

ISE Enterprise Architecture Framework

Version 2.0

September 2008



INFORMATION SHARING ENVIRONMENT ENTERPRISE ARCHITECTURE FRAMEWORK

Prepared by the
Program Manager, Information Sharing Environment

This page intentionally blank.

INFORMATION SHARING ENVIRONMENT GUIDANCE (ISE-G)
INFORMATION SHARING ENVIRONMENT (ISE)
ENTERPRISE ARCHITECTURE FRAMEWORK (EAF)
VERSION 2.0

1. Authority. The National Security Act of 1947, 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.

2. Purpose. The *ISE EAF* issuance provides a strategic roadmap to enable long-term business and technology standardization and information systems planning, investing, and integration in the ISE. The intent of the *ISE EAF* is to document and organize the ISE mission business goals and processes, services, data, and technologies, and other operational capabilities necessary to facilitate information sharing. The *ISE EAF* builds upon and leverages existing policies, business practices, and technologies in use by Federal, State, local and tribal (SLT) governments in a manner that fully protects the legal rights of all United States persons.

This *ISE EAF Version 2.0* supersedes *ISE EAF Version 1.0* issued August 2007. This newest version of the *ISE EAF* provides additional structured descriptions of the ISE's associated business processes, information flows and relationships, services, and high-level data packet descriptions and exchange relationships.

3. Applicability. The *ISE EAF* 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, consistent with Section 1016(i) of the IRTPA, as amended.

4. References. *ISE Implementation Plan*, November 2006; *ISE Enterprise Architecture Framework (EAF)*, Version 1.0, August 2007; *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).

5. Definitions.

- a. Enterprise Architecture - is a strategic information asset base, which defines the mission, the information necessary to perform the mission and the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. [Endorsed definition from the Federal CIO Council]
- b. Federal Enterprise Architecture Framework - a business-driven framework that defines and aligns Federal business functions and supporting technology and includes a set of five common models (performance, business, data, services component, and technical).
- c. ISE Enterprise Architecture Framework - presents a logical structure of ISE business processes, information flows, and relationships, services, and high-level data packet descriptions and exchange relationships.
- d. ISE Implementation Agent - refers to an organization responsible for providing additional infrastructure and services supporting an integrated identity and access management process in the ISE.
- e. ISE participant - any Federal, State, local or tribal government organization that participates in the ISE (ISE Implementation Plan, November 2006).
- f. Segment Architectures - are logically arranged documents 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).

6. Guidance. This *ISE EAF* 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. The *ISE EAF* 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 EAF*; and
 - 2) Monitor the implementation and use of the *ISE EAF* and subsequent updates in alignment with Federal Enterprise Architecture (FEA) assessment guidance.

b. Each ISE participant shall:

- 1) Incorporate *ISE EAF* 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 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});
- 3) Incorporate the *ISE EAF* attributes into agencies transition planning strategy for enterprise architecture or Information Sharing Segment Architectures development and implementation;
- 4) Abide by ISE performance goals and strategies while implementing the *ISE EAF*; and
- 5) Abide by ISE privacy and civil liberties policies while implementing the *ISE EAF*.

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



Thomas E. McNamara
Program Manager for the
Information Sharing Environment

Date: October 21, 2008

Attachment(s):

ISE EAF Version 2.0
ISE EAF Version 2.0 Appendices

This page intentionally blank.

INFORMATION SHARING ENVIRONMENT ENTERPRISE ARCHITECTURE FRAMEWORK, VERSION 2.0

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

September 2008

This page intentionally blank.

TABLE OF CONTENTS

List of Figures	vi
List of Tables	vii
Executive Summary	ix
Chapter 1 – Introduction	1
1.1 Background	1
1.1.1 Vision	1
1.2 Purpose and Scope	2
1.3 ISE EAF Review and Release Approach.....	2
1.4 ISE Architecture Program Product Set	3
1.5 Enterprise Architecture Principles.....	3
1.5.1 ISE EAF Overarching Principles	3
1.5.2 ISE EAF Operating Principles	4
1.5.3 ISE EAF Technical Principles.....	5
1.6 Definitions.....	5
1.6.1 Terrorism, Homeland Security, and Law Enforcement Information as it Relates to Terrorism.....	5
1.6.2 ISE Participants.....	7
1.6.3 Affected Organizations.....	7
Chapter 2 – ISE Architecture Program Overview	9
2.1 Enterprise Architecture Framework Concepts	9
2.2 The ISE Enterprise Architecture Framework	11
2.2.1 ISE Implementer’s View	14
2.2.2 The ISE Core Segment	15
2.2.3 The ISE Participant Segments	16
2.3 ISE Implementation Agents Roles and Responsibilities	18
2.4 Coordination, Integration, and Re-use.....	20
Chapter 3 – Policy and Governance, Drivers and Requirements.....	23
3.1 Policy and Governance	23
3.1.1 Decision Making.....	23
3.2 The Federal Transition Framework Catalog	24
3.3 Drivers and Requirements.....	25
Chapter 4 – Information Security and Assurance	27
4.1 Introduction.....	27
4.2 Information Security and Assurance Overview	27
4.3 Policy and Governance	27
4.4 Risk Management.....	28
4.5 ISE Information Security and Assurance Model	29

