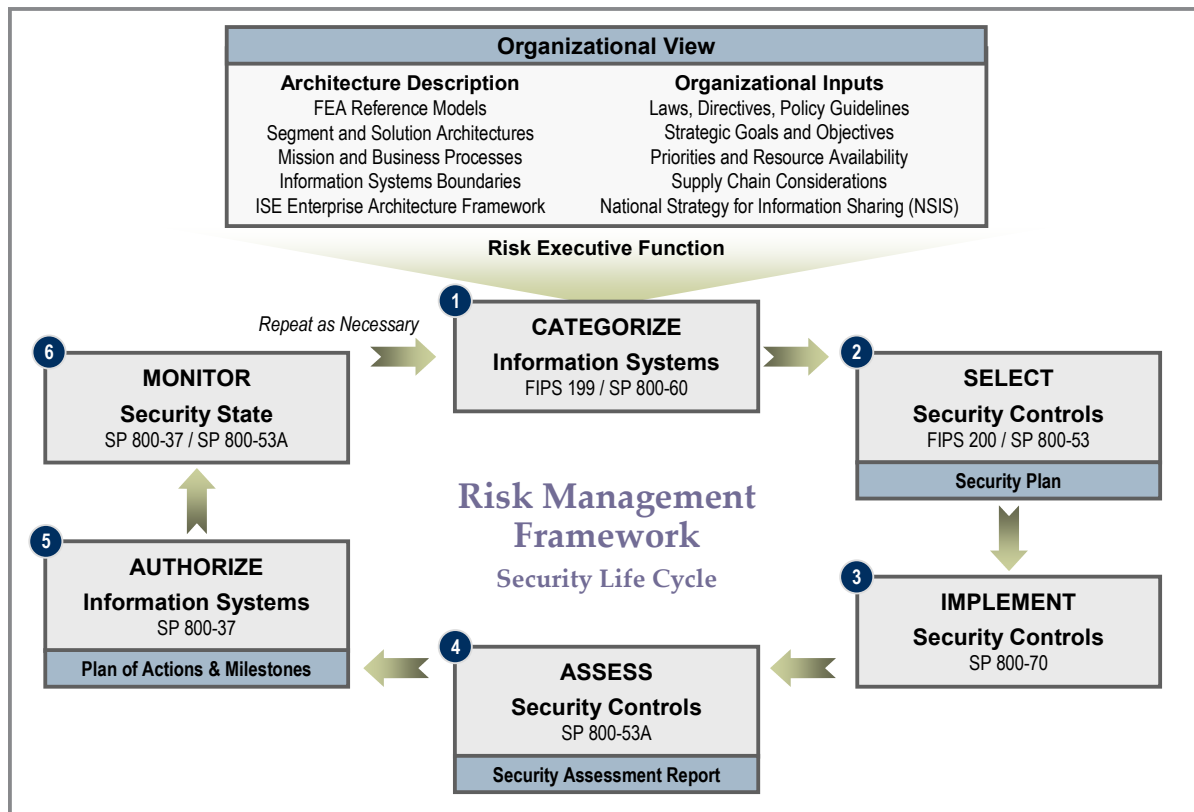


Figure 2-2. The ISE Risk Management Framework (RMF)

Step 1 – Categorize the ISE information system(s) and the information residing within the systems based on the security category recommendations from the CTISS technical standard for IA. The levels used are *low-impact*, *moderate-impact*, and *high-impact*, which are defined in detail in the listed implementation documents. This categorization must consider the potential impacts of not sharing the information as well as potential impacts if the information is shared. It also depends on the overall categorization of all the networks to which the ISE participant intends to connect. The highest categorization level would be maintained by all information systems that are connected. For example, if the local network risk assessment establishes it to be *low-impact* and is negotiating a reciprocal agreement with a network that was established at *moderate-impact*, the network that is established *low-impact* will need to adjust its security posture (security controls baseline) to meet the *moderate-impact* risk security controls baseline as presented in NIST SP 800-53 and its associated annexes. This type of scenario is mitigated by following the information systems categorization implementation guidance documented in the NIST Federal Information Processing Standards (FIPS) 199 and SP 800-60.

Step 2 – Select an agreed-to set of safeguards and countermeasures for ISE information system(s) based on the security categorization and recommendations from the ISE. Supplement the agreed-to set of safeguards and countermeasures based on an assessment of ISE participants' site-specific risk conditions including organization-

specific security requirements, specific and credible threat information, cost-benefit analyses, or special circumstances. Document the set of safeguards and countermeasures in the ISE information system(s) security plan including the rationale for any refinements or adjustments to the implemented set of safeguards and countermeasures based on ISE participants' site-specific conditions. Implementation details for establishing the appropriate security controls are found in the NIST guidance, FIPS-200 and SP 800-53, with the *low-impact*, *moderate-impact*, and *high-impact* baselines listed in SP 800-53 Annex 1, 2, or 3.

Step 3 – Implement the safeguards and countermeasures in the ISE information system(s). Implementation details are presented in NIST SP 800-70, which provides detailed instructions as well as a list of common products checklists on how and when to create checklists. A security configuration checklist (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of instructions for configuring a product to a particular operational environment. It could also include templates or automated scripts and other procedures. Typically, checklists are created by IT vendors for their own products; however, checklists are also created by other organizations such as consortia, academia, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. Checklists may be particularly helpful to small organizations and individuals that have limited resources for securing their systems.

Step 4 – Assess the implemented safeguards and countermeasures for effectiveness using appropriate methods and procedures to determine the extent to which the safeguards and countermeasures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the ISE system. This step is essential to demonstrating the degree of “trustworthiness” of the system, a critical input to the risk decision and maintenance of trust within the ISE. NIST SP 800-53A provides the implementation details for security control assessments. Once an organization has completed steps one, two, and three, or if the network is operational and the organization wants to baseline its security level, the organization should follow the assessment process established in 800-53A.

Step 5 – Authorize the ISE information system(s) operation (with implemented safeguards and countermeasures) based upon a determination that the risk to the ISE participants' operations and assets, to individuals, to other organizations (that are part of the ISE community), and to the Nation resulting from the operation of the system is acceptable. The steps for implementing the authorization process are published in NIST SP 800-37.

Step 6 – Monitor and assess agreed-to set of safeguards and countermeasures in the ISE information system(s) on a continuing basis, including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate ISE officials on a regular basis. Security monitoring is implemented through local policy using the NIST SPs 800-37 and 800-

53A. ISE participants should establish local security monitoring policy, which satisfies any reciprocal agreements and/or ISE governance direction.

By following this set of guidelines, all ISE participants will be using a common, continually updated approach to risk management of their information systems, processing, and storing terrorism and/or homeland security information. By leveraging these standards and guidelines, ISE participants can reduce staffing and management required for risk management, thus reducing costs and increasing overall effective security for their organization.

2.3 ISE Trust Relationships

Information sharing in the ISE depends on establishing trust relationships among ISE participants. Common certification and accreditation policies, standards, community-wide processes, and procedures leading to reciprocity agreements with the ISE will help promote this trust.

One such example of a reciprocity document is Intelligence Community Directive (ICD) 503. Published in September 2008, ICD 503 delineates joint Department of Defense (DoD) and Director of National Intelligence (DNI) reciprocity goals. Although ICD 503 does not apply to SLT governments and is not binding upon other federal agencies, it is an example of a reciprocity agreement that could be used as a template for agreements between such entities.

Table 2-1. ICD 503 Purpose

ICD 503 Purpose
“This policy implements strategic goals and focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.”

The ISE leverages the NIST body of documents as the baseline for CTISS Technical Standards. Implementing trust relationships requires each ISE participant to meet or exceed these voluntary consensus standards. For example, the standards for the Federal Government include following the NIST documentation, which covers risk management, computer security, and network security as a few examples. It is recommended that non-Federal participants meet the NIST-documented common standards. Figure 2-3 provides a graphic representation of this process and illustrates the types of evidence that can be used to support the establishment of trust among ISE participants.

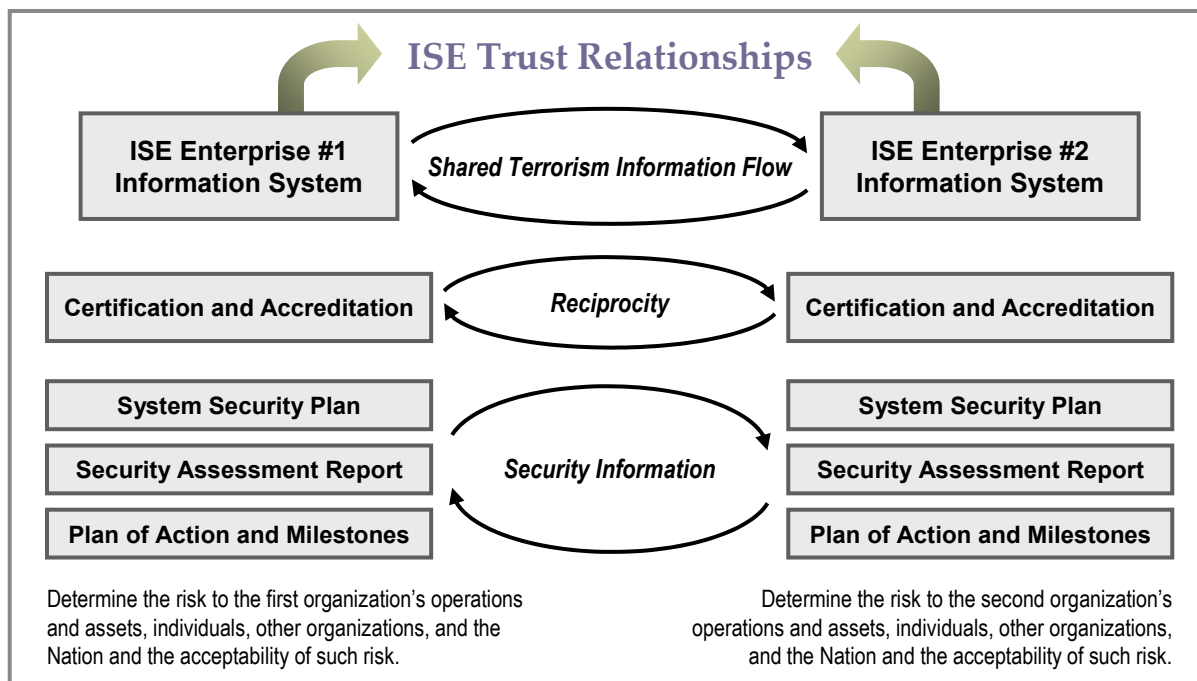


Figure 2-3. Building Trust Relationships through Security Due Diligence and Reciprocity

Trust relationships among ISE participants depend on carrying out each of the five elements of trust described in Table 2-2. The objective, through common Certification and Accreditation (C&A) standards, is to achieve an understanding of the prospective ISE participant's information security programs and information system(s) and to agree upon a level of security necessary to establish trusted cross-enterprise information sharing. Levels of security depend on the consistent plans and actions taken by the ISE participants to implement common and appropriate safeguards and countermeasures for their information system(s) interconnecting through the ISE Core. The effectiveness of the security implementation is conveyed in key organizational security documentation, such as certification and accreditation policy, information System(s) Security Plan(s) (SSP), security assessment reports, and Plans of Actions and Milestones (POA&M).²⁴

²⁴ Information system(s) security plans, security assessment reports, and plans of action and milestones are used by authorizing officials to make authorization decisions, understanding and explicitly accepting enterprise risk. The documents are generated during the execution of the Risk Management Framework described in Section 2.2.

Table 2-2. ISA Five Elements of Trust

Information Security and Assurance Five Elements of Trust	
i.	Identifying common goals and objectives for sharing terrorism information, to include various requirements across the ISE
ii.	Agreeing upon risks associated with terrorism information sharing activities
iii.	Agreeing upon the degree of trustworthiness needed for the ISE information system(s) processing, storing, or transmitting shared terrorism information in order to adequately mitigate risks
iv.	Through testing, determine if respective implementations of ISE information system(s) are worthy of being trusted to operate within the agreed-upon levels of risk despite environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation
v.	Providing ongoing monitoring and oversight ensuring that the ISE trust relationships are being maintained

Trust cannot be conferred upon ISE participants; it must be earned through partner corroboration, common use of security policies and practices, and other such reciprocal agreements. ICD 503, along with agreements within the law enforcement community, are examples of implementing organizational reciprocity agreements for information systems that process and store terrorism and/or homeland security information.

2.4 Systems Validation and Testing for the ISE

Application and hardware security is an integral component to system trustworthiness. An ISE Application Security Program that follows NIST and Committee on National Security Systems (CNSS) guidance will contribute to the development and maintenance of trust relationships among ISE participants and their information systems.

For implementation, ISE participants are encouraged, whenever possible, to use assessment results and related documentation available on ISE information systems' components from independent or third party testing organizations such as NIST, CNSS, and International Organization for Standardization (ISO) in their overall security assessment process.

Risk mitigation of application and hardware security is accomplished through various means depending on the application. NIST product assessments can be followed such as FIPS140-x Security Requirements for Cryptographic Modules,²⁵ Common Criteria Certification,²⁶ independent third party software validation and testing for proprietary

²⁵ The vendor list of validated cryptographic modules can be found at <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm>.

²⁶ This links to the Common Criteria certified products lists can be found at <http://www.commoncriteriaportal.org/products.html>.

software,²⁷ and any other Federal, State or local certification body recognized by the ISE.

2.5 Training

Uniform ISE training programs that incorporate counterintelligence cyber awareness will lead to trust and reciprocity and provide the means to show others how the organization handles and protects shared terrorism and/or homeland security information. This, in turn, enhances confidence and maximizes sharing.

All ISE participants should follow and meet their organizational minimum information security and assurance awareness user training, undertaken at least annually. Organizations should conduct training and keep records of those ISE participants who have completed training as part of the system certification packages for reciprocity within the ISE.

In addition to the annual user training, ISE participants should address specific information security and assurance training through a common and federated approach. The CTISS Committee will recommend ISA training for consideration by the ISE. These standards will assist all ISE participants in setting up and performing appropriate ISE-specific training within their organizations.

²⁷ This links to a Department of Homeland Security document depicting a "Secure Software Development Life Cycle Process" found at <https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/sdlc/326-BSI.html>.

Chapter 3 – ISE Architecture Implementation Life Cycle

3.1 Introduction

ISE participants are encouraged to plan, budget, and invest in the ISE by adopting common business practices and principles, and incorporate reusable service and data assets. Across the five ISE communities,²⁸ ISE participants continue to make strides to standardize an enterprise-level approach through the use of ISE Shared Spaces for making terrorism-related information available, accessible, and discoverable. The *Federal Segment Architecture Methodology (FSAM)*²⁹ is an emerging best practice that provides for architecture reuse and facilitates the standardization of information and supporting IT resources across the ISE. This standardization will help to ensure community-wide information resource integration and coordination.

3.2 Federal Segment Architecture Methodology

The *FSAM* is a step-by-step process for developing and using segment architecture; it leverages existing “best practice” analysis techniques and easy-to-use templates to expedite architecture development (See Figure 3-1). Following the steps in the *FSAM* helps ensure community-wide information resource integration and coordination. The top level of the methodology consists of five key process steps that provide guidance on identifying and validating the business need and the scope of the architecture. The *FSAM* defines the current (“As Is”) and target states for the segment architecture and develops transition plans for the performance, business, data, services, and technology layers of the architecture.

²⁸ The five communities as defined by the ISE Implementation Plan are Intelligence, Law Enforcement, Defense, Homeland Security, and Foreign Affairs.

²⁹ The *Federal Segment Architecture Methodology (FSAM)*, released on 9 December 2008, and is available at www.fsam.gov.

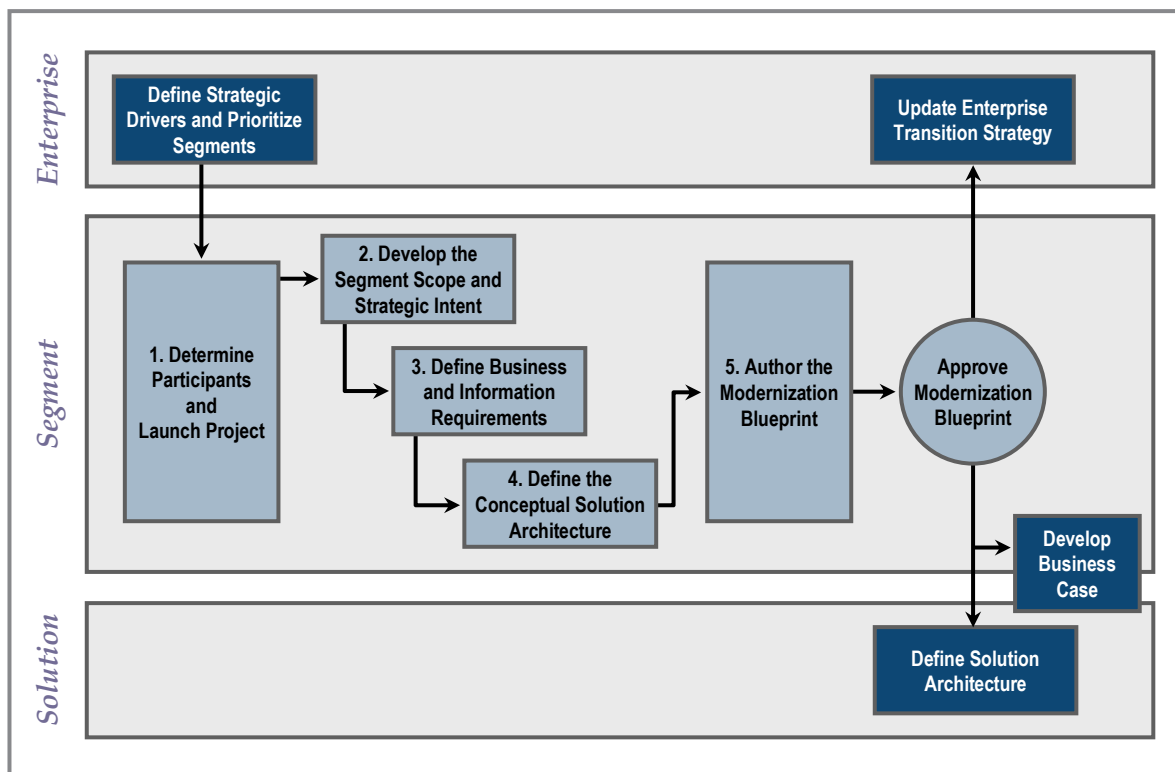


Figure 3-1. FSAM Methodology

The *FSAM* also includes guidance for developing a segment architecture using repeatable “how-to” processes that support business and results-oriented modernization planning. As the *FSAM* relates to the ISE, key questions for resolution during the initial stages of development and consideration include

- What are the vision and performance goals for the segment that will support ISE requirements?
- What are the design alternatives for achieving the performance goals in the ISE?
- What ISE-related projects are required to achieve the target segment architecture and in what order should they be executed?
- What are the primary change drivers in the ISE affecting the segment?
- What are the current segment systems and resources?
- What are the deficiencies or inhibitors to success, and how can information security within the segment be improved?

While representatives from Federal departments and agencies designed this methodology, its relevancy traverses the entire ISE to include SLT governments, and foreign and private sector partners. The *FSAM* also provides an organized blueprint for complying with the roles and responsibilities established by the *National Strategy for Information Sharing (NSIS)*. Similar to activities described within the *FSAM*, it is

recommended that ISE participants establish processes and systems for gathering, processing, analyzing, and disseminating terrorism, homeland security, and law enforcement information while protecting the privacy and other legal rights of U.S. Persons, as provided for under U.S. law.