4.5.1	Four Partitions of the <i>ISE EAF</i> Architect's View in Relation to IA Capabilities.....	30
4.5.2	ISE IA Model	30
4.5.3	Information Assurance Categories	31
4.6	Identity and Access Management (IdAM) Framework	36
4.6.1	The ISE IdAM Framework	36
4.6.2	IdAM Functionality	37
Chapter 5	– Business Partition	39
5.1	Introduction.....	39
5.2	Performance Management Overview	39
5.3	FEA and ISE EAF	40
5.3.1	The FEA BRM	40
5.4	ISE Business Process Framework	40
5.4.1	Target Business Processes.....	42
5.4.2	The ISE Business Partition.....	43
5.5	Core Business Process Analysis and Information Flows for ISE Mission Business Processes	47
5.5.1	ISE Business Process Modeling Methodologies	47
5.5.2	Information Flows.....	47
5.6	Business Process Application Example.....	48
5.6.1	ISE Suspicious Activity Report (ISE-SAR)	48
5.6.2	Identification and Screening (TWL Components).....	50
5.6.3	Alerts, Warnings and Notifications (AWN).....	52
Chapter 6	– Application and Service Partition.....	55
6.1	Introduction.....	55
6.1.1	Overview	55
6.1.2	An Introduction to Service Oriented Architecture	55
6.1.3	Terminology	56
6.2	FEA Service Component Reference Model Mapping	57
6.3	Baseline Application and Service Partition	59
6.4	Application and Service Target Partition – ISE Core Segment.....	60
6.4.1	Overview	60
6.4.2	ISE Shared Spaces.....	61
6.4.3	Transport.....	63
6.4.4	Network Management Function	65
6.4.5	ISE Portal Services	65
6.4.6	ISE Management Portal (IMP)	67
6.4.7	ISE Core Services.....	68
6.4.8	Mission Processes Usage of ISE Core Services.....	74
6.5	Target Application and Service Partition – ISE Participant Segment.....	83

Chapter 7 – Data Partition	85
7.1 Introduction.....	85
7.1.1 Functional Standards	86
7.1.2 Linkage Between Business and Data Partitions.....	86
7.2 “TO-BE” Data Partition	87
7.2.1 Compliance with the FEA Data Reference Model	87
7.3 Common Terrorism Information Sharing Standards	90
7.3.1 NIEM and UCore 2.0.....	94
7.3.2 Critical Success Factors.....	98
7.3.3 Observations and Issues.....	98
Chapter 8 – Technical Partition.....	101
8.1 Introduction.....	101
8.2 Technical Reference Model Mapping	102
8.3 Access Layer	106
8.4 Services Layer.....	107
8.5 Translation Layer.....	107
8.6 Transport Layer	108
8.7 ISE Shared Spaces Layer	109
8.8 Technological Best Practices.....	109
8.9 CTISS Program Technical Standards.....	110
8.10 Technical Standards under Consideration.....	114
 Appendices	
Appendix A – ISE EAF Acronym List.....	A-1
Appendix B – ISE EAF Glossary.....	B-1
Appendix C – ISE Business Processes	C-1
Appendix D – ISE SAR Information Flow Description.....	D-1
Appendix E – ISE Identification and Screening Business Process Analysis: Terrorist Watchlist Component – June 2008	E-1
Appendix F – ISE Alerts, Warning, and Notification Business Process Analysis – June 2008.....	F-1
Appendix G – ISE Shared Spaces and Core Discussion	G-1

LIST OF FIGURES

Figure 2-1. The ISE Is a Virtual Environment to Share Terrorism Information	12
Figure 2-2. ISE EAF	13
Figure 2-3. ISE Enterprise Architecture Framework: Implementer’s View.....	15
Figure 2-4. Approved Guideline 2 Framework.....	17
Figure 2-5. ISE EAF Bridging the Community Spectrum.....	18
Figure 3-1. ISE Governance.....	23
Figure 4-1. The ISE Risk Management Framework	29
Figure 4-2. IA Relative to Four Partitions of the ISE Architect’s View	30
Figure 4-3. IA Model.....	31
Figure 5-1. ISE Business Process Framework.....	41
Figure 5-2. Relationship Mapping of Mission Processes and ISE Core Services.....	42
Figure 5-3. The BRM Sub-Function Added to the FEA BRM	44
Figure 5-4. The FEA BRM Highlighting ISE Attributes	45
Figure 5-5. Interdependencies of Mission Process to FEA BRM Sub-functions.....	46
Figure 5-6. National SAR Process Steps	48
Figure 5-7. ISE-SAR Information Flow Diagram.....	49
Figure 5-8. Consolidated TWL Nomination and Export Information Flow.....	51
Figure 5-9. Consolidated TWL Screening, Encounter Management, and Quality Assurance Information Flow.....	52
Figure 5-10. ISE AWN Information Flow	53
Figure 6-1. FEA Service Component Reference Model	56
Figure 6-2. Application and Service Partition of the ISE TO-BE Architecture.....	61
Figure 7-1. DRM Overview	87
Figure 7-2. DRM Abstract Model.....	89
Figure 7-3. CTISS Framework	92
Figure 7-4. CTISS Universal Core Development.....	95
Figure 7-5. CTISS Information Exchange Life Cycle.....	96
Figure 8-1. CTISS Framework	102
Figure 8-2. FEA Technical Reference Model	103
Figure 8-3. Conceptual View of Typical Participant Connection to the ISE	105
Figure 8-4. Technology View of Participant ISE Shared Space	106

LIST OF TABLES

Table 1-1. ISE Architecture Program Products	3
Table 2-1. Levels of Architectures	10
Table 2-2. ISE EAF Partitions	14
Table 6-1. FEA Service Component Reference Model Alignment to ISE Core Mission Process	58
Table 6-2. Mapping of ISE Core and Portal Services to SRM Service Domain and Type	59
Table 6-3. Discovery Service Capabilities	70
Table 6-4. Security Services Capabilities	71
Table 6-5. Mediation Service Capabilities	71
Table 6-6. Messaging Service Capabilities	72
Table 6-7. ESM Service Capabilities	73
Table 6-8. Storage Service Capabilities	73
Table 6-9. Collaboration Services Capabilities	74
Table 6-10. Mapping of AWN Information Flow to <i>ISE EAF</i> Core Services and FEA SRM	76
Table 6-11. Mapping of ISE SAR Top-level Business Process to ISE EAF Core Services and FEA SRM	78
Table 6-12. Mapping of TWL Information Flow to <i>ISE EAF</i> Core Services and FEA SRM	81
Table 7-1. CTISS Information Exchange Life Cycle Support of the FEA DRM.....	98
Table 8-1. Technical Reference Model Mapping	104
Table 8-2. CTISS Program Technical Standards	111
Table 8-3. ISE Technical Standards being Considered.....	115

This page intentionally blank.

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, released on 25 October 2005, 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.”

Furthermore, on 16 December 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 how information is acquired, accessed, shared, and used within the ISE.²

On 31 October 2007, the President issued the first *National Strategy for Information Sharing* to prioritize, unify, and integrate the Nation’s efforts to advance the sharing of terrorism-related information among Federal and SLT officials, the private sector, and foreign partners. This strategy takes a holistic approach for improved information sharing capabilities at all levels of government and with the private sector. An underlying set of guiding principles resulted from this strategy: (i) effective information sharing comes through strong partnership among Federal, SLT authorities, private sector organizations, and foreign partners; (ii) information acquired for one purpose, or under one set of authorities, might provide unique insights when combined to foster a culture of awareness and use information that was not known to support and protect counterterrorism efforts.; (iii) procedures, processes, and systems must draw upon and

¹ Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, Title I, Subtitle A, § 1016 (codified as 6 U.S.C. § 485). Section 1016 of IRTPA was amended on August 3, 2007 by the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title V, Subtitle A, § 504. This version of the ISE Enterprise Architecture Framework (EAF) does not address the additional authorities and requirements set forth in P.L. 110-53; these will be addressed in a future version of the ISE EAF. Of note, however, the new law expands the scope of the ISE to explicitly include homeland security information and weapons of mass destruction information and sets forth additional ISE attributes. It also endorses and formalizes 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 Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment (White House: Washington, DC, 2005), Section 1, found at <http://www.whitehouse.gov/news/releases/2005/12/20051216-10.html>.

integrate existing technical capabilities; (iv) information sharing must be woven together; and (v) State and major urban area fusion centers represent a valuable information sharing resource and should be incorporated into the national information sharing framework.