3.3 FSAM and ISE Architecture Implementation Life Cycle Alignment

The activities represented in Figure 3-2, the ISE Architecture Implementation Life Cycle (ISEA ILC), are similar and closely aligned to the activities and tasks explained within the FSAM. The term “life cycle” refers to a continuous iterative process that ISE participants and ISE Implementation Agents should follow in implementing their capability to interface with the ISE.

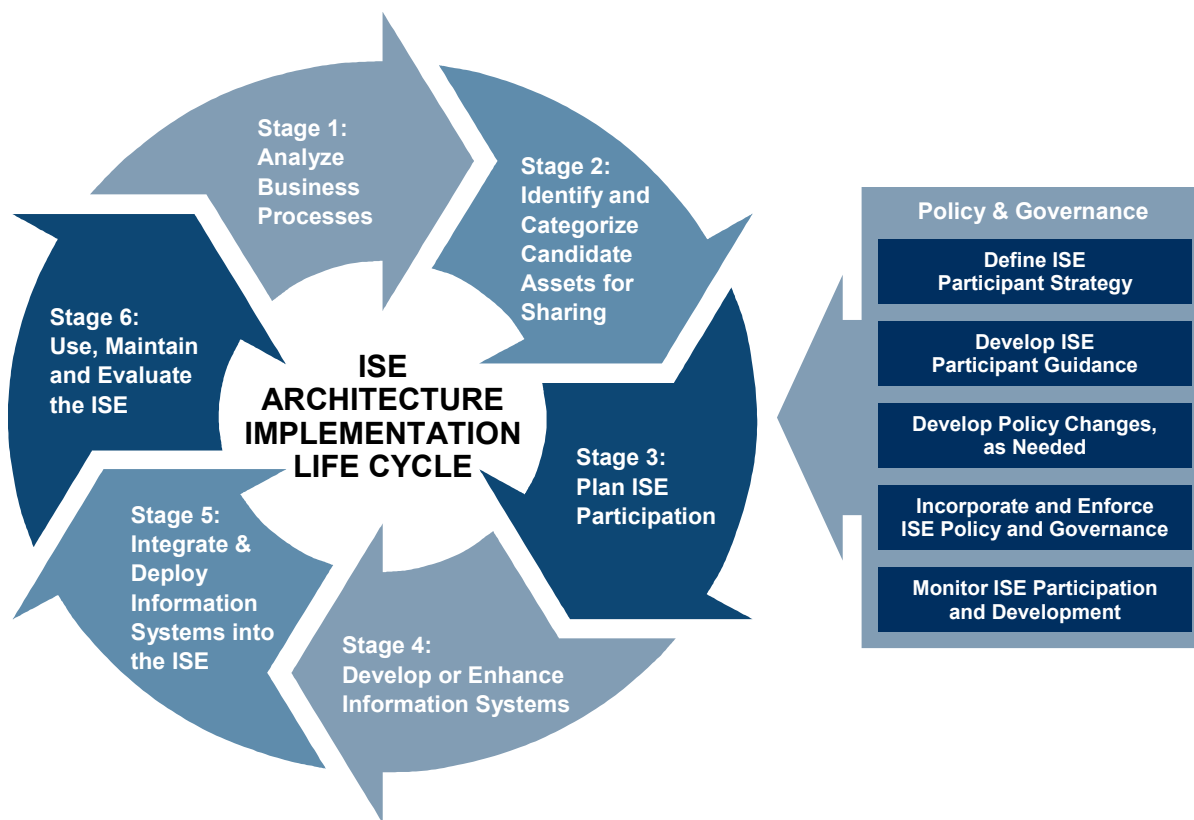


Figure 3-2. ISE Architecture Implementation Life Cycle

The FSAM developers used as “best practices” the ISE architecture principles established by both the *ISE EAF, Version 1.0* dated August 2007³⁰ and the *ISE PAIS, Version 1.0* dated May 2008.³¹ The iterative stages explained within the ISEA ILC map to key activities and tasks explained in the overarching *FSAM*. The ISEA ILC presents a

³⁰ PM-ISE, *Information Sharing Environment Enterprise Architecture Framework, Version 1.0*, August 2007, found at <http://www.ise.gov>.

³¹ PM-ISE, *Profile and Architecture Implementation Strategy, Version 1.0*, May 2008 is available at <http://www.ise.gov/pages/eaf.html>.

six-stage process that follows the guidance found in the *ISE EAF* to develop and implement information sharing segment architectures and ISE Shared Spaces. Capitalizing on the recent issuance of the *FSAM* in December 2008, the activities and tasks of the ISEA ILC are presented as key activities within the *FSAM* process steps. Similar to the *FSAM*, the stages identified within the ISEA ILC require ISE participants to work collaboratively in support of ISE-wide “To Be” mission business processes. This engagement offers opportunities for reuse and exposure of shareable common assets across the ISE rather than stove-piped development. From a security and trust perspective, the *FSAM* and the ISEA ILC also apply the security principles and trust models established within the *ISE EAF* by the CNSS and NIST as codified by the FEA Security and Privacy Profile (SPP).³² The *ISE-SAR Evaluation Environment (EE) Segment Architecture, Version 1.0*, is considered a model that demonstrates utility of the *FSAM* for a real-time operational scenario.

3.3.1 FSAM Process Step 1: Determine Participants and Launch Project

This process step helps ensure all relevant stakeholders are engaged in the ISSA development process. This step also begins segment architecture development and includes constant involvement and validation of effort throughout the development process.

While the *FSAM* requires the identification of the Executive Sponsor as it relates to the ISE, ISE Implementation Agents have the responsibility to provide ISE participants the ability to post and share their terrorism related information through the ISE Core. The *ISE EAF* outlines an ISE Implementation Agent’s responsibilities within the Business, Application and Services, Data, and Technical partitions that must be performed to ensure integration within the ISE. ISE Implementation Agents have high-level understandings of the planning concepts and resource commitments needed to develop an ISSA. The development of an ISSA requires commitment by ISE Implementation Agents and careful analysis of the “As Is” environment. This analysis yields opportunities to improve, modernize, enhance, or remove inhibitors that prevent forward progress toward the “To Be” state. The analysis should: 1) identify what components of the ISE participants’ architecture are in place, and 2) what components are needed to achieve the “To Be” state. Chapter 6 of the *ISE Implementation Plan*³³ establishes a communication strategy that identifies the organizations and affected *ISE EAF* partitions. The communication strategy captures the key messages and themes relevant for all ISE participants who expect to integrate with the ISE.

The requirements and activities of this FSAM process step are addressed within Stage 1 of the ISEA ILC.

³² FEA Security and Privacy Profile (SPP) can be found at: <http://www.whitehouse.gov/omb/e-gov/fea/>.

³³ Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, November 2006, found at <http://www.ise.gov>.

3.3.2 FSAM Process Step 2: Develop the Segment Scope and Strategic Intent

Aside from engaging appropriate stakeholders and gaining stakeholder concurrence with ISSA direction and implementation, it is equally important to understand and document the scope and strategic intent of the ISSA. This activity is important as it summarizes the components and stakeholders that are engaged in subsequent ISSA development activities, and identifies ISE participants needed to achieve the targeted state in the purpose statement. The summary description provides the scope and context through which subsequent information sharing process steps are bound.

ISE Implementation Agents reference the *NSIS* and *ISE EAF* for the strategic direction and goals established for the ISE and all segments that will integrate with it. The ultimate goal of the ISE is to “integrate terrorism information from multiple sources and to provide maximum and appropriate access to such information.”³⁴ As defined in *Section 1016 of the IRPTA*, the ISE is “an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section.”³⁵ As enablers to support the ISE, ISE Implementation Agents ensure the “To Be” state aligns with the identified scope of the ISE.

Questions that must be answered by ISE Implementation Agents and/or ISE participants who are defining mission needs should include the following:

1. How does this implementation align and support requirements identified within the NSIS?
2. What information will be shared based on CTISS Functional Standards and other guidance?
3. Is information being shared today? Why or why not?
4. What is the intended use of the information?
5. What mission processes are supported?
6. Who has the data needed to share, or who has previously unknown terrorist information that could augment existing data?
7. How is data accessed?
8. Who/where are the authoritative sources of data usage and interpretation?
9. What are the risks or the consequences if sharing does not take place?

³⁴ Ibid.

³⁵ Intelligence Reform and Terrorism Act of 2004 (IRPTA), Public Law No. 108-458 (17 December 2004). Section 1016 of IRPTA was amended on 3 August 2007 by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Public Law No. 110-53.

10. What are the business processes and the outcomes to achieve the level of trust (risk mitigation/management) to assess the security protections used within the ISE?³⁶
11. Where are the gaps?
12. What policies (at Federal, State, local, and tribal levels) need to be revised to enable and make for an effective integration within the ISE?
13. What is the mission risk of not having access to the information? Is that a managed risk or a risk to be avoided?
14. How has the unanticipated user risk been mitigated?
15. Who are our exchange partners?
16. In what form is our organization required to share information today?

Throughout this process, ISE Implementation Agents should monitor other ISE-related activities to stay abreast of what capabilities are planned or already available. The ability of the ISE participant to identify and address these fundamental questions may minimize inhibitors that affect the use of ISSAs and ISE Shared Spaces. ISE participants must consider security implications of sharing information and what the risks are to any organization.

3.3.2.1 Validate and Communicate the Scope and Strategic Intent

The *ISE EAF* refines the segment scope and strategic intent, ensuring the proposed scope and strategic intent are aligned with the overall ISE architecture. The PM-ISE and ISE partners created these ISE documents for establishing the vision and strategic direction as ISE participants' transition to a culture of sharing common terrorism-related information.

3.3.3 FSAM Process Step 3: Define Business and Information Requirements

During this process step, ISE participants and ISE Implementation Agents develop a thorough understanding of the assets available for exposure via the ISE based on ISC agreed-upon intent and direction for the ISSAs as outlined in the previous steps. ISE participants and ISE Implementation Agents should analyze their business processes and targeted outcomes and establish their part of the ISE common risk management governance process to balance the access of information with risks among all Federal, State, local, tribal, foreign government, and private sector partners. The activities and requirements of the ISEA ILC, *Stage 1 (Analyze Business Process)* and *Stage 2 (Identify and Categorize Candidate Assets for Sharing)*, coincide with the analysis achieved during these FSAM process steps. All subsequent activities within this FSAM process step are driven and directly influenced by assessing current business processes and information resources. Establishing a strong understanding of the

³⁶ Section 1016 of IRTPA.

current baseline environment and activities are fundamental towards enhancing and achieving the desired mission outcomes. The FSAM incorporates the activities within the ISEA ILC Stage 1 to ensure all stakeholders and components are engaged and support the activities required to achieve defined mission performance metrics. It is also the responsibility of ISE participants to validate and approve the parameters that define the segment boundaries. More detailed analysis performed in process step 3 may warrant adjustments to the segment scope and context. Any additional information uncovered during this analysis is consolidated for consideration by the ISE participants. While flexibility on the scope is encouraged, avoidance of arbitrary scope creep is recommended.

Multiple desired outcomes are derived from this business process analysis. First, there is a uniform identification and understanding with ISE participants and ISE Implementation Agents of the current “As Is” business processes. Second, goals and objectives identified in Section 3.3.2 (FSAM Process Step 2) for participation in the ISE are validated. Third, ISE participants should determine what modifications (based on identified gaps/shortfalls) will achieve target “To Be” processes for integrating with the ISE.

Once business process analysis is complete, based on the framework already established with the ISE mission business processes, ISE participants should develop a migration plan that transitions use of “As Is” business processes, information flows, and technology to “To Be” versions consistent with those documented in the *ISE EAF* and other ISE documentation. As an integral part of this planning, ISE participants identify the required level of system trustworthiness, including statutory/regulatory restrictions on information sharing. This includes special handling procedures to adequately address the risks determined in the previous stage and define the requirements necessary to achieve this trustworthiness.

3.3.3.1 Identification and Understanding of “As Is”

The key artifacts created during this activity are the “As Is” business process information flows, the business and data architecture adjustments, and target information flow diagrams required to define the activity and outcomes of sharing ISE mission-related information. Likewise, each ISE participant must identify what gaps exist in current asset inventories. This analysis identifies what components of the enterprise, segment, and solution architectures are in place, and further, what components are needed to achieve the target state. This is a key activity within FSAM Process Step 3.

The *FSAM*, with principles of the ISEA ILC Stage 1, requires identification of the business processes, information flows, and information system(s) development, improvement, and deployment activities that enable participation in the ISE. Each activity is influenced or driven by ISE policy and governance components, including strategy provisions and monitoring functions to support advancing the ISE. Each activity plays an integral role in enterprise architecture and CPIC activities performed by each ISE participant. ISE participants should implement courses of action and governance in

accordance with ISE issuances. A key success is to analyze and document the current business and information requirements, aligned with appropriate security risk and mitigations required to assist in the design and delivery of an ISSA.

Additionally, the potential risks and impacts of sharing or not sharing are determined. A solution for concerns related to information dissemination is to appropriately use data tagging dissemination or release controls, and handling instructions to ensure the integrity of the data is not compromised. ISE participants must be keenly aware of and familiar with identification, security controls, and categorizations that have been put in place to assist in this process. ISE participants should have an understanding of organization-level security control documentation and policies which articulate the parameters and tolerance levels for the organization. This step receives the outputs of the previous steps, and in coordination with the business owners and other stakeholders, translates the activities described in the previous steps into an actionable and realistic execution of an ISSA. This is a concerted, collaborative, cross-organizational effort to analyze the existing mission business processes. This analysis consists of building an asset inventory, an information flow, and identifying gaps that hinder the “As Is” business processes from supporting cross-organizational target mission business processes.

3.3.3.2 Asset Inventory

In identifying their assets, ISE participants and ISE Implementation Agents create an asset inventory. The assets selected for this inventory directly support and affect cross-ISE capability to effectively share information. Assets that do not support the cross-ISE “To Be” processes should not be included in this inventory. Typically, services and applications selected for sharing in this process support or give access to the identified data assets. The assets identified for sharing are categorized in accordance with ISE policy and guidance regarding potential impacts upon the organization from the perspective of what may occur if the information is shared and what may occur if the information is not shared.

To create an asset inventory, ISE participants should use the following high-level procedures:

1. Identify and categorize sharable data assets as documented within the CTISS Functional Standards.
2. Align data assets with identified ISE mission business processes in segment architectures as identified by CTISS and in the *ISE EAF* (e.g., SAR, TWL, and AWN).
3. Identify information exchanges as documented in the *ISE-SAR Functional Standard* for each SAR data asset to be shared.³⁷

³⁷ The Information Exchange Package Documentation (IEPD) Clearinghouse provides a broad variety of information on IEPDs. This source includes examples that have been submitted by individuals and organizations who have

4. Identify and categorize service assets for sharing.
5. Create service descriptions.³⁸
6. Identify and categorize application assets for sharing.
7. Create application descriptions.
8. Leverage existing documentation (Functional Standards, *ISE EAF*, Service Level Agreements [SLAs]) rather than recreate additional documentation.
9. Append known information on security restrictions and information handling instructions.

During this activity, ISE participants and ISE Implementation Agents develop thorough understandings of the data, services, capabilities, subject matter expertise, and application assets available for exposure via the ISE. Additionally, this categorization is used to explicitly identify the risks that are accepted by ISE participants, including limitations by regulation, statute, or prior stakeholder agreement on whether and how the information is shared.

Data assets are stored, accessed, and retrieved within ISE Shared Spaces and transferred across or within the ISE. If an information exchange does not exist for a targeted data asset, it must be developed and made available for participants via the ISE Core. Service and application assets are described using applicable documents and SLAs. In addition, as needed, ISE participants must reassess the validity of information to be discoverable and shared to ensure sustained applicability for use and integration within the ISE. ISE participants may store information within their respective ISE Shared Spaces or third parties may provide this through arrangements between the ISE participants and the internal originator of the information.

When considering an asset for the counterterrorism mission, each ISE participant should consider whether that asset is

1. Valuable to other ISE participants' counterterrorism missions.
2. Sufficiently documented and has defined and actionable performance metrics.
3. Related to any of the identified ISE mission business processes.
4. Available as reusable services.
5. Appropriately tagged.

implemented the Global Justice XML Data Model (Global JXDM) and the National Information Exchange Model (NIEM). These examples can be found at Internet site <http://www.it.ojp.gov/iepd/>.

³⁸ The standards for providing Web service descriptions are maintained by the World Wide Web Consortium (W3C). Documentation for this standard can be found at Internet site <http://www.w3.org/TR/ws-desc-reqs/>.

3.3.3.3 Gap Analysis

As potential business processes, information flows, practices, or rules are analyzed, ISE participants may identify related policy changes. This activity directly aligns the requirements indicated within FSAM Process Step 3 and ISEA ILC Stage 1 (*Analyze Business Processes*) and Stage 2 (*Identify and Categorize Candidate Assets for Sharing*) which examine the need to prepare a Gap Analysis Assessment. ISE Implementation Agents and ISE participants (to include intra-agency and cross-agency considerations) must evaluate and identify areas for improvement, based on possible ineffective, unused, or rigid processes that do not lend to enabling an effective and operational ISE.

Understanding what assets an ISE participant does not govern is equally important as being aware of what a participant does govern. The identification of these gaps is discovered by performing an asset gap analysis. Asset gap analysis is performed to identify the assets required to improve the business processes of the ISE participant. To create an asset gap analysis, ISE participants should use the following high-level procedures:

1. Leverage existing ISE-related mission business process analysis to identify asset gaps.
2. Identify gaps within the data, application, and service layers of segment architectures by assessing defined target architectures against current data application and service architectures to identify possible limitations in current design.
3. Identify and categorize asset types required (data, service, or application).
4. Coordinate SLAs with ISE Implementation Agents for service and application assets.

ISE participants should conduct this analysis, with the knowledge of what potential assets are available through the cross-ISE target mission analysis, in close collaboration with business process analysis.

At this stage, it is critical that ISE Implementation Agents and ISE participants be mindful of opportunities to add capabilities or features to their service or core capabilities that further the general goals of the ISE. Additions can include, for example, embracing new capabilities that implement new and emerging collaborative technologies or opportunities.

When gaps or modifications are identified, the initial reaction is to change the process/practices and improve the resources to support the need. Recognizing that some modifications are based on environmental circumstances and are beyond agency level control, ISE participants are encouraged to make appropriate adjustments while maintaining support and participation within the ISE.

3.3.4 FSAM Process Step 4: Define the Conceptual Solution Architecture

An ISE conceptual solution architecture is a structured, technical arrangement of documents, derived from the ISSA. It should be scoped to describe the particular functions or processes ISE participants will implement related to terrorism information, identify methods for achieving operational outcomes, and define specific IT assts, applications, and components for procurement and implementation.

Once the business process analysis and asset inventories are created, each ISE participant can begin to develop and enhance agency-level IT components to meet requirements identified within section 3.3.2 (*FSAM Process Step 2: Develop the Segment Scope and Strategic Intent*) and address any gaps identified, in conjunction with ISE Implementation Agents. This FSAM step continues to build on the analysis performed in each of the previous steps. Using the gap analysis and current asset inventory, new development and enhancement of data, service, and application assets can be targeted. Where gaps exist that cannot be filled with existing or enhanced components, new components should be developed. ISE participants and ISE Implementation Agents integrate newly developed, modified, reused, and/or enhanced IT components into their ISE Shared Spaces.