The *Information Sharing Environment Implementation Plan*,³ in response to IRTPA and presidential direction, provided an initial description of the ISE plans, policies, requirements, and governance structure. The Implementation Plan introduced the ISE architecture and standards programs as cross-community, perpetuating programs to help ISE participants plan, install, and operate their information resources in a manner that will contribute components of their internal infrastructures into the physical instantiation of a nationwide counterterrorism ISE.⁴ While participants in the ISE are still responsible for their own counterterrorism missions and systems supporting these missions, the physical ISE, as a functioning system-of-systems, will improve the overall effectiveness of individual counterterrorism business processes and capabilities through increased access to terrorism information across the ISE community. This counterterrorism mission enhancement addresses one of the recommendations from the 9/11 Commission to unify “the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional governmental boundaries.”⁵ Furthermore, it also supports those capabilities necessary to resolve the problems identified in the ISE Presidential Guideline 2 Report, where “multiple communications channels, processes, and systems are used at the Federal level,” and where “the lack of a systemic and coordinated approach to sharing terrorism information can result in the production and dissemination of mixed and at times competing messages from Federal officials.”⁶

Consistent with the Presidential Guidelines directing that “the ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures” and with “the objective of establishing a decentralized, comprehensive, and coordinated environment,” and other national level authorities, the Office of the Program Manager for the Information Sharing Environment (PM-ISE) developed and issued the *ISE Enterprise Architecture Framework (ISE EAF)*,⁷ Version 1.0 in August 2007. The *ISE EAF* and supporting Common Terrorism Information Sharing Standards (CTISS) Program helped improve information sharing practices, reduce barriers to sharing, and institutionalize sharing by providing a new construct for planning, installing, and operating nationwide information resources within the infrastructure fabric of the

³ Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, November 2006, found at Internet site <http://www.ise.gov>.

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

⁵ National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, (U.S. Government Printing Office: Washington, DC, 2004), 400.

⁶ Extracted from the Recommendations for Presidential Guideline 2, found at Internet site www.ise.gov.

⁷ The Office of Management and Budget (OMB) has suggested the term “enterprise architecture framework” for the ISE rather than “enterprise architecture” because the *ISE EAF* is a cross-agency construct providing guidance to agencies developing the information sharing components of their enterprise architectures. The term “enterprise architecture” is used in the OMB context to refer to an architecture prepared by a Chief Information Officer (CIO) to manage the IT resources of a specific department or agency.

ISE. *ISE EAF, Version 1.0* laid the foundation in defining practices and methodologies required to build implementable and executable information sharing enterprise architectures and segment architectures leveraging core ISE principles. This version of the *ISE EAF* builds on the foundation established in Version 1.0 to provide more specificity and granularity for ISE business mission processes and information flows and includes Implementation Agent roles and responsibilities for implementation within the ISE Core. This version also provides a cross mapping of ISE mission business processes to the Federal Enterprise Architecture (FEA) Business Reference Model (BRM) sub-functions.

This page intentionally blank.

Chapter 1 – Introduction

1.1 Background

1.1.1 Vision

The vision for the ISE is to create a powerful new national capability to share, search, and analyze terrorism information. The ISE will link information across jurisdictional boundaries and create a distributed, protected, trusted environment for sharing information. The ISE will leverage the National Counterterrorism Center (NCTC) as the focal point for information aggregation and discovery to support information sharing at the Federal level. It will provide mechanisms to permit partner agencies at the Federal and State/local levels (e.g., fusion centers) to share data based on common standards and practices.

The ISE will also supply capabilities to discover and link terrorism information on a national basis. It will facilitate the process of detecting relationships among people, places, things, and events and improve the ability of analysts to “connect the dots” among seemingly unrelated data. It will provide a directory of community contact information, currently established as the Electronic Directory Service, and collaboration tools that will be discussed in Chapter 6.

The envisioned ISE will derive a set of the desired capabilities and, furthermore, leverage, to the maximum extent practicable, existing systems, processes, policies, and information. It will interface to ongoing developments within all Federal agencies to include the information assurance work being addressed by the National Security Agency (NSA), the Net-Centric Enterprise Services (NCES) being addressed by the Defense Information Systems Agency (DISA), the Global Information Grid (GIG), and the Department of Defense (DoD)/Intelligence Community (IC) Universal Core being addressed by the Department of Defense (DoD) and the Director of National Intelligence/CIO, the Continuity Communications Architecture and the National Command and Coordination Capability (NCCC) under development by the National Communication System (NCS), and the National Information Exchange Model (NIEM) development under the leadership of the Department of Justice (DoJ) and the Department of Homeland Security (DHS).

The envisioned ISE will enable the sharing of information within three security domains, including Controlled Unclassified Information (CUI)/Sensitive but Unclassified (SBU), Secret/Collateral, and TS/Sensitive Compartmented Information (SCI). Networks will connect peer-authorized users from Federal Government agencies, State, and major urban area fusions centers and, where appropriate, the private sector and foreign partners.

1.2 Purpose and Scope

Section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004*⁸ calls for the President to “create an Information Sharing Environment (ISE) for the sharing of terrorism information” among Federal, SLT governments, and, where appropriate, with private sector entities and foreign partners, in a manner consistent with the protection of homeland and national security and with the protection of privacy and civil liberties. To assist in the development of the ISE, the *Intelligence Reform and Terrorism Prevention Act* provides for the designation of a Program Manager (PM) “responsible for information sharing across the Federal Government.”

The *Intelligence Reform and Terrorism Prevention Act* further requires a description addressing the impacts of the ISE on enterprise architectures of participating agencies.⁹ Similarly, the December 2005 Presidential Memorandum directs building the ISE upon existing Federal Government resources that include standards, systems, and architectures.¹⁰ This *ISE EAF* will drive long-term information sharing requirements leveraging reuse capabilities for improvement and information systems planning, investing, and integration to support the effective conduct of U.S. counterterrorism activities.

The *ISE EAF* will be used to guide the implementation of the ISE capability. The *ISE EAF* sets the direction and provides incremental steps toward the targeted capability. This document provides a description of the *ISE EAF*.¹¹ It was developed to meet three objectives:

- To provide a comprehensive, high-level description of the ISE architecture
- To establish the architectural framework for implementing ISE capabilities
- To identify key architectural decisions that have been made or must be made

1.3 ISE EAF Review and Release Approach

Future versions of the *ISE EAF* will be published to include additional material resulting from ongoing analysis and review by ISC members. Subsequent versions will also be published to incorporate future business processes and information flows. A note has been added at several places within the document to indicate that work is proceeding and, in some cases, to request specific inputs from reviewers. Input from the ISE community will be reflected in subsequent release versions of this document. Changes

⁸ 6 U.S.C. § 485(b).

⁹ 6 U.S.C. § 485(e)(2).

¹⁰ Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment, *Ibid.*, Section 1.

¹¹ The OMB has suggested the term “enterprise architecture framework” for the ISE rather than “enterprise architecture” to highlight the fact that the ISE is a cross-agency construct to be used as guidance for agencies developing the information sharing aspects of their enterprise architectures. The term “enterprise architecture” is used in the OMB context to refer to the architectures prepared by CIOs to manage the IT resources of a specific department or agency.

will be made in accordance with PM-ISE configuration management procedures implemented by the ISE Chief Architects' Roundtable.

1.4 ISE Architecture Program Product Set

The ISE Architecture Program is described in a series of architectural products for development. This *ISE EAF* provides a strategic overview with more detailed descriptions being incorporated as additional business processes and requirements for the ISE are defined. The product set is summarized in Table 1-1.

Table 1-1. ISE Architecture Program Products

Title	Description
<i>ISE Drivers and Requirements Specification</i>	A high-level specification of the ISE authoritative sources and requirements that establishes the foundation for creating the <i>ISE EAF</i> .
<i>ISE EAF</i>	A high-level description of the components, structure, and unifying characteristics of the ISE.
<i>ISE Profile and Architecture Implementation Strategy (PAIS)</i>	A guide for ISE Federal departments and agencies that describes what each must do to connect to the ISE, expose data to the ISE, and access data and services provided by the ISE.

1.5 Enterprise Architecture Principles

Principles are underlying and fundamental elements of sound enterprise architectures. In general, architecture principles are intended to influence the development, maintenance, and use of enterprise architectures. They guide the development of architecture by providing criteria for selecting alternative architectural choices. They are developed from industry best practices and standards. Highlights are provided below.

1.5.1 ISE EAF Overarching Principles

The Federal Chief Information Officers (CIO) Council has established a set of Federal Architecture Principles from which the following *ISE EAF* overarching principles have been derived.¹² Each ISE participant has its own enterprise architecture (EA) that addresses its unique mission. The *ISE EAF* will not replace these existing architectures or ongoing agency architecture developments. However, the *ISE EAF* will augment existing architectures by identifying the relationships needed to facilitate terrorism information sharing among ISE participants.

¹² CIO Council, Architecture Principles for the U.S. Government, (CIO Council: Washington, DC, 2007) found at Internet site www.cio.gov.

To achieve the vision for the ISE, the *ISE EAF* uses and recognizes the following overarching principles:

- The Federal Government is a single, unified enterprise
- Federal agencies collaborate with other Governments and people
- The Federal architecture is mission-driven
- Security, privacy, and protecting information are core Government needs
- Information is a national asset
- The Federal architecture simplifies Government operations

Viewed together, the ISE's vision and *ISE EAF* overarching principles (1) represent the focal point for agencies' ISE information sharing-focused IT initiatives and (2) influence foundational elements for agencies to develop the Performance Reference Model (PRM) sections of their EA. With regard to the PRM, agency-specific EAs will have to be evaluated against the *ISE EAF*'s vision and overarching principles in the context of the organization's mission, IT initiatives, and related outputs and outcomes to establish a clear "line of sight" to an agency's desired results.¹³ Using this approach, agencies will be able to develop measures to not only assess IT performance, as prescribed in the PRM, but also ensure adherence to the *ISE EAF*'s vision and principles.