The process begins with establishing the ISE participant's assets as configuration items and resources to enable the operational mission processes. Each IT component must accommodate information security requirements and adhere to CTISS. Each component developed should directly support data, service, and application assets identified during the business process analysis and asset inventory stages and map to the ISE participants' ISSA. Similar to activities described in the ISEA ILC Stage 4 (*Develop or Enhance Information Systems*) and Stage 5 (*Integrate and Deploy Information Systems into the ISE*), this FSAM process step addresses the ISE requirements for each participant to leverage organization-level development procedures and makes the appropriate enhancements in support of ISSA and solution architectures performance requirements. As such, the conceptual solution architecture provides an integrated view of the combined systems, service, and technology, and the interfaces between them.

In building an ISE Shared Space within enterprise and/or segment architectures, each ISE participant determines the organization's shareable counterterrorism assets.³⁹

Some key questions posed during this stage include

- What risk is incurred if this information is shared?
- What risk is incurred if this information is not shared?

Once ISE participants document the expected results within an ISSA, the foundation is established for implementation of the solution architecture. ISE participants can then

³⁹ Assets are defined as the data, services, and applications within an organization's infrastructure.

execute those requirements leveraging ISE business, and CTISS standards and practices. For example, the *ISE-SAR Evaluation Environment Segment Architecture* describes those business and functional outcomes related to specific, terrorism-related suspicious activity reporting that will drive necessary programmatic and solution decisions consistent with ISE-SAR implementation.

The *FSAM* offers recommended key activities, tasks, and considerations for implementation of solution architectures. The section below highlights those activities and includes specific implementation detail related to the ISE mission business areas.

3.3.4.1 Assess Systems and Technology Environment for Alignment with Performance, Business, and Information Requirements

Leveraging the *Business and Information Requirements* described in section 3.3.3 and the *Scope and Strategic Intent* documented in section 3.3.2, this sub activity collects and analyzes the information pertaining to the “As-Is” use of systems and services and assesses how well these systems and services support the performance, business, and data architectures. This analysis provides ISE participants and ISE Implementation Agents the ability to determine and measure if the systems and services in the segment are performing to deliver business value for the costs associated with operating and maintaining them.

3.3.4.2 Identify Service and Solution Reuse Opportunities

Within the *FSAM*, there are discreet activities and tasks that promote opportunities for reuse of common services. ISE participants’ ability to leverage common enterprise solutions will enable those organizations to realize significant cost avoidance and cost savings when having to acquire associated standard IT hardware and software products. As ISE participants develop shared IT components, there is a reduced need to develop new components, leveraging shared assets to support information sharing. This is the foundation of using a Service Oriented Architecture (SOA). As more services become available, the ability to create composite applications to support the enterprise and segment architecture becomes easier and more cost efficient.

SOA is a paradigm for organizing and using distributed capabilities under the control of different ownership areas and implemented using various technology stacks. In general, entities (people and organizations) create capabilities to solve or support a solution for the problems they face in the course of their business. SOA provides a powerful framework for matching needs and capabilities, and for combining capabilities to address those needs by leveraging other capabilities. This framework is useful within the ISE to ensure common services are available. The *ISE EAF* aligns to the FEA Practical Guide Framework Service Oriented Architecture (PGFSOA) model. As with any other architecture, SOA can be expressed in a manner that is decoupled from implementation. Software architects generally use standardized conventions for capturing and sharing knowledge.

If new IT components are required, ISE participants should use the following high-level procedures:

- Use the ISE participant-specific development cycle to design and develop IT components
- Augment internal design artifacts with service or application specifications that instruct other ISE participants on procedures to leverage IT components and map to other ISE participants' enterprise architectures, including markings and handling instructions
- Create and execute IT component unit and integration test cases
- Update and enhance information exchanges to accommodate changes made during the development cycle
- Update and enhance SLAs to accommodate changes made during the development cycle
- Update information exchange schemas, service descriptions, and standards
- Develop standards-based translation (mediation) services to enable the exchange of information or data for each legacy component being leveraged
- Develop User Access Controls, as required, based on information restrictions and handling instructions.

3.3.5 FSAM Process Step 5: Author the Modernization Blueprint

This FSAM process step is the culmination of all the previous steps. Similar to activities described in the ISEA ILC Stage 5 (*Integrate and Deploy Information Systems into the ISE*), and Stage 6 (*Use, Maintain, and Evaluate the ISE*), FSAM Process Step 5 begins the iterative process of identification and categorization of findings, and the definition of associated transition options that address segment performance improvement opportunities. Additionally, ISE requirements are outlined for each participant to leverage mission-level development procedures and make the appropriate enhancements in support of their ISSA and solution architectures.

The key outcome of this step is a set of implementation recommendations validated by all stakeholders that contribute to a detailed, actionable segment architecture blueprint. Within the ISE, ISE participants are encouraged to follow FSAM during ISSA and ISE Shared Space development.

This page intentionally blank.

Chapter 4 – ISE Shared Spaces Development and Implementation

4.1 Overview

ISE Shared Spaces⁴⁰ are networked data and information repositories used to make standardized terrorism-related information, and applications and services accessible to all ISE participants (across the law enforcement, intelligence, homeland security, foreign affairs, and defense communities). Additionally, ISE participants may create or use their ISE Shared Space to make services and data accessible, as appropriate, to other organizations that participate in the ISE.

4.1.1 ISE Shared Spaces

An ISE Shared Space denotes infrastructure where segment and solution architectures are implemented leveraging CTISS or other ISE approved standards, and where each ISE participant makes terrorism information accessible to the ISE community. This infrastructure remains outside an ISE participant's internal network yet is under the management and control of that ISE participant.

The implementation of an ISE Shared Space and interface to the ISE Core facilitates access to information in the ISE for all ISE participants (Federal, State, local, tribal governments, the private sector and foreign partners).

4.1.2 ISE Shared Spaces Hosting Options

Various hosting and implementation options are available to establish a participant's ISE Shared Space. These hosting options include

- *Department Level:* A department, agency, or other ISE participating organization would establish an ISE Shared Space or multiple ISE Shared Spaces to facilitate terrorism information sharing for the entire organization, to include assigned bureaus and subordinate offices. The ISE Shared Space(s) would be interconnected with other ISE participants to provide access to standardized information.
- *Component/Other Level:* An organizational element or subcomponent of the larger department, agency, or ISE participant that would be responsible for establishing an ISE Shared Space supporting that component's responsibilities for interfacing with the ISE. An ISE Shared Space, established by this component, would be a portion of the network infrastructure operated and maintained by this component and would provide an ISE interface on behalf of the entire organization.

⁴⁰ See Appendix F of this document for additional information on ISE Shared Spaces development.

- **Third Party Level:** ISE participants may leverage the services and infrastructure of another third party service provider, who is a member of the ISE community, for “virtually” establishing their ISE Shared Space. ISE participants, leveraging a third party service provider to host their ISE Shared Space, should have well-defined service level agreements (SLAs) to address the issues of resourcing, management, continuity of operations, data stewardship, and ownership.

A detailed discussion of the ISE Shared Spaces concept is contained in Appendix F; a case study of an ISE Shared Space implementation is also presented in Chapter 5.

While an ISE Shared Space is unique to the organization it supports (Federal, State, local, tribal governments, the private sector and foreign partners), certain characteristics and requirements are common to all ISE Shared Spaces. This chapter addresses the implementation of an ISE Shared Space using the Hosting and Implementation Model, one of the ISE Shared Spaces implementation options discussed in Appendix F. Activities for development and implementation of an ISE Shared Space that adhere to the Hosting and Implementation Model include, but are not limited to

- System/Software Development Life Cycle
- ISE Shared Space Requirements
- ISE Shared Space Security
- Hardware and Software
- Software Development
- System Integration and Testing
- Other Implementation Considerations

4.2 System/Software Development Life Cycle

The System/Software Development Life Cycle is a proven standardized process that helps ensure that systems and software are developed to achieve outcomes and functionality that satisfy the specified goals (requirements).

The system/software development life cycle consists of four (4) separate and distinct phases: requirements definition, design (both high level and detailed), software implementation, and system integration and testing.

4.2.1 Requirements Definition

Requirements should be defined as completely as possible, leaving as little room for ambiguity as possible. Completion of the requirements definition phase should be accomplished by a signed agreement between the developing organization and the organization implementing all the requirements of the system.

The *ISE EAF*, CTISS Functional and Technical Standards, and Chapter 3 of this *PAIS* provide derived requirements that ISE participants can use when implementing their ISE Shared Space. ISE participants should consider adherence to a SOA-based methodology and the reuse of previously developed applications, services, and functionality when mapping the defined requirements to the design phase.

4.2.2 Design

4.2.2.1 High Level

Upon completion of the requirements phase, work should commence on the high-level design of the system. At this point requirements are mapped into broad functionality. The ISE Shared Spaces high-level design should leverage the ISE Shared Spaces and ISE Core services architectural concepts identified within the *ISE EAF*, the ISE Shared Spaces concept outlined in Appendix F of this *PAIS*, and the *ISE-SAR EE Segment Architecture*.⁴¹ The *high-level* design phase is concluded with a Design Review (DR), which ensures that the *high-level* design defines the functionality documented in the requirements phase.

4.2.2.2 Detailed Design

Upon completion of the high-level design phase, work should commence on the detailed design of the system. Detailed design provides the programmers the applications and/or functionality with all information necessary to complete the code development. ISE Shared Spaces design should include review of the technical specifications of the ISE Implementation Agent provisions to access the ISE Core, examination of Information Exchange Package Documentation (IEPD) and Extensible Markup Language (XML) schemas for storage, and adherence to CTISS Functional and Technical Standards.

The detailed design phase is concluded with a Critical Design Review (CDR) with representatives from the development organization (designers, programmers and IT security) meeting with the implementers and determining that the design defines the functionality documented in the requirements and high-level design phase. CDR coverage includes reviewing ISE Shared Space interfaces to ISE Implementation Agents, ensuring standards are baselined, and that all requirements are mirrored by applicable functionality.

4.2.3 Software Implementation

The software implementation process commences once the detailed design has been accepted by the ISE participant. Developers implement all code directly from the detailed design. Deviations from the design should be reviewed with the design

⁴¹ PM-ISE, *ISE-SAR EE Segment Architecture*, can be found at <http://www.ise.gov>.

personnel, ensuring that the code functions as required and that interfaces between functionality are consistent between applications.

During the coding phase programmers are responsible for ensuring that all code developed meets the requirements, as specified, and unit testing (testing of each application component individually) is completed. As each application and/or unit is completed, interoperability between applications should be tested using mock data as part of sub-system testing.

4.2.4 System Integration and Testing

As applications and/or functionality are completed and tested against each other, the entire system should be integrated with the required/prescribed hardware configuration. This process, termed System Integration and Testing, provides the final phase of the development process. It is during this phase that all software functionality is tested using the specified hardware and the connections to other systems.

This phase is completed with a formal series of tests run by the development organization to show the procuring organization that the system meets or exceeds all requirements and provides the required functionality.

4.3 ISE Shared Space Requirements

The requirements for building an ISE Shared Space are defined as follows:

4.3.1 Inputs

- An ISE Shared Space shall be able to accept applicable (i.e., properly formatted) inputs.
- An ISE Shared Space shall be able to accept inputs from the authorized databases or data stores via an automated transfer process.
- Users shall be authorized via the identified ISE Core before being able to submit queries to an ISE Shared Space.
- An ISE Shared Space shall accept federated queries from other ISE Shared Spaces.
- Authorized users shall be able to submit a federated query to the system requesting selected records.

4.3.2 Process

- An ISE Shared Space shall accept CTISS-compliant Functional Standard records and process them through the Extract, Translate, and Load (ETL) function while operating within the appropriate ISE privacy guidelines (see Section 1.4). The ETL process performs the following functionality:

- Extracts data from the applicable data store on the current operating system.
- Transforms the data extracted from the current operating system into the format specified and agreed to in the CTISS Functional Standard. This conversion includes all applicable code values, date and time formats, etc.
- Creates the proper XML (which adheres to IEPD specifications) file.
- Removes the actual personal information (as identified by the Functional Standard “privacy fields”) when generating the XML, including only applicable metadata (authorized by the originating organization).
- Loads the converted data, inclusive of schema updates, into the data store on the ISE Shared Space server, or converts data as it is passed from the third party broker directly to the requestor.
- The system will send data to an ISE Shared Space, but prior to that data being stored in an ISE Shared Space database, it shall be processed through the ETL.
- ETL processing is unique to each organization because of the type of data being sent to an ISE Shared Space system. Federal, State, local, tribal government, private sector, and foreign partner organizations maintain their IEPD record information in any of a number of formats containing multiple types and sets of data. The ETL shall take the data as it exists in the current system and
 - Extract personal information from the record and electronically verify that it has been cleansed in accordance with ISE privacy guidelines.
 - Translate the remaining data into a format (XML schema) consistent with the CTISS Functional Standards.
 - Load the reformatted CTISS Functional Standard compliant record into the ISE Shared Space database.
- An ISE Shared Space shall store all ETL-processed records in the ISE Shared Space database as specified in the *ISE EAF*.
- CTISS Functional Standard compliant records shall be available for review via a federated query, per section 6.4.8.2 of the *ISE EAF*.
- Users shall have the capability to submit a request for CTISS Functional Standard records via a federated query.
- Federated queries shall have the capability to request records from multiple ISE Shared Spaces (federated queries will be available to users of an ISE Shared Space but are not a development requirement of an ISE Shared Space).
- An ISE Shared Space shall have the capability to respond to federated queries generated by other ISE Shared Spaces and processed through the ISE Core.

- An ISE Shared Space shall develop and maintain an audit log of all information and requests that transpire on the ISE Shared Space system. All audit log information shall be shared with the requestor's home organization and maintained in the system for one year.
- Administrators shall have the capability to request local audit log information.
- For auditing purposes, the search capability shall collect data on the requestor. This data shall be stored in an audit log.

4.3.3 Outputs

- Local users shall receive query results online in electronic format.
- An ISE Shared Space shall send the results of a federated query to the requestor in electronic format.

4.3.4 General Requirements

- Version Control – All software developed for an ISE Shared Space shall be controlled using version control either via an internal mechanism or via third party commercial off-the-shelf (COTS) software. (Many third party version control applications exist including a number that are free to the developer.)
- Administrator Capabilities – An ISE Shared Space system shall possess administrator capabilities so that an administrator is able to maintain the system. Such capabilities include, but are not limited to
 - Maintaining network connectivity.
 - Managing system backups.
 - Monitoring and managing the load on the system (either directly or through the enterprise load balancer).
 - Managing the removal of old or obsolete data from the system.
 - Adding connectivity to new workstations, etc.
- Training – There shall be the ability for the organization's personnel to provide training to new users of the system. Such training may use "real" data or may use data generated expressly for training purposes.

4.3.5 Summary of ISE Shared Space Requirements

Figure 4-1 depicts how an ISE Shared Space can be implemented. At a minimum, the ISE Shared Space is connected to the current system on one end and to other ISE Shared Spaces via the ISE Core on the other end.

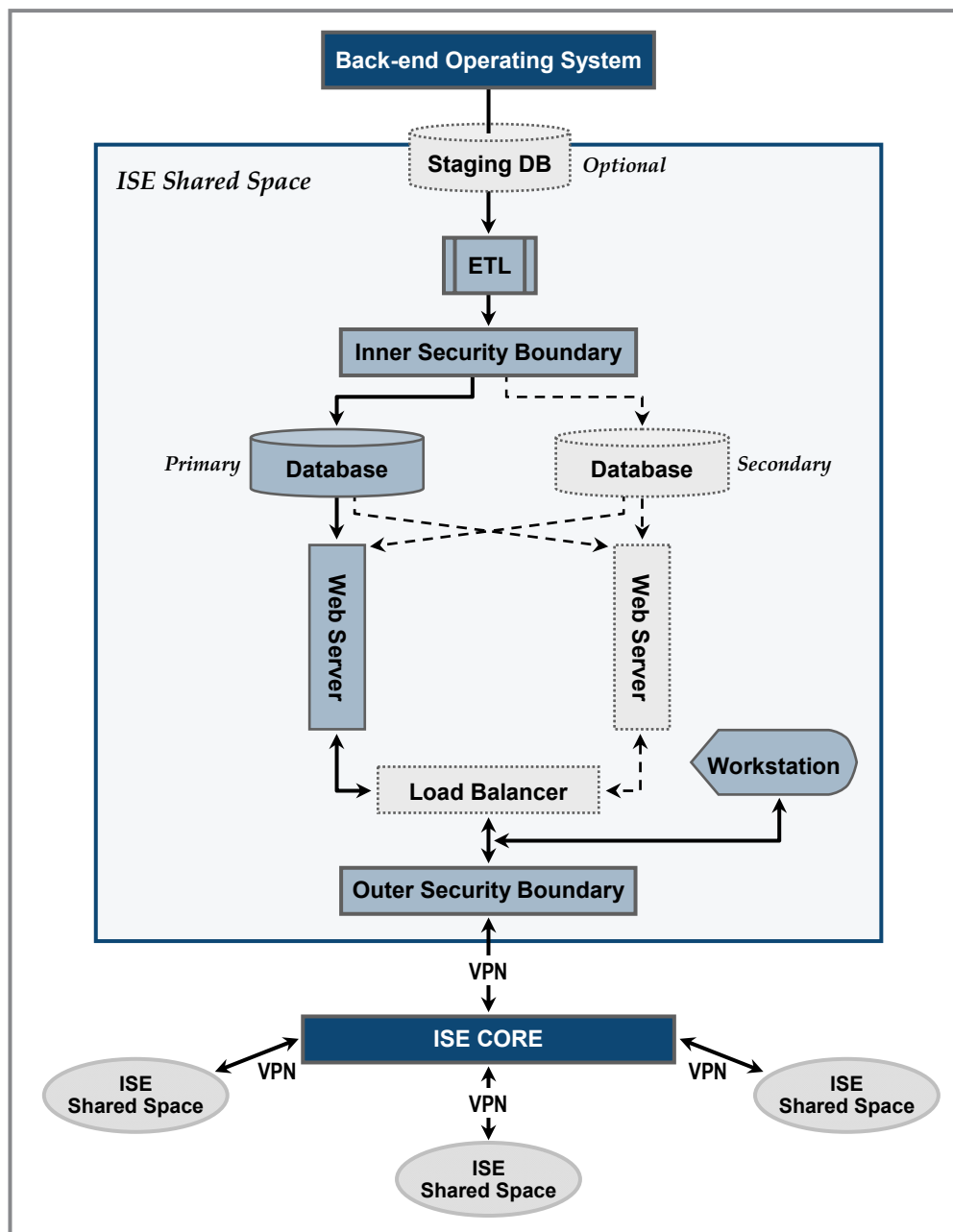


Figure 4-1. Conceptual ISE Shared Space implementation

Data is received from the current system either directly, or as recommended, via a staging database. Once the data is received it is processed through the ETL application and data is then stored in the ISE Shared Space database. Data stored in the ISE Shared Space can be accessed locally by authorized users or via the ISE Core by other ISE Shared Spaces, utilizing Virtual Private Network (VPN) point-to-point (P2P) transfer over the Internet which is used as a transport medium.

Figure 4-1 further depicts the implementation recommended to support 99.99% availability. In order to provide redundancy and failover, it is recommended that multiple servers and a load balancer be implemented to provide the minimum redundancy required.