1.5.2 ISE EAF Operating Principles

The creation of the ISE was mandated by the *Intelligence Reform and Terrorism Prevention Act*. *ISE EAF* operating principles are summarized below:

- The Federal Enterprise Architecture Framework is an ISE point of linkage;¹⁴
- Terrorism information sources and methods must be protected;¹⁵
- Information security policies and practices are applied to systems¹⁶
- The NCTC serves as an aggregation and coordination point for the ISE;¹⁷
- Fusion Centers are SLT information dissemination points; and¹⁸
- Increased situational awareness posture is a driver for the ISE.¹⁹

¹³ See OMB – The Federal Enterprise Architecture Program Management Office, How to Use the Performance Reference Model, Version 1.0, September 2003, p.7.

¹⁴ Derived from OMB, Circular A-11 (OMB: Washington, DC, 2007) and *Federal Enterprise Architecture Program EA Assessment Framework, 2.1* (OMB: Washington, DC, 2005).

¹⁵ Derived from Executive Order 13388: Further Strengthening the Sharing of Terrorism Information to Protect Americans, found at Internet site <http://www.whitehouse.gov/news/releases/2005/10/20051025-5.html>.

¹⁶ Derived from the E-Government Act of 2002, Pub. L. No. 107-347, Title III.

¹⁷ Derived from 50 U.S.C. § 404o.

¹⁸ Derived from Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Section 3.4.

¹⁹ Derived from Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Section 3.2.

- The ISE will define participant roles and responsibilities²⁰
- Federal laws and mandates will be followed within the *ISE EAF*
- The ISE will identify laws and mandates that impede information sharing and recommend changes

1.5.3 *ISE EAF* Technical Principles

Though the ISE will be a virtual environment, its physical infrastructure and access will include IT elements leveraged across the ISE community. A set of best practices and mandates for the technical components of the *ISE EAF* is established through Federal law as well as industry practices for similar types of environments. This set of *ISE EAF* technical principles was created with reference to existing Federal EA efforts such as those of the Intelligence Community and other ISE participants. The following list describes the *ISE EAF* Technical Principles to be applied:

- Leverage existing strategies for ISE infrastructure
- Prevent single points of failure in ISE network design
- Access information in the ISE electronically
- Use service-level-agreements (SLAs) to govern services and appropriate activities
- Collect system performance metrics from ISE assets
- Evaluate vendor capability for determining the best ISE technical solutions
- Use voluntary-consensus and Government-unique standards as appropriate

1.6 Definitions

The definitions in this section are extracted from authoritative sources and are repeated here for the convenience of the reader.

1.6.1 Terrorism, Homeland Security, and Law Enforcement Information as it Relates to Terrorism

The ISE is focused on sharing terrorism information, homeland security information, and law enforcement information as it relates to terrorism. In developing the *ISE EAF*, this statement and the definitions below will, at a high level, bound the scope of information to be shared.

Terrorism information is defined in the *Intelligence Reform and Terrorism Prevention Act* as “all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to

²⁰ 6 U.S.C. § 485.

- 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
- Threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations
- Communications of or by such groups or individuals
- Groups or individuals reasonably believed to be assisting or associated with such groups or individuals”²¹

Homeland security information is defined in the Homeland Security Act, as amended, as “any information possessed by a Federal, State, or local agency that

- Relates to the threat of terrorist activity
- Relates to the ability to prevent, interdict, or disrupt terrorist activity
- Would improve the identification or investigation of a suspected terrorist or terrorist organization
- Would improve the response to a terrorist act”²²

For purposes of the ISE, **law enforcement information** means “any information obtained by or of interest to a law enforcement agency or official that is both

- Related to terrorism or the security of our homeland
- 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”²³

²¹ 6 U.S.C. § 485(a)(5).

²² 6 U.S.C. § 482(f)(1).

²³ Extracted from the Recommendations for Presidential Guideline 2, found at Internet site www.ise.gov.

1.6.2 ISE Participants

Unless otherwise specified in this document, the term “ISE participants” means all Federal, SLT entities, private sector organizations, and foreign partners that participate in the ISE.

1.6.3 Affected Organizations

The ISE serves five communities:

- Defense
- Foreign Affairs
- Homeland Security
- Intelligence
- Law Enforcement

These communities are composed of Federal and SLT governments, the private sector and foreign partners. Within each of these entities are first responders, operators, analysts, decision makers, and investigators who have information to share and need information to accomplish their missions. The ISE will provide the ways and means to make terrorism information available, discoverable, and useful by all ISE participants. In the example of Suspicious Activity Reporting (SAR), Alerts, Warnings, and Notifications (AWN), and Terrorist Watchlisting (TWL), these information exchanges occur across the entire ISE, providing information to support not only local activities, but potentially contributing to nationwide activities and other counterterrorism missions that may benefit from the initial gathering of SAR, AWN, and TWL information.

Success of the ISE depends on the degree of cooperation, coordination, and alignment among this diverse set of ISE participants. Further, the ISE must align with, complement, and support the individual missions of the ISE participants. The Nation’s terrorism information infrastructure cannot be separated from existing infrastructure supporting other mission priorities. An effective ISE will, at times, require changing the policies, business rules, processes, and technical systems that currently exist within the counterterrorism operating environment.

This page intentionally blank.

Chapter 2 – ISE Architecture Program Overview

2.1 Enterprise Architecture Framework Concepts

The U.S. Code defines an *enterprise* as “the related activities performed (either through unified operation or common control) by any person or persons for a common business purpose, and includes all such activities whether performed in one or more establishments or by one or more corporate or other organizational units.”²⁴ In this context, an enterprise can be a business unit, an entire corporation, a government agency, or a collection of businesses joined together in a partnership. The Government Accountability Office (GAO) maintains “An enterprise architecture provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., a Federal department) or a functional or mission area that cuts across more than one organization.”²⁵

The Federal Government has adopted a federated architecture approach. The Federal Enterprise Architecture Framework (FEAF) describes the top level of the federation and provides broad guidance for explaining a common approach for Enterprise Architecture (EA) development applicable across the Federal Government. However, as mandated by the Clinger-Cohen Act, each department has its own departmental enterprise architecture for which the head of agency is responsible through a Chief Information Officer.²⁶ These department-specific architectures must map back to the FEAF to demonstrate alignment and allow for investment management across the entire Federal Government enterprise. Within each department, agencies may develop subsidiary architectures that link back to the departmental EA and provide additional mission-specific details. Similarly, many SLT governments have or are developing EAs. Input from these partners will be reflected in future *ISE EAF* versions as appropriate.

In general, EAs are strategic management tools that help organizations view the relationships among missions, information, technology, and transitional processes through depictions of current environments (termed “AS-IS”) and future environments (termed “TO-BE”).





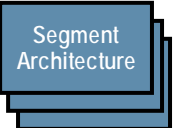


Table 2-1 depicts the hierarchical relationships among the various levels of architectures used within individual agencies and organizations across the ISE that are influenced by the *ISE EAF*. Consistent with Office of Management and Budget (OMB) guidance, frameworks and profiles, enterprise, segment, and solution architectures provide different perspectives and levels of detail for agencies and organizations in their EA planning.

²⁴ 29 U.S.C. § 203(r)(1).

²⁵ U.S. Government Accountability Office, Report GAO-06-219 (U.S. Government Printing Office: Washington, DC, 2005), 7.

²⁶ The Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), Pub. L. No. 104-106, Division E.

Table 2-1. Levels of Architectures

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

At the highest level, frameworks provide logical structures for classifying and organizing complex enterprise architecture information. Specifically the Federal Enterprise Architecture Framework (FEAF) provides "a structure for organizing Federal resources and for describing and managing Federal Enterprise Architecture activities."²⁷ The FEAF provides the basis for evaluation of each agency's EA by OMB. The OMB EA Assessment Framework measures agency effort to use information and information technology to improve agency performance by (1) closing mission performance gaps identified, (2) avoiding cost through collaboration, reuse and process reengineering/ product enhancements, (3) strengthening quality of investment, and (4) improving the quality, validity, and timeliness of program performance output. For ISE community stakeholders, the *ISE EAF* is based on the FEAF and presents a logical structure of strategic direction, business processes, information flows and relationships, services, and high-level data packet descriptions and exchange relationships intended to improve overall performance of implementation within the ISE. A companion document to the *ISE EAF*, the *ISE Profile and Architecture Implementation Strategy (PAIS)*, provides further clarification of how ISE participants are to implement and use their enterprise architectures to connect to the ISE. Overall, attributes at the framework level guide the migration of nationwide information resource capabilities and interfaces into individual agency/organization enterprise, segment, and solution architectures.

²⁷ CIO Council, Federal Enterprise Architecture Framework, Version 1.1, (CIO Council: Washington, DC, 1999), C-6.