4.4 ISE Shared Space Security

The requirements necessary to satisfy security issues when developing an ISE Shared Space are many and varied. To understand the in-depth aspects and detailed requirements as they apply to security in the development of the ISE Core and ISE Shared Space, refer to the *ISE IA Technical Standard* (ISE-G-106), *ISE IdAM Framework* (ISE-G-108) and Appendix G of this document.

Security aspects for consideration when developing an ISE Shared Space fall into three (3) categories:

1. Connectivity between the current system and the ISE Shared Space
2. Connectivity between the ISE Shared Space and the ISE Core
3. Security within the ISE Shared Space

4.4.1 Current System and ISE Shared Space Connectivity

ISE data is transferred from the current system to the ISE Shared Space either directly or via a staging database that sits outside the ISE Shared Space. Although a staging database is not required, it is recommended and can be used as the delimiter between the current system and the ISE Shared Space. ISE data is sent to the ISE Shared Space for processing by the ETL. Between the staging database (and current system), an inner security boundary should exist that prevents unauthorized intrusion. Refer to section 4.5.3 Firewall/VPN for a discussion regarding firewall requirements and Appendix G for an in-depth discussion on security and IdAM.

Data transfer between the current system and the ISE Shared Space is one way: data is input into the system, modified as required, and stored in the ISE Shared Space database. Movement of data out of the ISE Shared Space back to the current system is neither required nor supported and therefore should be prevented.

Should personnel from the current system need access to ISE data residing in the ISE Shared Space, they are required to access all data as an authorized user on an ISE Shared Space.

4.4.2 ISE Shared Space(s) and ISE Core Connectivity

Each ISE Shared Space is a unique entity within the ISE. Each ISE Shared Space is connected to other ISE Shared Spaces via the ISE Core. Federated queries are routed to other ISE Shared Spaces via the ISE Core utilizing VPN tunneling. It is the responsibility of each ISE Shared Space owner to ensure that data requests coming from the ISE Core or data being transmitted directly from an ISE Shared Space are authorized and not corrupted by outside influences.

Each ISE Shared Space user connects to a central Web portal to submit a query. The portal software brokers the query, forms the federated query for a selected set of ISE Shared Spaces, and coordinates and manages the communication to execute the query.

4.4.3 Security within an ISE Shared Space

Within an ISE Shared Space, data is stored, manipulated and retrieved from an ISE Shared Space database via the Web server. Security considerations for each of these applications are discussed in Appendix G.

4.4.3.1 Database

The database shall be configured in such a manner as to

- Store only records sent via the ETL
- Respond only to data requests from an ISE Shared Space web server

The database shall maintain a detailed audit log of all requests processed by the database, including but not limited to

- All record requests
- Any request to store data not received from the ETL
- Any request for data originated by the ISE Core

4.4.3.2 Web Server

The Web server is responsible for processing all requests for data from the database. The Web server shall be configured to accept data requests from two distinct origins: a local user or via a federated query from the ISE Core. The Web server shall maintain a detailed audit log of all requests including, but not limited to

- All record requests
- All requests not generated by an internal user
- All requests not originated by the ISE Core

4.5 Hardware/Software Configuration

The following table lists, at a minimum, an example of current technology best practice implementation of the hardware required to set up and host an ISE Shared Space.

Table 4-1. ISE Shared Space Hardware Requirements

Hardware	Minimum	Fault Tolerant
Server	Single Server	Multiple Servers
Load Balancer	N/A	Yes
Firewall	Yes	Yes
Router	Yes	Yes
Web Application Server	HTML Capable	Rapid Web Dev Software

4.5.1 Server(s)

Each server used in an ISE Shared Space should contain, at a minimum, the following components:

- Multi-core processor, minimum 2.6 GHz
- 4-GB RAM
- Four 250-GB hot swappable hard drives
- Two 1-GB Network Interface Cards (NIC)
- Redundant Array of Independent Disks (RAID) Controller
- Operating system
- Relational Database Management System (RDMS)
- CD-RW/DVD ROM drive

It is recommended, but not required, that an ISE Shared Space be a fault-tolerant system with failover capabilities. If it is determined that an ISE Shared Space needs to be a fault-tolerant system, it is recommended that an additional server be added to the configuration to ensure complete failover. Refer to Figure 4-1 for a sample configuration.

4.5.2 Load Balancer

If an organization has determined that it requires its ISE Shared Space to be available at all times, the developing organization should employ a redundancy failover system. An enterprise load balancer is one component of a redundant failover system.

Load balancing is the process by which load (number of requests, number of users, etc.) is spread throughout a network so that no individual device becomes overwhelmed

by too much traffic, causing it to fail. Load balancing also involves redirection in the case of server or device failure to allow for failover and promote fault tolerance. A hardware load balancer usually consists of three (3) servers: two servers processing the requests and a third server directing (load balancing) requests between the two servers. In case one server fails, the load balancing server redirects all traffic to the remaining server until the failed server is put back into service.

4.5.3 Firewall/VPN

To protect data and services from being compromised, a high-level firewall with VPN capabilities is recommended for use in the ISE Shared Spaces environment.

The following are capabilities that should be considered when choosing enterprise level firewall technology:

- Trusted Firewall Technology – Flexible policy capabilities prevent unauthorized access to network resources or vital corporate information
- Threat-protected VPN
- Adaptive design
- Easy deployment and management

A well-designed VPN uses several methods for keeping ISE participants' connection and data secure:

- Firewalls

A firewall provides a strong barrier between an ISE participant's private network and the Internet. The ISE participant can set firewalls to restrict the number of open ports, what type of packets are passed through, and which protocols are allowed through. Some VPN products can be upgraded to include firewall capabilities by running the appropriate Internetwork Operating System (IOS) on them. ISE participants should have firewalls in place before implementing a VPN; firewalls can also be used to terminate the VPN sessions.

- Encryption

Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Most computer encryption systems belong in one of two categories:

- Symmetric-key encryption⁴²
- Public-key encryption⁴³

⁴² Encryption algorithms that use the same key for encrypting and for decrypting information are called symmetric-key algorithms. The symmetric key is also called a secret key because it is kept as a shared secret between the sender and receiver of information.

- Internet Protocol Security (IPSec)

IPSec provides enhanced security features such as better encryption algorithms and more comprehensive authentication.

IPSec has two encryption modes: tunnel and transport. Tunnel encrypts the header and the payload of each packet while transport encrypts only the payload. Only systems that are IPSec-compliant can take advantage of this protocol. In addition, all devices must use a common key and the firewalls of each network must have established similar security policies. IPSec can encrypt data between various devices, such as:

- Router to router
- Firewall to router
- PC to router
- PC to server

- Authentication, Authorization and Accounting (AAA) Server

AAA servers are used for more secure access in a remote-access VPN environment. When a request to establish a session comes in from a dial-up client, the request is proxied to the AAA server. AAA then checks the following:

- Who you are (authentication)
- What you are allowed to do (authorization)
- What you actually do (accounting)

The accounting information is especially useful for security auditing, billing or reporting purposes.

4.5.4 Web Application Server

A Web application service will allow developers to provide a web interface to the user for accessing the applicable CTISS compliant Functional Standard records. While no specific web application server is required, it is recommended that one be used that allows the developers to rapidly develop functionality that can be incorporated into the system.

While web applications can be developed using many products or even developed in-house, using a rapid application development product and methodology will provide the development organization with a platform not only to complete the initial development but also to extend the applications as new requirements for an ISE Shared Space are identified and required for implementation.

⁴³ Encryption algorithms that use different keys for encrypting and decrypting information are most often called public-key algorithms but are sometimes also called *asymmetric key algorithms*. Public key encryption requires the use of both a private key (a key that is known only to its owner) and a public key (a key that is available to and known to other entities on the network).

4.6 Software Development

As part of the design and implementation process, ISE participants should consider all aspects of software development including, but not limited to, SOA, Web services, and reuse of existing applications, services, functionality, and systems or components previously developed and/or implemented outside the ISE Shared Space development environment.

4.6.1 Data Flow into an ISE Shared Space

1. On a scheduled basis, electronic data is transferred from the local database to an ISE Shared Space.
2. Prior to storing that data in an ISE Shared Space database, the data must be processed by ETL to remove any personal information, as appropriate, from the record and reformat the existing data into an XML schema that meets CTISS Functional Standard requirements.
3. The new formatted record will then be stored in an ISE Shared Space database and shall be available to authorized users for sharing within the ISE.

Note: It is not a requirement of the current system to stage data prior to the data being sent to an ISE Shared Space. Therefore, the current system may push its entire data store to an ISE Shared Space for processing each time a data transfer is performed. This activity will necessitate that the ETL process all records each time a data transfer from the current system is performed. Although not a requirement, it may be beneficial to set up a staging database that will allow the system to review records and pass only the new or updated records to the ETL for processing.

4.6.2 Query Request

1. User accesses an ISE Shared Space via an authorized access method.
2. User submits a local ISE Shared Space request.
3. An ISE Shared Space processes the request and gathers all reports meeting the search criteria.
4. An ISE Shared Space formats the response.
5. An ISE Shared Space presents all returned data to the user electronically.

4.6.3 Federated Query Request

1. User accesses an ISE Shared Space via an authorized access method.
2. User submits a local ISE Shared Space request.
3. An ISE Shared Space processes request and sends request to the ISE Core.
4. An ISE Shared Space waits for federated query response to come from other ISE Shared Spaces.

5. An ISE Shared Space formats federated query response.
6. An ISE Shared Space presents all returned data to the user electronically.

4.6.4 Federated Request Response

1. An ISE Shared Space receives federated query from the ISE Core.
2. An ISE Shared Space processes the federated query, gathering all reports that meet the search criteria.
3. An ISE Shared Space formats the federated query response.
4. An ISE Shared Space sends formatted federated query response to the originating ISE Shared Space.

4.7 System Integration and Testing

Once development is complete, the ISE Shared Space software should be integrated with the hardware required to host the system. This system integration should be accomplished using a non-production environment that exactly duplicates the production environment. Each component of the system should be tested, and simulated connections to the current operating system environment, the ISE Core, and other ISE Shared Spaces should be implemented to ensure that the system works as intended. As part of the final system testing, live connections (where possible) should be established to each externally connected system to test the connection, data flow, and processes.

Upon successful system integration testing, the ISE Shared Space should be implemented into the production environment.

4.8 Other Implementation Considerations

The developing organization may want to consider some of the following additional implementation issues.

4.8.1 Development, Testing, and Production Environment

It is recommended that when developing an ISE Shared Space system, three separate and distinct environments should be used. Development can be accomplished in many smaller separate environments such as at individual personal computers or workstations. As each piece of functionality is completed, it should be transferred to a central repository and controlled using version control software (refer to general requirements in Section 4.3 ISE Shared Space Requirements). This repository should contain the official version of all code as it is developed. It is the code that resides in the development libraries that should be used for sub-system testing. Code can also be transferred to a separate testing environment when system testing commences. When problems in the code are identified, fixes or modifications to the code should always be

made in the development libraries under strict version control to ensure that a baseline of code always exists.

4.8.2 Additional Recommendations

- Fail Over/Redundancy – It is recommended that each ISE Shared Space consist of multiple servers with a separate load balancing server supporting the ISE Shared Space servers. Each server should consist of a minimum of four (4) hot swappable disk drives supporting a minimum RAID 1. Utilizing load balancing technology and multiple redundant servers, each ISE Shared Space should be able to maintain 99.99% availability.
- RAID 1 – It is recommended that each server have at a minimum RAID 1 capability so that should one hard drive on the server fail, no data will be lost and the system will continue to function without any loss of data, functionality, or performance.

RAID Level 1 is usually referred to as mirroring. A Level 1 array provides redundancy by duplicating all the data from one drive on a second drive so that if either drive fails, no data is lost. Higher RAID levels such as RAID 0+1 or 10 may also be employed. RAID 10 is a combination of RAID Levels that utilizes multiple RAID (mirrored) sets into a single array. Data is striped across all mirrored sets. As a comparison to RAID 5, where lower cost and fault tolerance is important, RAID 0+1 utilizes several drives to stripe data (increased performance) and then makes a copy of the striped drives to provide redundancy. Any disk can fail and no data is lost as long as the mirror of that disk is still operational. The mirrored disks eliminate the overhead and delay of parity. This level array offers high data transfer advantages of striped arrays and increased data accessibility (reads). System performance during a drive rebuild is also better than that of parity based arrays since data does not need to be regenerated from parity information but rather is copied from the other mirrored drive.

- Database Synchronization – If a Fail Over/Redundancy system is employed, ISE participants should consider ensuring that the databases between the multiple servers residing behind the load balancer are synchronized at all times. For enterprise-level environments, consideration should be given to utilizing a clustered database environment.

This page intentionally blank.

Chapter 5 – Case Study: Washington, DC Metropolitan Police Department (MPD) ISE Shared Space

The following scenario demonstrates the application of the ISE Architecture Implementation Life Cycle discussed in Chapter 3 and the ISE Shared Spaces development and implementation overview presented in Chapter 4. *Included solely for illustration, the scenario is intended to be a non-prescriptive description of how ISE participants might implement an ISE Shared Space.* The ISE Shared Space implementation at MPD demonstrates the usage of the concepts introduced in the *ISE EAF*, the *ISE-SAR Evaluation Environment Segment Architecture*,⁴⁴ and the previous four chapters of this document to implement an ISE Shared Space.

Note: The PM-ISE does not endorse or recommend specific vendor-based solutions; vendor references are for documentation completeness of the MPD Case Study. This Case Study represents one appropriate implementation of an ISE Shared Space. The Washington, DC MPD tailored the actual implementation to meet the short operational schedule.

5.1 Overview

Washington, DC was selected as one of the twelve (12) sites to participate in the ISE-SAR Evaluation Environment. In order to support the emergent requirements of the Presidential Inauguration on January 20, 2009, MPD and PM-ISE agreed to expedite the implementation of the SAR process, including the sharing of ISE-SAR with other law enforcement agencies supporting the Inauguration through an ISE Shared Space. This support included building an ISE Shared Space and connecting that ISE Shared Space to the DC MPD Alert Management System (AMS), which contains un-vetted MPD SAR information. Once vetted, the ISE-SAR would be sent from the AMS to the ISE Shared Space in the *ISE-SAR Functional Standard* format. For the purposes of the Inauguration, SARs that met the criteria for referral to the Joint Terrorism Task Force (JTTF) were inputted directly via VPN into the Federal Bureau of Investigation's (FBI's) eGuardian⁴⁵ system. Currently, the Department of Justice (DOJ) and the FBI are establishing an interface between eGuardian and their ISE Shared Space.

⁴⁴ The *Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Concept of Operations (CONOPS)* and *ISE-SAR EE Segment Architecture* can be found at <http://www.ise.gov>.

⁴⁵ The eGuardian system enables near real-time sharing and tracking of terror information and suspicious activities with the FBI's Federal, State, local, and tribal partners. eGuardian is a spin-off of a similar but classified tool called Guardian that the FBI uses to share information with vetted partners. Additional information on eGuardian can be found at <http://www.fbi.gov>.

5.2 DC MPD's Alert Management System

The AMS is MPD's analytical environment for vetting all criminal SAR information for the Washington, DC metro area. AMS has multiple functions: a secure Web-based user interface for inputting data; a defined workflow for vetting the information in AMS; options for providing police officer status and availability; and serves as the storage mechanism for citizen tips and leads and suspicious activity data. The AMS system also provides the ISE-SAR data elements (in the *ISE SAR Functional Standard* format) used to populate the associated MPD ISE Shared Space.

5.3 Data Analysis and Migration Process

Data flows into the AMS from various sources, such as the citizen tip hotline (via telephone and Web interface), MPD Officer Reports, information from the business community, etc. All data gathered from the sources listed above is entered into tips forms; the information is verified for clarity; and then the forms are filed in the AMS database. MPD analysts review the information and determine whether the information meets the threshold for an ISE-SAR. If it is determined that the information is an ISE-SAR, the analyst sets a flag in the record "tagging" it as an ISE-SAR. By setting this flag, the record is sent from the AMS internal data system to the MPD ISE Shared Space. If the SAR meets the threshold for referral to the JTTF as a terrorism investigative lead, an additional flag is set and a copy of the SAR file is sent to eGuardian from the ISE Shared Space.

At scheduled intervals all records tagged as SAR records are electronically transferred from the AMS database to a staging database that is separate and distinct from the AMS. This database contains all information required for record input to the MPD ISE Shared Space.

5.4 MPD's Implementation of ISE Shared Space

This section describes the actual MPD ISE Shared Space configuration implemented for the Washington, DC MPD Fusion Center in support of its SAR operations. This discussion is broken into five (5) parts: hardware specifications and configuration, software infrastructure, security, interfaces, and integration configuration. In addition, there are sections titled "Project Results" and "Future Considerations," which are based upon phased-in system requirements not yet achieved.

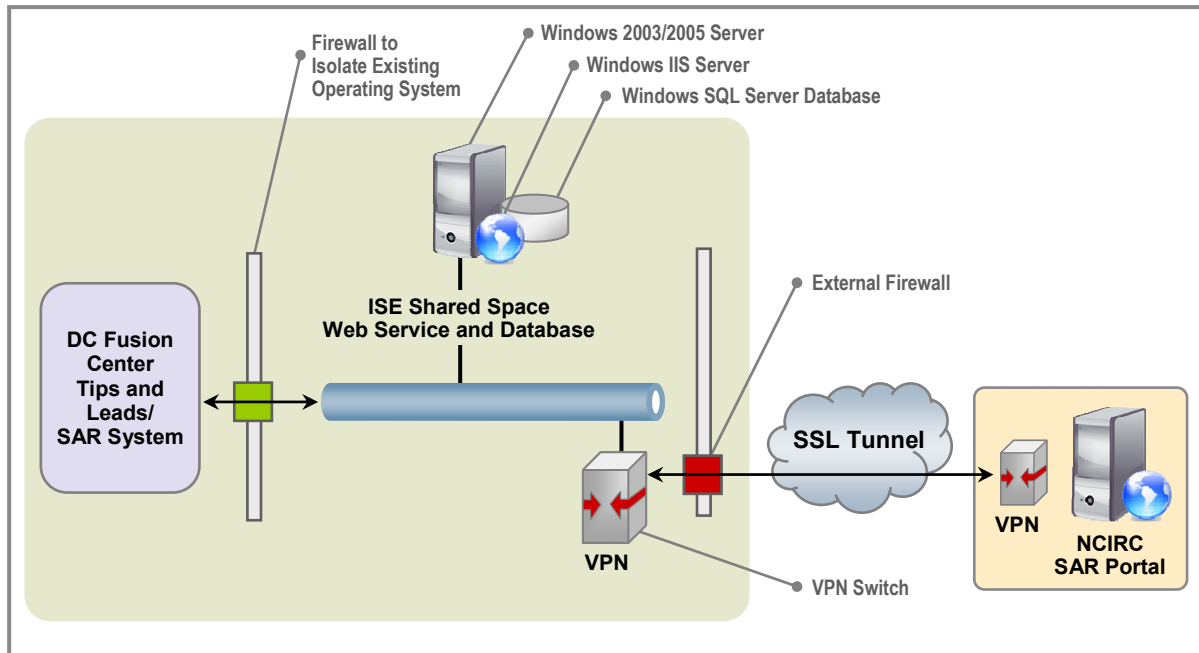


Figure 5-1. Detailed Component Layout

This illustration shows how the components of the ISE Shared Space server were configured at the DC MPD. The firewalls separating the various components are depicted as Proxies. The firewall devices were programmed with appropriate routing rules to provide effective isolation between the National Criminal Intelligence Resource Center (NCIRC) and the current DC MPD operating system.

5.4.1 Hardware Specifications and Configuration

The hardware specifications listed below represent the computer server platform used to build the MPD ISE Shared Space. The software configuration residing on the server consists of a Database Management System (DBMS); a web server; a Secure File Transfer Protocol (SFTP) server; operating system; and an ETL utility.

Table 5-1. Hardware Specifications

Quad Core Xeon E5420 Processor 2x6 MB Cache, 2.5 GHz, 1333 MHz FSB, PE2950
4 GB 667 MHz (4x1 GB), Dual Ranked Fully Buffered DIMMs
LOM NICs are TOE Ready
146 GB 15K RPM Serial-Attach SCSI 3 Gbps 3.5-in HotPlug Hard Drive
PERC6i SAS RAID Controller, 2x4 Connectors, Int, PCIe, 256MB cache, x6 Bkpl
No Floppy Drive for x6 Backplane
Windows Server 2003 R2 Standard Edition with SP2 Includes 5 CALs
Onboard Broadcom 5708 1GBE Networking
24X IDE CD-RW/DVD ROM Drive

Bezel for PE 2950
1x6 Backplane for 3.5-inch Hard Drives
Electronic Documentation and OpenManage DVD Kit
146GB 15K RPM Serial-Attach SCSI 3 Gbps 3.5-in HotPlug Hard Drive
Integrated SAS/SATA RAID 5, PERC 6/i Integrated
Universal Sliding Rapid/Versa Rails, includes Cable Management Arm
Redundant Power Supply with Y-Cord
Power Cord, NEMA 5-15P to C14,15 amp, wall plug, 10 feet / 3 meter
Microsoft SQL Server 2005 Standard (1 Socket), OEM, NFI Includes Media
146GB 15K RPM Serial-Attach SCSI 3 Gbps 3.5-in HotPlug Hard Drive
146GB 15K RPM Serial-Attach SCSI 3 Gbps 3.5-in HotPlug Hard Drive
146GB 15K RPM Serial-Attach SCSI 3 Gbps 3.5-in HotPlug Hard Drive

5.4.2 Software Infrastructure

The software components configured and implemented in the MPD ISE Shared Space server included

- Operating System – The MPD ISE Shared Space server components were deployed on a server grade computer executing the Windows Server (Windows 2003) operating system.
- Web Server – Internet Information Service (IIS) Web Server (part of the Microsoft Server Platform).
 - A Web server is a computer program that is responsible for accepting Hypertext Transfer Protocol (HTTP) requests from *clients* (user agents such as Web browsers), and serving them HTTP responses along with optional data contents, which usually are Web pages such as Hypertext Markup Language (HTML) documents and linked objects (images, etc.). In practice many Web servers also implement the following features:
 - Authentication, optional authorization request (request of user name and password) before allowing access to some or all resources.
 - Handling of static content (file content recorded in server's file system(s)) and dynamic content by supporting one or more related interfaces (SSI, CGI, SCGI, FastCGI, JSP, PHP, ASP, ASP.NET, Server API such as NSAPI, ISAPI, etc.)
 - HTTPS support (by secure socket layer [SSL] or transport layer security [TLS]) to allow secure (encrypted) connections to the server on the standard port 443 instead of usual port 80.
 - Content compression to reduce the size of the responses (to lower bandwidth usage, etc.).

- Virtual hosting to serve many websites using one IP address.
- Large file support to be able to serve files whose size is greater than 2 GB on 32 bit operating systems (OS).
- Bandwidth throttling to limit the speed of responses in order to not saturate the network and to be able to serve more clients.
 - The IIS Web Server hosts the ISE Shared Space Server Web Service and is the only component visible from the MPD ISE Shared Space server environment. In general terms, the Web services support two interfaces. The first interface supports three methods to retrieve SAR data while the second interface supports two methods to return audit logs and the status of data loads into the database server.
- Database Management System – the Database Management System is the focal point of the MPD ISE Shared Space providing SAR record storage and retrieval services. Using a database management system allows for efficient storage of SAR and provides the means to retrieve data utilizing advanced search techniques. MPD utilizes MS-SQL Server Database MS-SQL 2005. The MPD ISE Shared Space server database contains the following attributes:
 - A star schema layout includes all of the searchable information in the SAR records logically grouped into flatter, de-normalized data tables. Borrowing the concept from data warehousing, these would be referred to as dimensions.
 - The dimension tables form associations with the SAR and Suspicious Activity related metadata. This metadata would support the tagged data elements outlined in the *ISE-SAR Functional Standard*.
 - The SAR XML record itself is generated when the data is loaded from the current system, stored in its entirety, and is associated with the SAR metadata (as indicated in Figure 5-2).
 - The dimensions, designed in accordance with the data elements and model detailed in the *ISE-SAR Functional Standard*, represent the following entities:
 - SAR/Suspicious Activity Metadata: Contains information about the tip itself, its code/classification, the date and time when reported, and the date and time when the suspicious activity was observed.
 - Person: Houses all of the searchable information about the person but is contained in a single table.
 - Location: Contains information about the location of the suspicious activity.
 - Target: Contains information about the intended target of the suspicious activity.
 - An example of an ISE Shared Spaces database entity relationship diagram (ERD), which conforms to the *ISE-SAR Functional Standard*, is shown in Figure 5-2.

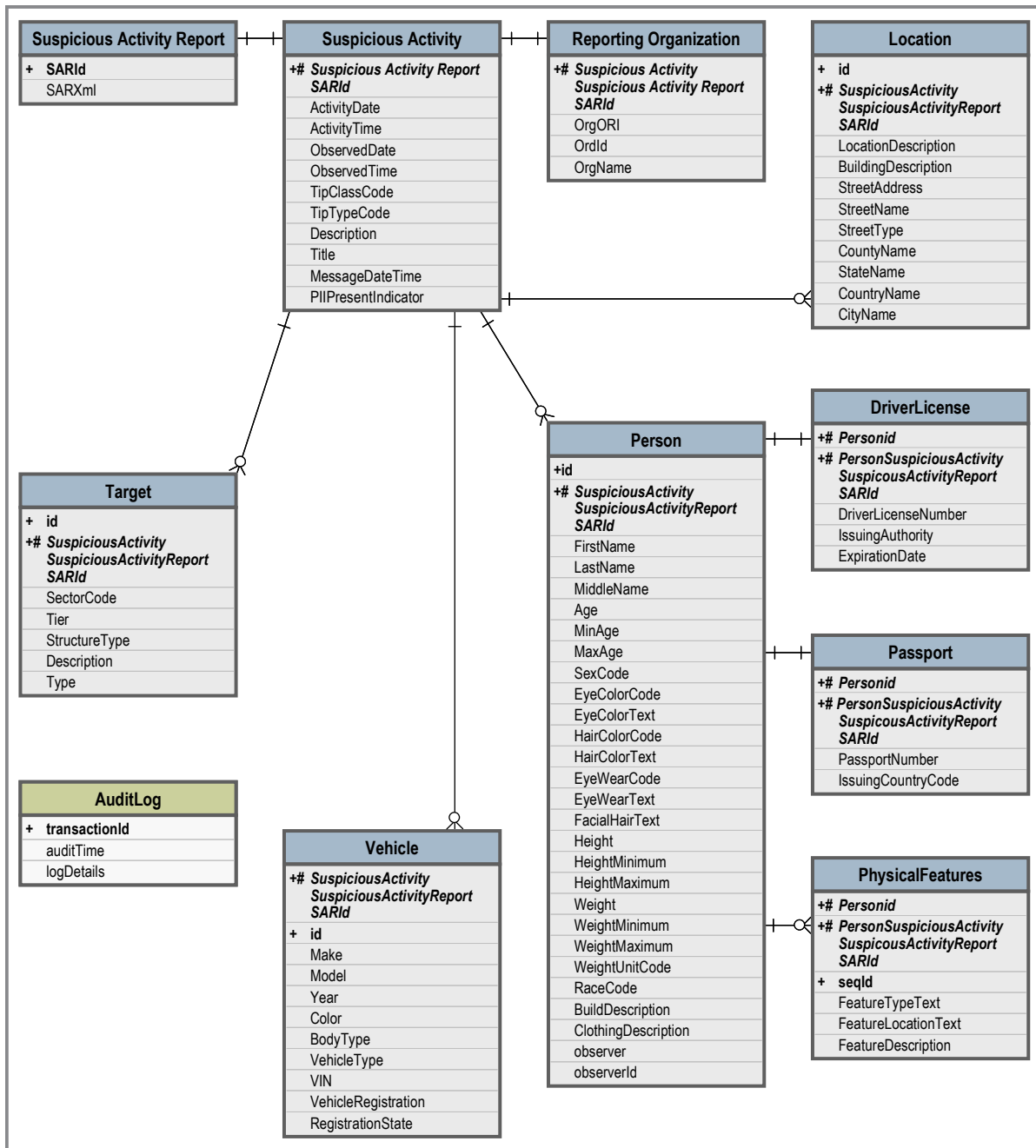


Figure 5-2. Example: ISE Shared Space Server Database Entity Relationship Diagram

- Additionally, the database server supports searches on the SAR Narrative and SAR Title. The current implementation involves using the text search capabilities of the database server and making the search results available to the querying entity.

- ETL – This process will be used to map existing data into the common format of the ISE Shared Space server database.
- The database server is used to perform ETL operations. The ETL scripts were built specifically to perform the following tasks:
 - Transform the data from the current format into the format specified in the *ISE-SAR Functional Standard*. This conversion includes transformation of the code values, date and time formats, etc.
 - Load the data published by the existing operating systems into the star schema database of the MPD ISE Shared Space Server.
 - Create the SAR XML (meeting the *ISE-SAR Functional Standard* specification) and store it into the appropriate table.
- File Transfer Protocol (FTP) Server – SFTP Server file transport.
 - The server is configured with an SFTP server that was used to receive data from the current system. The SSH File Transfer Protocol (sometimes called Secure File Transfer Protocol or SFTP) is a network protocol that provides file transfer and manipulation functionality over any reliable data stream. It is typically used with version two of the secure socket handler (SSH) protocol transmission control protocol ([TCP] port 22) to provide secure file transfer but is intended to be usable with other protocols as well.

5.4.3 Security

Security components configured to protect the MPD ISE Shared Space server from unauthorized access included firewalls, a VPN Router deployed between existing operating systems and the ISE Shared Space, and a Web portal interface.

5.4.4 Interfaces

The MPD ISE Shared Space server interfaces with the web-based federated search/retrieval engine that executes on the NCIRC⁴⁶ portal platform. Submitted requests for information from the MPD ISE Shared Space server through the NCIRC portal are processed after being properly authenticated at the Law Enforcement Online (LEO), Homeland Security Information Network (HSIN), or Regional Information Sharing Systems Network (RISSNET™). In order to better support the automated interfaces and to ensure interoperability with a growing set of applications, the MPD ISE Shared Space

⁴⁶ NCIRC, is a secure website accessible via Law Enforcement Online (LEO) and the Regional Information Sharing Systems Network (RISSNET™). The NCIRC website contains information regarding law enforcement intelligence operations and practices and provides criminal justice professionals with a centralized information bank to access a multitude of criminal intelligence resources. (<http://www.ncirc.gov/>). The NCIRC portal is a secure system and once authenticated through the NCIRC portal, personnel are able to access ISE Shared Space data via federated queries and in this instance are able to access the MPD ISE Shared Space. The NCIRC instantiates some functionality of the ISE Core as documented in the *ISE-SAR EE Segment Architecture*.

server will leverage existing segment architectures (ex., *ISE-SAR EE Segment Architecture*) available from one of the ISE communities.

- NCIRC portal Interface: This interface, executes the SARSearchQuery, that supports the following operations:
 - **getMatchingSARSummaries**: Accepts a predefined set of queries that are derived from metadata standards accepted by the *ISE-SAR Functional Standard* and returns SAR summary, SAR ID (unique identifier), Activity Date and Time, Tip Class Code and Tip Type Code.
 - **getSARDetail**: Accepts a list of SAR IDs and returns the corresponding SAR records to the user.
 - **getMatchingSAR**: In addition, the interface also supports an unimplemented operation (to be built later) that accepts search parameters and returns complete SAR records. It is anticipated that authorized users would require such an operation.
- Management Interface: This interface, called the **SARAuditQuery**, supports the following operations:
 - **getQueryLog**: This operation accepts a time period and returns the transaction logs in the specified time period.
 - **getETLLog**: This operation accepts a time period and returns the logs pertaining to the ETL (data load) operations of the ISE Shared Space server.

5.4.5 Integration Configuration

This section describes the methods used to integrate the MPD ISE Shared Space server with the MPD database and the NCIRC portal.

The MPD ISE Shared Space server receives messages from the NCIRC portal. The actual connectivity between the User Interface (UI) (NCIRC portal) and the MPD ISE Shared Space server is established over a VPN through point-to-point tunnels. The VPN connectivity components are located behind firewalls and only the VPN traffic is being exchanged between the remote firewalls and the central VPN concentrator.

The VPN device at the MPD ISE Shared Space server communicates with the Web Server which in turn relays the database queries into the database. The database and the Web server IIS reside on the same server hardware. A similar connection is used from the current system to the MPD ISE Shared Space server, as shown in Figure 5-3.

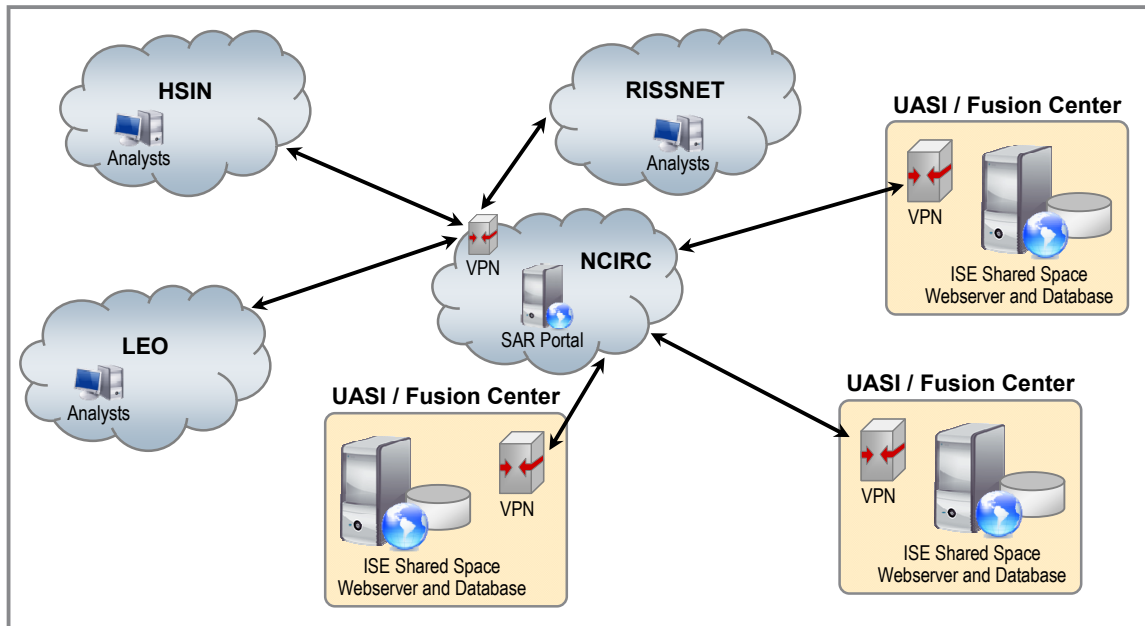


Figure 5-3. High Level Network Diagram

5.5 Project Results

The choice of an agile development methodology and implementation approach was one of the key success factors in the effort to develop and deploy ISE-SAR capture, management, and sharing within 90 days of project kickoff. This flexible, results-oriented approach allowed MPD to work through or around technical and procedural obstacles that could have derailed the effort at many points. The most important agile best practices used in this project were

- Collocating software engineers with fusion center analysts and end-users, enabling rapid and effective communication among the system's builders and customers.
- Developing through a series of short iterations (one week or less) of coding, testing, deployment, and review, creating a fast and virtuous feedback loop.
- Dividing the project into several small teams (1-3 engineers) with well-defined interfaces between each module, preventing schedule bottlenecks.

In concert with the agile development methodology, MPD took a practical approach to technical standards and policies. The team used published standards wherever possible. This approach proved invaluable because of the rapid evolution of ISE-SAR management procedures and agreements during the course of the effort. Leveraging experienced agile developers with extensive domain knowledge was also essential. This approach ensured that the hands-on implementers could build to an information sharing specifications or create new architectural elements when necessary.

MPD developed and delivered three separate levels of training: Front Line Officer, Analyst, and Executive. This training is important to the proper gathering, analysis and sharing of SAR information, including protections of privacy and civil liberties.

The technology used by the DC MPD Fusion Center to develop its ISE Shared Space complies with CTISS Technical Standards and the DC MPD SAR process is in alignment with the *ISE-SAR Functional Standard*. DC MPD's Privacy Policy guided the sharing of SAR information. This Privacy Policy, which meets the ISE Privacy Guidelines, provided guidance on what information could be shared.

Additionally, DC MPD used the *ISE-SAR Functional Standard* Information Exchange Package Documentation (IEPD) format to transfer (via SFTP) information to applicable law enforcement agencies. While some SAR processes were implemented manually, these manual processes successfully provided secure information sharing.

5.6 Future Considerations

The DC MPD project team developed and implemented the ISE Shared Space rapidly to accommodate the Presidential Inauguration on January 20, 2009. Because of the aggressive development cycle, DC MPD developed this system with an initial goal of providing ISE-SAR related information directly to applicable law enforcement agencies that supported the Inauguration. The MPD ISE Shared Space will continue to exist and will expand as required in the future.

The following future enhancements are being considered by DC MPD:

- Expanding the Web services capabilities within the MPD ISE Shared Space as well as work with the appropriate organizations to expand the capabilities of the ISE Core.
- Connectivity between the MPD ISE Shared Space to eGuardian data via the ISE Core once eGuardian has implemented an ISE Shared Space.
- Ensuring adherence to all privacy and personal information policies and procedures.
- Developing and instituting training for applicable personnel on ISE Shared Space operations.



**INFORMATION SHARING ENVIRONMENT
PROFILE AND ARCHITECTURE IMPLEMENTATION STRATEGY,
VERSION 2.0**

APPENDICES

This page intentionally blank.

Appendix A – Architecture and Infrastructure Committee Letter



April 4, 2008

Dear Ambassador McNamara,

On behalf of the Federal Chief Information Officers (CIO) Council's Architecture and Infrastructure Committee (AIC) Leadership, thank you for affording us the opportunity to review the Information Sharing Environment (ISE) Profile. The AIC Leadership fully supports the use of the Federal Enterprise Architecture (FEA) Reference Models in organizing the implementation of the ISE, as it is only through true business driven architecture that information sharing is effective. It is clear that the concepts and strategies included in this ISE document will help agencies involved with anti-terrorism activities and will support the President's Management Agenda. The AIC recognizes the benefits of this guide for a plethora of agencies and departments within the Federal government, as well as state and local governments.


After review, the AIC Leadership recommends that the Program Manager, Information Sharing Environment (PM-ISE) issue this document with the inclusion of a few modifications. The AIC Leadership reached the consensus that the document is better described as a Profile and Architecture Implementation Strategy for the ISE community. The ISE Profile includes reporting requirements specific to the ISC member organizations, and that aspect of its content goes beyond the scope of current FEA Profiles. In addition to the title change, the AIC Leadership recommends that the title reference to the FEA should be moved from the front cover to the inside cover to demonstrate approval of the Office of Management and Budget (OMB), but not indicate that this document is a direct OMB product. For example, the inside cover could read *"This document was reviewed and approved by the Federal Architecture and Infrastructure Committee and the Office of Management and Budget to be a valid Profile and Architectural Implementation Strategy for the Information Sharing Environment."*

We copied the CIOs of affected agencies and their contributing member on this memorandum to ensure all relevant parties received a direct copy of the document. Given the reporting requirements suggested within the document, this will ensure that affected parties, especially ISC members, are aware of the actions required by their agencies.

Again, we thank the PM-ISE for the opportunity to review this document and for providing the government with such a strong document that will help guide the implementation of information sharing requirements for the ISE community, as well as applicable state and local governments.

Sincerely,

Michael Carleton 
Architecture and Infrastructure Committee Co-Chair
Chief Information Officer, US Department of Health and Human Services

Molly O'Neill 
Architecture and Infrastructure Committee Co-Chair
Chief Information Officer and Assistant Administrator, US Environmental Protection Agency

This page intentionally blank.

Appendix B – Acronyms

AAA	Authentication, Authorization, and Accounting
AATT	Authorization and Attribute Tiger Team
ABAC	Attribute Based Access Control
AIC	Architecture and Infrastructure Committee
AMS	Alert Management System
API	Application Programming Interface
ASP	Active Server Page
ASP.NET	Active Server Page for .Net
AWN	Alerts, Warnings, and Notifications
BRM	Business Reference Model
C&A	Certification and Accreditation
CDR	Critical Design Review
CES	Core Enterprise Services
CGI	Common Gateway Interface
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
COI	Community of Interest
CONOPS	Concept of Operations
COOP	Continuity of Operations Planning
COTS	Commercial Off-the-Shelf
CPIC	Capital Planning and Investment Control
CT	Counterterrorism
CTISS	Common Terrorism Information Sharing Standards
CUI	Controlled Unclassified Information
DB	Database
DBMS	Database Management System
DHS	Department of Homeland Security
DME	Development, Modernization, and Enhancement
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice

DR	Design Review
EA	Enterprise Architecture
EAAL	E-Authentication Assurance Level
EAF	Enterprise Architecture Framework
EE	Evaluation Environment
EO	Executive Order
ERD	Entity Relationship Diagram
ETL	Extract, Translate, and Load
EU	European Union
FastCGI	Fast Common Gateway Interface
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FIPS	Federal Information Processing Standards
FSAM	Federal Segment Architecture Methodology
FTP	File Transfer Protocol
GJXDM	Global Justice XML Data Model
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network-Critical Sectors
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IA	Information Assurance
IC	Intelligence Community
ICD	Intelligence Community Directive
ICE	Immigration and Customs Enforcement
IdAM	Identity and Access Management
IDP	Identity Provider
IEPD	Information Exchange Package Document/Documentation
IIA	ISE Implementation Agent
IIS	Internet Information Service (Microsoft)
ILC	Implementation Life Cycle

INTERPOL	International Criminal Police Organization
IOS	Internetwork Operating System
IP	Implementation Plan
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4.0
IPv6	Internet Protocol Version 6.0
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA	Information Security and Assurance
ISAPI	Internet Server Application Programming Interface
ISC	Information Sharing Council
ISE	Information Sharing Environment
ISEA	Information Sharing Environment Architecture
ISEA ILC	Information Sharing Environment Architecture Implementation Life Cycle
ISE-AM	Information Sharing Environment Administrative Memorandum
ISE-G	Information Sharing Environment Guidance
ISE-SAR EE	Information Sharing Environment Suspicious Activity Reporting Evaluation Environment
ISO	International Organization for Standardization
ISSA	Information Sharing Segment Architecture
IT	Information Technology
JABS	Joint Automated Booking System
JSP	Java Server Page
JTTF	Joint Terrorism Task Force
LE	Law Enforcement
LEO	Law Enforcement Online
LOB	Line of Business
MAC	Media Access Control
MPD	Metropolitan Police Department
MS-SQL	Microsoft Structured Query Language
NCIRC	National Criminal Intelligence Resource Center
NCTC	National Counterterrorism Center
NIC	Network Interface Controller
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology

NSAPI	Netscape Server Application Programming Interface
NSI	Nationwide SAR Initiative
NSIS	National Strategy for Information Sharing
O&M	Operations and Maintenance
OMB	Office of Management and Budget
OS	Operating System
P2P	Point-to-Point
PAIS	Profile and Architecture Implementation Strategy
PGC	Privacy Guidelines Committee
PGFSOA	Practical Guide Framework Service Oriented Architecture
PHP	Hypertext Preprocessor
PKI	Public Key Infrastructure
PM	Program Manager
PM-ISE	Program Manager, Information Sharing Environment
POA&M	Plan of Action and Milestones
RAID	Redundant Arrays of Inexpensive Disks
R-DEX	Regional Data Exchange
RDMS	Relational Database Management System
RISSNET	Regional Information Sharing System Network
RMF	Risk Management Framework
RSS	Regional Sharing System
SAML	Security Assertion Markup Language
SAR	Suspicious Activity Reporting
SBU	Sensitive But Unclassified (Security Classification)
SCGI	Secure Common Gateway Interface
SCI	Sensitive Compartmented Information (Security Classification)
SDLC	Systems Development Life Cycle
SFTP	Secure File Transfer Protocol
SGML	Standard Generalized Markup Language
SLA	Service Level Agreement
SLT	State, Local, and Tribal
SME	Subject Matter Expert
SOA	Service-Oriented Architecture

SOC	Security Operations Center
SP	Special Publication
SPP	Security and Privacy Profile
SSH	Secure Socket Handler
SSI	Service Side Include
SSL	Secure Socket Layer
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SVP	Service Provider
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TS	Top Secret (Security Classification)
TWL	Terrorist Watchlist
UAAS	Unified Authorization and Attribute Service
UASI	Urban Area Security Initiative
UI	User Interface
UN	United Nations
US	United States
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WSDL	Web Services Definition Language
XML	Extensible Markup Language
XSD	XML Schema Definitions

This page intentionally blank.

Appendix C – Bibliography

1. Executive Office of the President, Office of Management and Budget, *Federal Transition Framework*. See <http://www.whitehouse.gov/omb/e-gov/fea/> for latest version.
2. *Federal Enterprise Architecture Consolidated Reference Model*, Version 2.0, June 2006.
http://www.whitehouse.gov/omb/assets/fea_docs/FEA_CRM_v23_Final_Oct_2007_Revised.pdf
3. *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law No. 108-458, 118 Stat. 3638 (17 December 2004).
http://www.nctc.gov/docs/pl108_458.pdf
4. *National Security Act of 1947*, as amended (50 U.S.C. 402 et seq.).
http://www.intelligence.gov/0-natsecact_1947.shtml
5. Executive Office of the President, Office of Management and Budget (OMB), *Preparation, Submission, and Execution of the Budget*, Circular No. A-11, June 2006. http://www.whitehouse.gov/omb/circulars/a11/current_year/a11_toc.html
6. Office of Management and Budget (OMB), *Memorandum for Heads of Executive Departments and Agencies, Subject: Management of Federal Information Resources*, Circular No. A-130, Revised, (Transmittal Memorandum No. 4).
<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf>
7. The President, *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information*, Executive Order 13292, 25 March 2003.
<http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>
8. Program Manager, Information Sharing Environment, *Information Sharing Environment Enterprise Architecture Framework*, Version 2.0, September 2008.
http://www.ise.gov/docs/eaf/ISE-EAF_v2.0_20081021.pdf
9. Program Manager, Information Sharing Environment, *Information Sharing Environment Implementation Plan*, November 2006.
<http://www.ise.gov/docs/reports/ise-impplan-200611.pdf>
10. Program Manager, Information Sharing Environment, *The Information Sharing Environment Interim Implementation Plan*, January 2006.
http://www.ise.gov/docs/reports/ise_interim_implementation_plan-20060109.pdf
11. Executive Office of the President, Office of Management and Budget, *Federal Enterprise Architecture Program EA Assessment Framework 2.2*, October 2007, available at <http://www.whitehouse.gov/omb/e-gov/fea/>

12. Program Manager, Information Sharing Environment, *Profile and Architecture Implementation Strategy*, Version 1.0, May 2008. <http://www.ise.gov/docs/eaf/ISE-PAIS.pdf>

Appendix D – Glossary

Access Control—Limiting access to information system resources only to authorized users, programs, processes, or other systems.

[http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

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. [Executive Order 13388 Section (6)(a) and 5 U.S.C. 105]

Alerts, Warnings, and Notifications—Supports the preparation of and ensures timely dissemination and handling of terrorism alerts and warnings among ISE participants at appropriate security levels.

Audit—Independent review and examination of records and activities to assess the adequacy of system controls to ensure compliance with established policies and operational procedures and to recommend necessary changes in controls, policies, or procedures.

Authentication—Security measure designed to establish the validity of a transmission, message, or originator or a means of verifying an individual’s authorization to receive specific categories of information. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Authorization—Access privileges granted to a user, program, or process.

[http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Availability—Timely, reliable access to data and information services for authorized users. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Business Reference Model—A framework facilitating a functional (not organizational) “view of the Federal government’s lines of business (LoBs), including its internal operations and its services for citizens, independent of the agencies, bureaus, and offices that perform them.”

[http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v23_Final_Oct_2007.pdf]

Confidentiality—Assurance that information is not disclosed to unauthorized individuals, processes, or devices. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Continuity of Operations Planning (COOP)—Plans for continuing an organization’s (usually a headquarters element) essential functions at an alternate site and performing those functions for the duration of an event with little or no loss of continuity before returning to normal operations. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Controlled Unclassified Information (CUI)—Categories of unclassified information requiring controls that protect the information 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.

Core Enterprise Services (CES)—Services that enable both service and data providers on the “net,” by providing and managing the underlying capabilities to deliver content and value to end-users.

Data Accessibility—Those functional capabilities of the ISE that allow a user of the ISE to obtain data when needed. In particular, data accessibility depends on the principles that all data shall be posted to ISE Shared Spaces to enable access to all users except when limited by security, policy, or regulations.

Domain—A virtual environment governed by a single set of consistent policies. These policies include, but need not be limited to, security policies that govern authentication, authorization, availability, confidentiality, and integrity. Typically a domain is managed by a single organizational entity, such as a single agency, that enforces the applicable policies, e.g., the CIA domain. A group of agencies may also establish a new domain for sharing information by agreeing on a consistent set of policies for the data stored in that domain and designating a proxy to manage that domain, e.g., the Intelligence Domain.

Encryption—The process of obscuring information to make it unreadable without special knowledge.

Extensible Markup Language (XML)—XML is a simple, flexible text format derived from Standard Generalized Markup Language (SGML). Originally designed to meet the challenges of large-scale electronic publishing, XML also plays an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere. [<http://www.w3.org/XML/>]

Federal Enterprise Architecture—A business-driven framework that defines and aligns Federal business functions and supporting technology and includes a set of five common models (performance, business, service component, data, and technical).

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. 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 major urban area governments designed to coordinate the gathering, analysis, and dissemination of terrorist-related, law enforcement, and public-safety information.

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) improves the identification or investigation of a suspected terrorist or terrorist organization; or (d) improves the response to a terrorist act. [Section 892(f)(1) of the Homeland Security Act (6 U.S.C. 482(f)(1))]

Identity and Access Management— An overarching term often used to refer to the processes of authentication, authorization, assignment of attributes and privileges, access management, credential issuance, and the identification of a digital identity and the binding of that digital identity to an individual.

Identity Provider (IDP) — A technically implemented, *identity* related service that leverages technologies such as SAML 2.0 functionality, PKI credential services, and/or brokered trust between user systems.

Identity Provider Organization (IPO)— An ISE Implementation Agent (organization) that provides identity management services to ISE participants, such as identity proofing/vetting, credentialing, attribute provisioning, and/or local authentications services.

Information Assurance—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Information Sharing Council (ISC)—The Information Sharing Council was 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)] EO 13388, which superseded EO 13356, established the Information Sharing Council.

Information Sharing Environment (ISE)—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)]

ISE Suspicious Activity Report (ISE-SAR)—An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

Integrity—Quality of an information system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

[\[http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf\]](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf)

Interoperability—The capability of different programs to exchange data via a common set of business procedures and to read and write the same file formats and use the same protocols.

Intrusion Detection—The act of detecting actions that attempt to compromise the confidentiality, integrity, or availability of a resource. It does not necessarily prevent intrusion from occurring.

ISE Core—Basic infrastructure in the ISE that will facilitate and/or support the ISE environment at large; contains the core transport components and other services that will be used to interconnect the ISE Shared Spaces of each ISE participant and allow exchange of information.

ISE Enterprise Architecture Framework (EAF)—Presents a logical structure of ISE business processes, information flows, and relationships, services, and high-level data packet descriptions and exchange relationships.

ISE Implementation Agent—Refers to an organization responsible for providing infrastructure and services in the ISE Core Segment.

ISE participant—Any Federal, State, local, or tribal government organization, private sector entity, or foreign government organization (to include employees) that participates in the ISE.

ISE Shared Space— networked data and information repositories used to make standardized terrorism-related information (as defined through the Common Terrorism Information Sharing Standards [CTISS]), applications, and services accessible to all ISE participants (across the law enforcement, intelligence, homeland security, foreign affairs, and defense communities).

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.

Private Sector Partners—Includes vendors, owners, and operators of products and infrastructures participating in the ISE.

Program Manager—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)]

Quality of Service—The probability of the telecommunication network meeting a given traffic contract, or in many cases a term used informally to refer to the probability of a packet succeeding in passing between two points in the network within its desired latency period.

Security Domain—The term “Security Domain” refers to three security levels—Top Secret/Sensitive Compartmented Information (TS/SCI), Secret, and Sensitive but Unclassified (SBU).

Segment—Segments are individual elements of the enterprise describing core mission areas and common or shared business services and enterprise services. Segments are defined by the enterprise architecture.

Service—A contractually defined behavior that can be provided by a component, for use by any component, solely based on the interface contract.
[\[http://www.nces.dod.mil/aboutNCES/glossary_content.aspx\]](http://www.nces.dod.mil/aboutNCES/glossary_content.aspx)

Service-Based Architecture—A business-driven approach to software architecture that supports integrating the business as a set of linked, repeatable business tasks, or “services.” Services are self-contained, reusable software modules with well-defined interfaces and are independent of applications and the computing platforms on which they run. Service-based architecture helps users build composite applications, which are applications that draw upon functionality from multiple sources within and beyond the enterprise to support horizontal business processes.

Service Level Agreement (SLA)—SLA defines mutual understandings and expectations between a service consumer and a service provider. The service-level objectives that both the service consumer and the service provider agree upon usually include a set of indicators such as availability and average response time.
[\[http://www.disa.mil/nces/about_nces/glossary.html\]](http://www.disa.mil/nces/about_nces/glossary.html)

Service Provider Organization (SPO)— An ISE Implementation Agent (organization) that provides services to ISE participants, such as ISE Core Services, Identity and Access Management Services, and Electronic Directory Services. Services may leverage other services implemented by separate organizations to provide capabilities. As attribute-based-access control matures in the ISE, this access will migrate from local access control by the Service Provider to attribute-based access control.

Service Provider (SVP)— A technically implemented *access/authorization* related service that leverages technologies such as SAML 2.0 functionality, PKI credential services, and/or brokered trust between user systems.

Service-Oriented Architecture (SOA)—A business-driven approach to software architecture that supports integrating the business as a set of linked, repeatable business tasks, or “services.” Services are self-contained, reusable, software modules with well-defined interfaces and are independent of applications and the computing platforms on which they run. SOA helps users build composite applications, which are applications that draw upon functionality from multiple sources within and beyond the enterprise to support horizontal business processes.

State—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]

Suspicious Activity—Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

Suspicious Activities Report (SAR)—Official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

Terrorism Information—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, 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)(5)]

Terrorist Watchlist—The key source for all known and appropriately suspected terrorists and used by many U.S. Federal departments and agencies; State, local, and tribal (SLT) entities; and foreign and private sector partners in support of their operational mission.

Virtual Private Network (VPN)—A private communications network usually used within a company, or by several different companies or organizations, to communicate from remote locations over an insecure public network.

Web Service—Web services provide a standard means of interoperating between different software applications, running on a variety of platforms and/or frameworks. Web services are characterized by their great interoperability and extensibility, as well as their machine-processable descriptions using XML. They can be combined in a loosely coupled way in order to achieve complex operations. Programs providing simple services can interact with each other in order to deliver sophisticated added-value services. [<http://www.w3.org/2002/ws/Activity>]

Web Service Definition Language (WSDL)—WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate. [<http://www.w3.org/TR/wsdl>]

XML Schemas/XML Schema Definitions (XSD)—Express shared vocabularies and allow machines to carry out rules made by people. They provide a means for defining the structure, content, and semantics of XML documents. [<http://www.w3.org/XML/Schema>]

This page intentionally blank.

Appendix E – ISE Business Processes

Mission Business Processes	
Information Requirements and Roles	Supports handling of terrorism information requirements from ISE participants and prioritization of needs and allocation of resources. Provides status of actions against requirements. Feeds program and budget-planning processes for long term investments.
Alerts and Notifications	Supports the preparation of and ensures timely dissemination and handling of terrorism alerts and warnings among ISE participants, at appropriate security levels.
Suspicious Activity Reporting	Official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.
Identification and Screening	Supports the counterterrorism (CT) community efforts to identify and screen personnel and material. This support includes updates of terrorist watch-lists and making them available to ISE participants when needed. Ensures watch-list entries are consistent and current. It also encompasses efforts to identify and screen shipments for entry control into the U.S. or U.S. controlled areas for verifying eligibility to selected public and private sector services, and for law enforcement actions.
Analysis	Provides support as needed to analytic processes employed by ISE participants.
Operations	Provides ISE support to a variety of ISE operational activities, including collection, investigations, and inspections.
Policy and Decision Making	Supports policy maker information needs and other counterterrorism decision processes. Contributes fusion of disparate data into a strategic picture that allows decision makers to collaborate on possible courses of action and to preempt or to respond to events as necessary.
Response	Supports the counterterrorism community effort to respond (act) on a terrorism-related threat.
Protection	Supports the counterterrorism community effort to protect the territory, people, and interests of the United States.
Service Business Processes	
Access	A process used to grant an individual access to information and associated resources of ISE member communities based on verification of the individual's identity and associated attributes (Identity Management). The Access Process must ensure security and currency of credentialing and mission role information. It also protects personal identity information where applicable.
Discovery and Search	Allow ISE participants to conduct queries of disparate terrorism-related information; support ISE participants' ability to discover data from sources a participant may otherwise not know exists.

Service Business Processes (Continued)	
Dissemination	The process supports timely promulgation of terrorism information at the appropriate level of classification to ISE participants. The process supports data push, data pull, and Web-type posting of terrorism information. The Dissemination Process supports many ISE missions. In particular, it supports the Alerts and Notifications Process by delivering information to various communication outlets – both governmental and public/private sector.
Collaboration	The business processes and supporting applications that enable people to interactively work together analyzing and acting upon terrorism-related information.
Manipulation and Storage	Provide tools and techniques to organize or catalog information in a structured format that is searchable by other ISE participants. Satisfy mission needs for user response times with some combination of fast (on-line) and archival-type storage. Accommodate differences in agency taxonomies with some combination of standards, limited common shareable data, and/or mediation services to translate data between supplier and requestor ontologies. Establish applicability of links between searchable data structure and actual data repositories.
Electronic Directory Services	A product that assists in locating people and organizations related to or supporting the counterterrorism mission.
Information Protection/Assurance	Ensures that the sharing environment has at least the same level of system protection to terrorism-related information as is provided today to protect privacy and civil liberties.
Enabling Business Processes	
Issuances	Identify need for issuance, develop drafts, review and resolve, issue publication, monitor compliance.
Information Sharing Agreements	Provide common approaches for managing information sharing agreements between ISE participants.
Business Process and Performance Management	Identify problems in existing processes or need, assess impact, analyze and develop options for action, implement selected course of action, and monitor performance. Develop ISE-wide performance measures, monitor progress, ensure that department and agency goals and measures support ISE goals, prepare and publish annual ISE performance report.
Training/Cultural Change	Develops and executes ISE-wide training; provides guidance on, develops, implements, and monitors information sharing incentives.
Security Framework	Develops and implements a framework to ensure that terrorism information is handled securely and efficiently. (Specifically includes appropriate mechanisms to handle CUI/SBU and classified terrorism information.) Removes impediments to ISE clearances and visit handling, leverages certification and accreditation improvement, adopts and implements cross-domain solutions.
Standards and Architecture	Develop and maintain the ISE Enterprise Architecture Framework, the ISE Profile and Architecture Implementation Strategy (PAIS), and common standards.

Enabling Business Processes (Continued)	
Privacy and Civil Liberties Protection	Provides procedures and capabilities to ensure that privacy and civil liberties requirements are addressed in the ISE.
ISE Governance and Management	Ensure that the ISE governance process functions effectively and efficiently. This category includes processes that support ISE budgeting, auditing, and quality assurance.

This page intentionally blank.

Appendix F – ISE Shared Spaces

1 Overview

The ISE Shared Spaces concept is a key implementation approach for developing trust and community-wide information sharing across the entire ISE. ISE Shared Spaces are networked data and information repositories used to make standardized terrorism-related information, applications, and services accessible to all ISE participants (across the law enforcement, intelligence, homeland security, foreign affairs, and defense communities).

2 Definitions

2.1 General

ISE Shared Space: An ISE Shared Space standardizes terrorism information, as defined through the Common Terrorism Information Sharing Standards (CTISS) and is made available by one ISE participant to others, as appropriate. Additionally, ISE participants may create or use an ISE Shared Space to make their services and data accessible, as appropriate, to other ISE participants.

ISE Core: The ISE Core provides infrastructure and services necessary for the interconnection and use of information available through various ISE Shared Spaces.

2.2 Technical

ISE Shared Space: An ISE Shared Space consists of hardware, software, and/or services that serve as the ISE participant's infrastructure for ISE activity, as defined through the Common Terrorism Information Sharing Standards (CTISS). There may be multiple ISE Shared Spaces, each under the management, control, and resourcing responsibility of the ISE participant. This responsibility includes ensuring information security, data integrity, use, retention, and meeting other data stewardship requirements.

ISE Core: The ISE Core in the ISE has three major components: core services, portal services, and core transport. ISE Core Services provide ISE-level services used in operating the ISE (e.g., Discovery, Mediation, Storage, Collaboration, and Security). ISE Portal Services provide the infrastructure for those services used in interfacing the ISE Portal to the Core (including Network Management). ISE Core Transport entails the underlying telecommunications infrastructure (e.g., cables, routers, switches), which moves ISE data and information from one ISE Shared Space to another. The ISE Core segment functionality is demonstrated in the ISE-SAR Evaluation Environment.

3 Models

3.1 ISE Shared Spaces

In describing ISE Shared Spaces for identifying existing infrastructure to implement an ISE Shared Space or in planning for and establishing an ISE Shared Space, three models are considered:

- An information flow-driven model for an ISE Shared Space;
- A logical view model (or system-independent operational descriptions);
- A hosting and implementation model.

These models support ISE participants in their development of solution architectures that clearly identify the structure and attributes of the organization's ISE Shared Spaces in sufficient detail.

3.1.1 Information Flow Model

The information flow model for implementing an ISE Shared Space considers the mission or business drivers for organizations to follow in interfacing with the ISE Core. This model takes into account not only the requirements of ISE participants that produce ISE information but also the information needs of other ISE participants consuming another participant's information. These essentials are easily identified from the defined information flows from mission business processes that delineate the ISE. These drivers include

- *Specific Mission*: These information flows would be based upon defined ISE mission business processes presenting relationships, exchanges, and products for terrorism information sharing.
- *Community*: These information flows would be based upon mission business processes of participating organizations that make up a community of interest (COI). They may be associated with defense, homeland security, intelligence, foreign affairs, or law enforcement representative organizations with business processes that are part of that select community. Outputs of these COI processes may be data and information structured under CTISS for storage in an ISE Shared Space.
- *Entity*: These information flows would be based upon mission business processes of an individual organization (e.g., "entity").

3.1.2 Logical View Model

The logical model identifies three general implementation schemes:

- *Replication:* Storage of terrorism information from internal resources into an ISE Shared Space and making it accessible to other ISE participants using common services, such as discovery, storage, and collaboration for access and use. A familiar example of this scheme would be libraries that provide the general public on-line card catalog services for locating books yet also maintain their book records on their own internal systems for inventory and management purposes.
- *Web-Service:* Exposing terrorism information, services, and applications via Web services that interface with other ISE participant Web portals as appropriate. A familiar example of this is the approach used by on-line shopping vendors to make multiple brand product information and sales services accessible to the general public via the Internet. The Homeland Security Information Network - Critical Sectors (HSIN-CS) represents a workable model for secure, encrypted communications between the U.S. Department of Homeland Security (DHS) and vetted members of the Critical Infrastructure and Key Resources (CIKR) sectors as well as within and across the sectors.
- *Hybrid:* Allowing direct access, with appropriate access management safeguards, to selected applications and information within an ISE participant's infrastructure. An example is the collaborative use of a Case Management application used by two or more agencies cooperating in a joint CT investigation. Access would be granted after validating and ensuring appropriate authenticating credentials have been verified. An example of this scheme is police departments' accessing the Department of Justice's (DOJ) Joint Automated Booking System (JABS).

3.1.3 Hosting and Implementation Model

Given the logical information flow and models, various hosting and implementation options are available to establish a participant's ISE Shared Space. These hosting options include

- *Department Level:* A department, agency, or other ISE participating organization would establish an ISE Shared Space or multiple ISE Shared Spaces to facilitate terrorism information sharing for the entire organization, to include assigned bureaus and subordinate offices.

The ISE Shared Space(s) would be interconnected with other ISE participants to provide access to standard information. An example of such a department-wide application for providing a comprehensive repository of information is the FBI's Regional Data Exchange (R-DEx) or One-DOJ system. One-DOJ is designed to provide the capability to share full text law enforcement investigative information from Federal, State, and local investigative agencies working in association with the FBI. From an overarching programmatic perspective, in this option an ISE participant would continue to be responsible for the overall budgeting, resourcing, and installation of the ISE Shared Space on behalf of the entire organization and its affiliated offices.

- **Component/Other Level:** An organizational element or subcomponent of the larger department, agency, or ISE participant would be responsible for establishing an ISE Shared Space supporting that component's responsibilities for interfacing with the ISE. An ISE Shared Space, established by this component, would be a portion of the network infrastructure operated and maintained by this component and would provide an ISE interface on behalf of the entire organization. An example of such an implementation scheme is DHS's Regional Sharing System (RSS) that is under the responsibility of the Immigration and Customs Enforcement (ICE) agency providing bi-directional information sharing capabilities between the Federal government and State and local partners.
- **Third Party Level:** ISE participants may leverage the services and infrastructure of another third party service provider, who is a member of the ISE community, for "virtually" establishing their ISE Shared Space. Such an implementation option should be consistent with overall concepts for an ISE Shared Space as outlined in the *ISE EAF*. ISE participants, leveraging a third party service provider to host their ISE Shared Space, should have well-defined service level agreements (SLAs) to address the issues of resourcing, management, continuity of operations, data stewardship, and ownership. If an ISE participant expects/intends to leverage a third party service provider, any and all implications for operations would not be the sole responsibility of the ISE third party service provider. For example, if Department X decides to permit another department or agency to host its data for sharing in the other department or agency's ISE Shared Space, Department X remains ultimately responsible for the data stored and consumed within the third party resources servicing Department X's "virtual" ISE Shared Space.

3.2 ISE Core

Elements of the ISE Core are resourced, planned, installed, and operated by designated ISE Implementation Agents supporting the ISE. The ISE Implementation Agent's proposed enterprise, segment, and solutions architectures will clearly identify the structure and attributes that implement the ISE Core segment in sufficient detail to support the investment and allow other ISE participants to plan their ISE Shared Spaces appropriately.

A number of key assumptions are made with regard to ISE Implementation Agents:

- Configuration management and systems integration are best accommodated with a single, designated ISE Implementation Agent (also called Service Provider) within each information security domain (i.e., TS/SCI, Secret/Collateral, and CUI/SBU). Robust configuration management processes must be in place in the event of multiple ISE Implementation Agents.

- Security policies and practices, whether originating in one community or not, must be ubiquitous within each security domain of the ISE Core and between ISE Implementation Agents.
- Service Level Agreements (SLAs) will provide the necessary Quality of Service requirements and parameters for servicing the ISE Core.

3.2.1 Hosting and Implementation Model

Various hosting and implementation options are available to establish the ISE Core. These options include

- *ISE Implementation Agent:* A designated primary ISE Implementation Agent is responsible for resourcing and providing all or a portion of the ISE Core to ISE participants represented in the defense, homeland security, law enforcement, intelligence, and foreign affairs communities. Outsourcing of some services is an acceptable option, albeit SLAs should exist for all services, regardless of secondary outsourcing agents, to ensure Quality of Service is maintained across the ISE. Program management and operations oversight are the responsibility of the primary ISE Implementation Agent.
- *Single Community Implementation Agent:* A designated primary ISE Implementation Agent responsible for resourcing and providing all or a portion of the ISE Core to ISE participants in a particular community (e.g., defense, homeland security, law enforcement, intelligence, foreign affairs). Outsourcing of some services is an acceptable option; albeit SLAs should exist for all services, regardless of secondary outsourcing agents, to ensure Quality of Service is maintained across the ISE. A joint SLA should also exist between the other communities and each single community ISE Implementation Agent. Program management and operations oversight over all ISE Implementation Agents is conducted through a designated department, agency, or other governmental organization.
- *Community Partnering Implementation Agent:* Two or more communities of ISE participants join together to identify and resource a designated primary service provider for their respective communities or share service provider responsibilities redundantly for enhanced performance (e.g., using RAIDs). Outsourcing of some ISE Core services is an option; albeit SLAs should exist exclusively between this designated ISE Implementation Agent and other community ISE participants. A joint SLA should be established between ISE Implementation Agents with program management and operations.

This page intentionally blank.

Appendix G – ISE Shared Space Information Security and Assurance (ISA) Considerations

1.1 Introduction

This section outlines the ISE Shared Space Information Security and Assurance (ISA) implementation details in the following sections: ISE Core ISA, ISA Guidance Sources, ISE Shared Space ISA, ISE Shared Space Inner Security Boundary, ISE Shared Space Outer Security Boundary.

The ISE Shared Space Information Security and Assurance Is Designed to Protect:

- i. Back-end internal systems from potential threats posed by ISE Shared Spaces
- ii. The ISE Shared Space from potential threats posed by the back-end internal system
- iii. The ISE Shared Space from potential threats posed by the ISE Core
- iv. The ISE Shared Space from potential threats posed by ISE participants accessing an ISE Shared Space

1.2 ISE Core Information Security and Assurance

Each ISE participant community should identify if a Security Operations Center (SOC) exists and which SOC and/or SOCs could perform the Security Monitoring for the ISE Shared Spaces. All security appliances used throughout the ISE should provide data feeds to each of the participating SOCs through an encrypted out-of-band management connection. Connection requirements should be provided by each participating SOC.

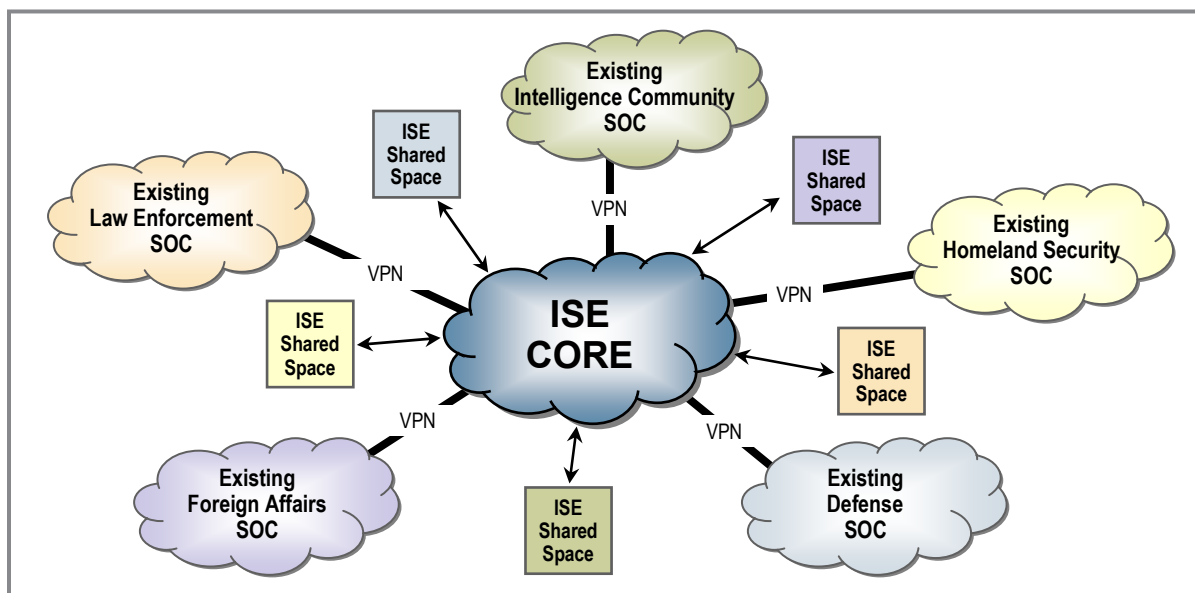


Figure G-1. ISE Core Security Operations Center Monitoring

1.3 Information Security and Assurance Guidance Sources

This section provides information on guidance documents available to support the development of secure ISE Shared Spaces. Following these guidelines provides common, implementable, and reusable security engineering best practices for protecting ISE Shared Spaces and the terrorism and/or homeland security-related information they share. These documents consist of two types of guidance: Security Technical Implementation Guides (STIGs) and Security Checklists.

NIST developed the STIGS and Security Checklists as directed by the Cyber Security Research and Development Act. They represent checklists of settings and options that minimize the security risks associated with each ISE Shared Space component that may be used. These guides and checklists are available from the NIST National Checklist Program.⁴⁷

Security Technical Implementation Guides (STIGs) are used for development and configuration of ISE Shared Spaces. The Security Technical Implementation Guides are the configuration standards used for applying standard information security and assurance configurations to information processing devices/systems. STIGs are used as development guidance for ISE Shared Spaces implementation. The specific set of STIGs applied will vary based on the products used in the implementation and the most current version listed on the NIST checklist web site.

Security Checklists are used for verifying information security and assurance of a deployed ISE Shared Space configuration. The Security Checklists (sometimes referred to as lockdown guides, hardening guides, or benchmark configurations) are essentially documents that contain instructions or procedures to verify the compliance to a baseline level of security. The specific set of checklists applied will vary based on the products used in the implementation and the most current version listed on the NIST checklist website.

1.4 ISE Shared Space Information Security and Assurance

The ISE Shared Space Logical Diagram depicted in Figure G-2 shows required components of an ISE Shared Space.

⁴⁷ The NIST Security Configuration Checklists can be found at: <http://csrc.nist.gov/checklists/index.html>.

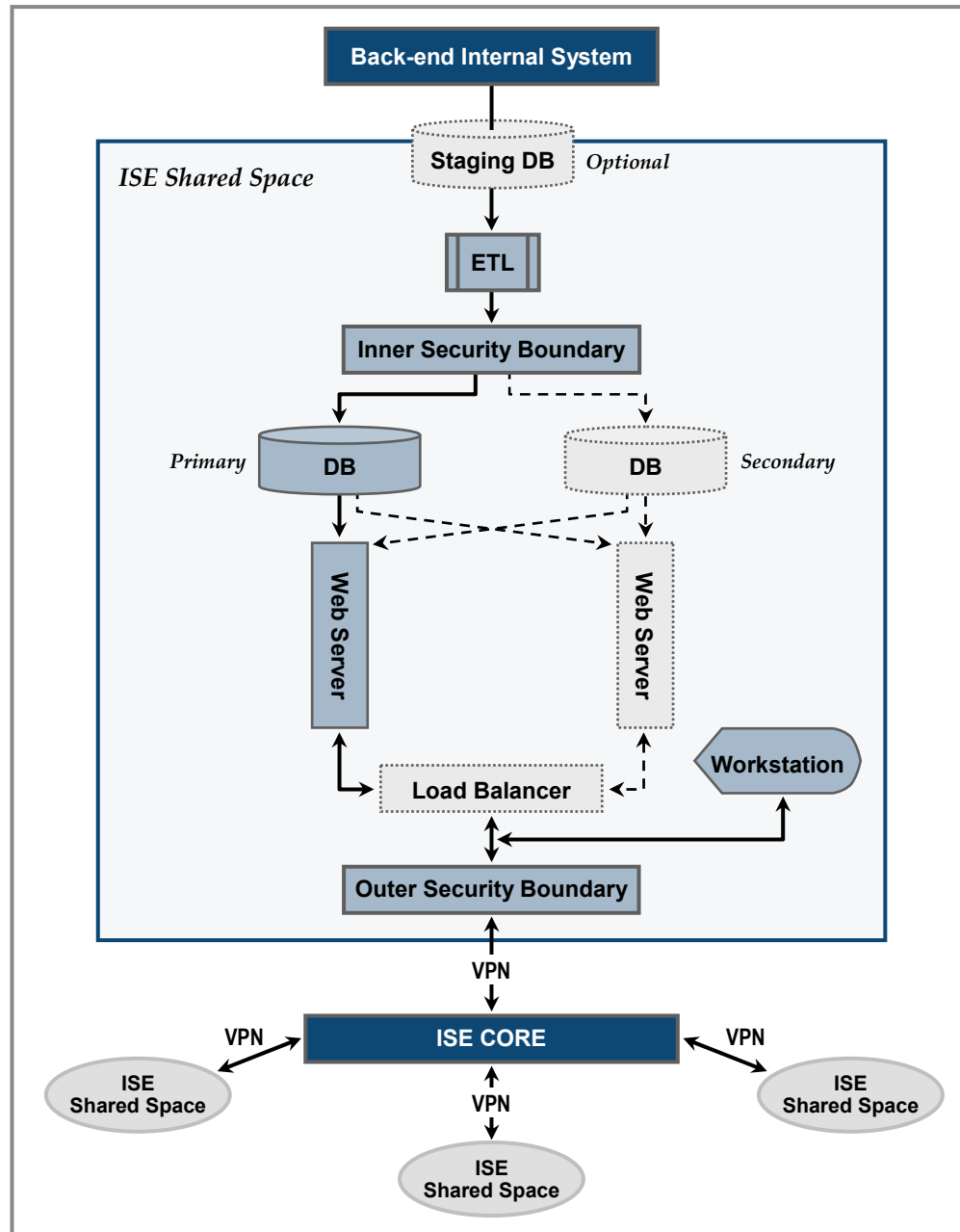


Figure G-2. ISE Shared Space Logical Diagram

The Security Configuration information listed in the sections below includes only the security behavioral requirements for the portions of the system that are above and beyond the types of configuration settings in the STIGS and Security Checklists described in section 1.3. These security behavioral requirements are based on an overall operational assumption that an ISE participant will access ISE Shared Spaces through existing ISE Core interfaces via the ISE Shared Space Outer Security Boundary, and not through the ISE Shared Space Inner Security Boundary. This

separation of duties/roles/business processes implements the security principal of “separation of duties.”

1.5 System Considerations

ISE Shared Spaces are implemented, certified, and accredited following the guidance in chapters 2 and 4 of this document and in accordance with the ISE participant requirements and authority responsible in the organization for System Security Authorization. The ISE Shared Space must meet or exceed the same security requirements of the ISE participant system(s) to which it connects and will be certified and accredited by the same organization responsible for C&A of the ISE participant. The implementation of ISE Shared Spaces will follow the ISE Privacy and Civil Liberties Implementation Guide where required.

1.6 Staging Database (optional)

The Staging Database is a temporary repository for information that the back-end internal system is placing in its ISE Shared Space. This staging area provides a secure method for ISE participants to place data in their respective ISE Shared Space without allowing other systems to access the ISE Core through the ISE Shared Space or the ISE Shared Space having direct communications with the originating ISE participants’ back-end systems. The following is the set of recommended security behavioral requirements for the Staging Database:

Staging Database: Recommended Security Requirements

- i. The Staging Database should be configured to only accept input pushed from the local ISE participant
- ii. The Staging Database should be configured to not allow data transfer back to the ISE participant
- iii. The Staging Database should be configured to push data to the ETL

1.7 Extract Translate Load (ETL)

The ETL provides the translation of data received from the Staging Database into a normalized format that has been agreed to by the ISE. The following is the set of recommended security requirements for the ETL:

ETL: Recommended Security Requirements

- i. The ETL should be configured to receive data only from the Staging Database
- ii. The ETL should terminate the processing of any data record that contains errors
- iii. The ETL should terminate the processing of any data record that does not meet the filter parameters set by the ISE Shared Space security administrator
- iv. The ETL should terminate the processing of any data record where normalization of a data field cannot be performed
- v. The ETL should record in the security audit logs any terminations of data record processing
- vi. The ETL should be configured to deliver only normalized records to the ISE database through the Inner Security Boundary

1.8 ISE Shared Space Inner Security Boundary

The Inner Security Boundary provides a controlled communications path between the ETL and the ISE database.

1.9 Database

The Database is composed of a single or a two-node system with fail-over capability. This database will store the records released by the local ISE participant for query by other ISE participants. The data will be accessed through the Web interface provided by the ISE Shared Space Front-End Web Server(s). The following is the set of recommended security behavioral requirements for the database:

Database: Recommended Security Requirements

- i. The database should validate any records received from the ETL prior to placing them in the database
- ii. After receiving a record from the ETL, the database should terminate ingest of a record when it does not validate properly
- iii. The database should record in the security audit logs when a record received from the ETL does not validate properly
- iv. The database should record in the security audit logs when a request to ingest records is received from any source other than the ETL
- v. The database should be configured to respond only to queries from the Front-End Web Server
- vi. The database should validate queries from the Front-End Web Server to ensure that only authorized queries are processed
- vii. The database should record in the security audit logs any attempts to query the database by sources other than the Front-End Web Server
- viii. The database should record in the security audit logs any failed queries
- ix. The database should record in the security audit logs any transition of operations from one database server to the other (note: only for implementations that contain a secondary database)

1.10 ISE Shared Space Front-End Web Server

The ISE Shared Space Front-End Web Server is composed of a single or a two-node system with fail-over capability. The Front-End Web Server provides the interface through which external ISE participants can query the database. The following is the set of recommended security requirements for the Front-End Web Server:

ISE Shared Space Front-End Web Server: Recommended Security Requirements

- i. The Front-End Web Server should validate the identity of external ISE participants requesting access to the local ISE Shared Space database
- ii. The Front-End Web Server should record in the security audit logs when the identity validation of a requestor fails
- iii. The Front-End Web Server should validate requestor responses to prevent a *Structured Query Language* injection attack through the Web interface
- iv. The Front-End Web Server should validate requestor responses to prevent modification of HTTP/HTTPS responses by the remote user
- v. The Front-End Web Server should record in the security audit logs a failure to validate a requestor response
- vi. The Front-End Web Server should accept communications only through the Outer Security Boundary
- vii. The Front-End Web Server should record in the security audit logs any transition of operations from one Front-End Web Server to the other (note: only for implementations that contain a secondary Front-End Web Server in fail-over configuration)
- viii. The Front-End Web Server should record in the security audit logs any termination of operations by a Front-End Web Server (note: only for implementations that contain an active secondary Front-End Web Server in a simultaneous operation configuration)

1.11 Load Balancer

The Load Balancer will be present only if the implementation contains a pair of Front-End Web Servers. The optional Load Balancer will support one of two configurations: (1) fail-over configuration between Front-End Web Servers, or (2) simultaneous operation configuration of both Front-End Web Servers. The following is the set of recommended security behavioral requirements for the Load Balancer:

Load Balancer: Recommended Security Requirements**In fail-over configuration:**

- i. The Load Balancer should transition all traffic to the secondary Front-End Web Server upon detection of a failure in the primary Front-End Web Server
- ii. The Load Balancer should record in the security audit logs any transition of network traffic from the primary to the secondary Front-End Web Server

In simultaneous operation configuration:

- i. The Load Balancer should transition all traffic to the remaining Front-End Web Server upon detection of a failure in one of the Front-End Web Servers
- ii. The Load Balancer should record in the security audit logs any transition of all network traffic to the remaining Front-End Web Server upon failure of the other Front-End Web Server

1.12 ISE Shared Space Outer Security Boundary

The Outer Security Boundary provides a controlled communications path between external ISE participants and the Front-End Web Server.

1.13 ISE Shared Space Inner Security Boundary

The ISE Shared Space Inner Security Boundary Logical Diagram depicted in Figure G-3 shows the required components of the Inner Security boundary that control communications between the ETL and the database. The Inner Security Boundary is composed of an Inner Boundary back-end internal system Facing Router, Inner Boundary Firewall, and Inner Boundary ISE Shared Space router.

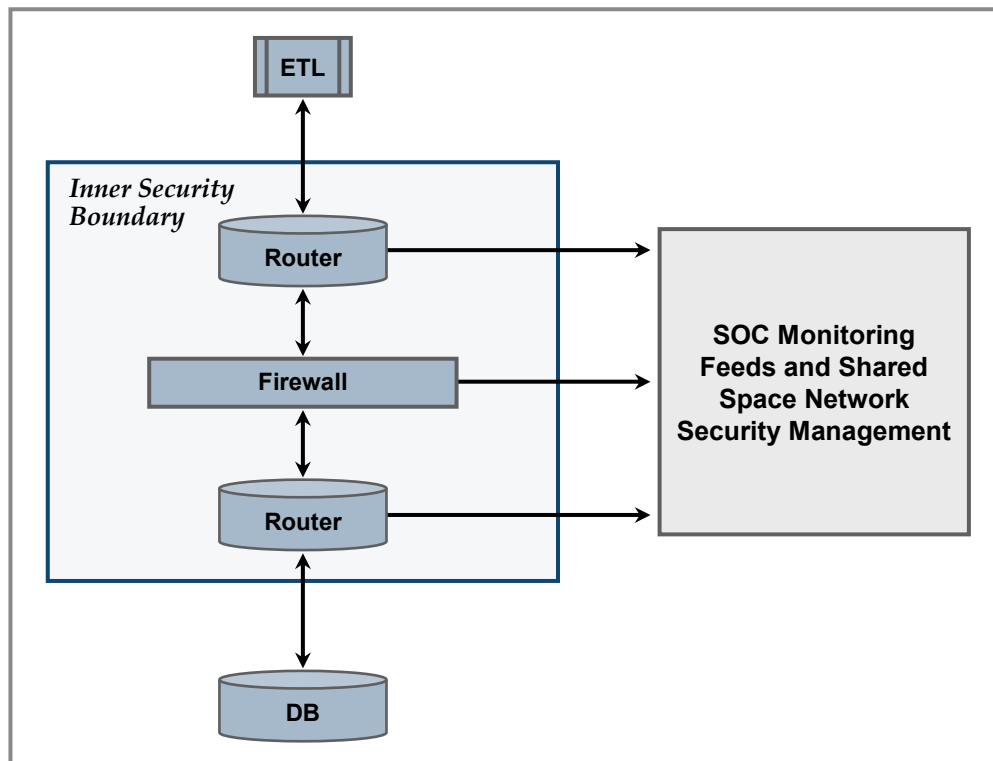


Figure G-3. ISE Shared Space Inner Security Boundary Logical Diagram

1.13.1 Inner Boundary Back-End Internal System Facing Router

The following is the set of recommended security requirements for the Inner Boundary back-end Internal System Facing Router:

Inner Boundary Back-End Internal System Facing Router: Recommended Security Requirements

- i. The Inner Boundary back-end internal system Facing Router should route traffic only from the ETL IP address to the Inner Boundary Firewall
- ii. The Inner Boundary back-end internal Facing Router should route traffic only from the ETL Media Access Control (MAC) address to the Inner Boundary Firewall
- iii. The Inner Boundary back-end internal system Facing Router should route only the approved ISE information transfer protocols⁴⁸ between the Inner Boundary Firewall and the ETL
- iv. Management of the Inner Boundary back-end internal system Facing Router should be performed through an out-of-band management port
- v. The Inner Boundary back-end internal system Facing Router should be designed to not allow routing between the network ports and the out-of-band management port

⁴⁸ Approved ISE information transfer protocols can be found in the ISE Guidance for Core Transport and Information Assurance at <http://www.ise.gov/pages/ctiss.html>.

1.13.2 Inner Boundary Firewall

The following is the set of recommended security requirements for the Inner Boundary Firewall:

Inner Boundary Firewall: Security Behavioral Requirements

- i. The Inner Boundary Firewall should allow only the ISE information transfer protocol to pass through the interface
- ii. The Inner Boundary Firewall should allow only the ISE information transfer protocol session to be initiated by the ETL side of the interface
- iii. Management of the Inner Boundary Firewall should be performed through an out-of-band management port
- iv. The Inner Boundary Firewall should be designed to not allow routing between the network ports and the out-of-band management port

1.13.3 Inner Boundary ISE Shared Space Router

The following is the set of recommended security requirements for the Inner Boundary ISE Shared Space router:

Inner Boundary ISE Shared Space Router: Recommended Security Requirements

- i. The Inner Boundary ISE Shared Space Router should route only traffic from the ISE Shared Space Database(S) IP address(s) to the Inner Boundary Firewall
- ii. The Inner Boundary ISE Shared Space Router should route only traffic from the ISE Shared Space Database(S) MAC address(s) to the Inner Boundary Firewall
- iii. The Inner Boundary back-end internal system facing ISE Shared Space router should route only the ISE information transfer protocols between the Inner Boundary Firewall and the ISE Shared Space Database(s)
- iv. Management of the Inner Boundary ISE Shared Space Router should be performed through an out-of-band management port
- v. The Inner Boundary ISE Shared Space Router should be designed to not allow routing between the network ports and the out-of-band management port

1.14 ISE Shared Space Outer Security Boundary

The ISE Shared Space Outer Security Boundary Logical Diagram depicted in Figure G-4 shows the required components of the Outer Security Boundary that control communications between the external requestors and the Front-End Web Server. The Outer Security Boundary is composed of an “Inside-VPN” ISE Shared Space Security Monitoring Appliance, Outer Boundary ISE Shared Space Facing Router, Outer Boundary Firewall, Outer Boundary ISE CORE Facing Router/VPN, and Outside VPN Security Monitoring Appliances.

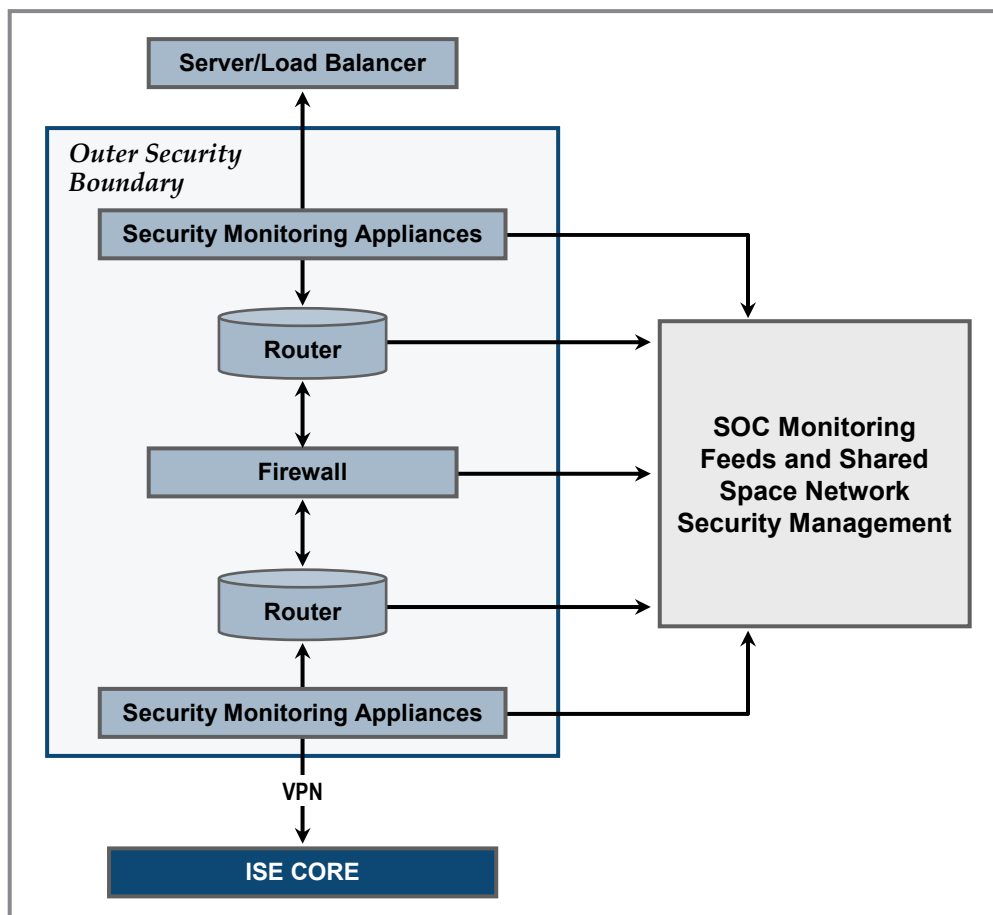


Figure G-4. ISE Shared Space Outer Security Boundary Logical Diagram

1.14.1 “Inside-VPN” ISE Shared Space Security Monitoring Appliances

The following is the set of recommended security requirements for the “Inside-VPN” ISE Shared Space Security Monitoring Appliances:

“Inside-VPN” ISE Shared Space Security Monitoring Appliances: Recommended Security Requirements

- i. The “Inside-VPN” ISE Shared Space Security Monitoring Appliances should examine network traffic passing through the Outer Security Boundary between the Load Balancer and ISE Core (note: only if Load Balancer is present in deployment)
- ii. The “Inside-VPN” ISE Shared Space Security Monitoring Appliances should examine network traffic passing through the Outer Security Boundary between the Front-End Web Server and ISE Core (note: only if Load Balancer is NOT present in deployment)
- iii. Management of the “Inside-VPN” ISE Shared Space Security Monitoring Appliances should be performed through an out-of-band management port
- iv. The “Inside-VPN” ISE Shared Space Security Monitoring Appliances should be designed to not allow routing between the network ports and the out-of-band management port

1.14.2 Outer Boundary ISE Shared Space Facing Router

The following is the set of recommended security requirements for the Outer Boundary ISE Shared Space Facing Router:

**Outer Boundary ISE Shared Space Facing Router:
Recommended Security Requirements**

- i. The Outer Boundary ISE Shared Space Facing Router should route traffic only to or from the Load Balancer IP address to the Outer Boundary Firewall (note: only if Load Balancer is present in deployment)
- ii. The Outer Boundary ISE Shared Space Facing Router should route traffic only from the Load Balancer MAC address to the Outer Boundary Firewall (note: only if Load Balancer is present in deployment)
- iii. The Outer Boundary ISE Shared Space Facing Router should route traffic only to or from the Front-End Web Server IP address(s) to the Outer Boundary Firewall (note: only if Load Balancer is NOT present in deployment)
- iv. The Outer Boundary ISE Shared Space Facing Router should route traffic only from the Front-End Web Server MAC address(s) to the Outer Boundary Firewall (note: only if Load Balancer is NOT present in deployment)
- v. The Outer Boundary ISE Shared Space Facing Router should route only approved ISE information transfer protocols between the Inner Boundary Firewall and the Load Balancer (note: only if Load Balancer is present in deployment)
- vi. The Outer Boundary ISE Shared Space Facing Router should route only approved ISE information transfer protocols between the Inner Boundary Firewall and the Front-End Web Server(s) (note: only if Load Balancer is NOT present in deployment)
- vii. Management of the Outer Boundary ISE Shared Space Facing Router should be performed through an out-of-band management port
- viii. The Outer Boundary ISE Shared Space Facing Router should be designed to not allow routing between the network ports and the out-of-band management port

1.14.3 ISE Shared Space Outer Boundary Firewall

The following is the set of recommended security requirements for the Outer Boundary Firewall:

Outer Boundary Firewall: Recommended Security Requirements

- i. The Outer Boundary Firewall should allow only approved ISE information transfer protocols to pass through the interface
- ii. Management of the Outer Boundary Firewall should be performed through an out-of-band management port
- iii. The Outer Boundary Firewall should be designed to not allow routing between the network ports and the out-of-band management port

1.14.4 ISE Shared Space Outer Boundary ISE CORE Facing Router/VPN

The following is the set of recommended security requirements for the Outer Boundary ISE CORE Facing Router/VPN:

**Outer Boundary ISE Core Facing Router/VPN:
Recommended Security Requirements**

- i. Management of the Outer Boundary ISE Core Facing Router/VPN should be performed through an out-of-band management port
- ii. The Outer Boundary ISE Core Facing Router/VPN should be designed to not allow routing between the network ports and the out-of-band management port
- iii. The Outer Boundary ISE Core Facing Router/VPN should be designed to not route any inbound network communication not received from a current validated VPN session
- iv. The Outer Boundary ISE Core Facing Router/VPN should be designed to not route any outbound network communication not addressed to a current validated VPN session

1.14.5 ISE Shared Space “Outside-VPN” Security Monitoring Appliances

The following is the set of recommended security requirements for the Outside Security Monitoring Appliances:

**“Outside-VPN” Security Monitoring Appliances:
Recommended Security Requirements**

- i. The Outside Security Monitoring Appliances should examine network traffic passing between the Outer Boundary ISE Core Facing Router/VPN and ISE Core
- ii. Management of the Outside Security Monitoring Appliances should be performed through an out-of-band management port
- iii. The Outside Security Monitoring Appliances should be designed to not allow routing between the network ports and the out-of-band management port

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>