Enterprise Architectures help organizations identify whether resources are aligned to internal mission and strategic goals and objectives, and are particularly useful in driving decisions affecting information technology investment portfolios. At the next level, segment architectures drive decisions for a business case or group of business cases supporting a core mission process or common service. And, at the lowest level, solution architectures define specific information technology assets in more detail such as applications or components, and the scope is primarily limited to a single project or capability.²⁸

The audience for this *ISE EAF* document, as Table 2-1 implies, are all ISE stakeholders and in particular the Chief Information Officers (CIOs), mission/business owners, Performance Improvement Officers (PIO), and enterprise architects of those Federal and SLT governments, private sector entities, and foreign partners that are participants in the ISE.

2.2 The ISE Enterprise Architecture Framework

Creating the ISE is not about building a massive new information system. The ISE aligns and leverages existing information sharing policies, business processes, technologies, and systems, and promotes a culture of information sharing through increased collaboration. OMB has suggested the use of the term “enterprise architecture framework” for describing the ISE architecture to highlight the fact that the ISE is a cross-agency construct.

Figure 2-1 illustrates the general *ISE EAF* architectural concept. The vision for the ISE is to create a powerful national capability to share and search terrorism information across jurisdictional boundaries. The ISE and the information resources developed using the *ISE EAF* will link ISE participants (Federal and SLT governments, foreign partners, and the private sector) and create a distributed, protected, and trusted environment for sharing information.

The ISE includes an ISE Core, which provides common services used by all participants. The ISE Core includes a connection capability and shared virtual spaces, indicated by the transparent cloud in the figure below. Each ISE participant uses shared services to expose selected counterterrorism-related data assets to the designated shared spaces.

²⁸ Office of Management and Budget, FEA Practice Guidance, (OMB: Washington, DC, 2006), 1-4, 1-5.

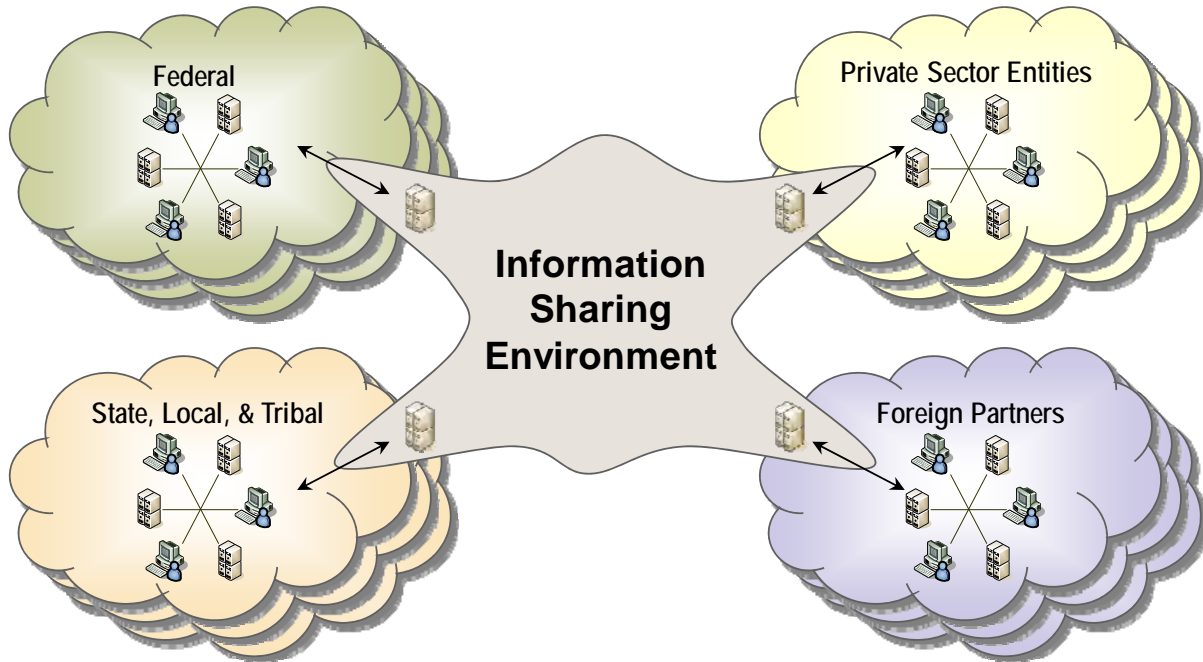


Figure 2-1. The ISE Is a Virtual Environment to Share Terrorism Information

The *ISE EAF* is illustrated in Figure 2-2. It is based on the Federal Enterprise Architecture Framework (FEAF),²⁹ modified to reflect the needs of the ISE. It also reflects the guidance provided in the OMB *EA Assessment Framework*.³⁰

²⁹ CIO Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (CIO Council: Washington, DC, 2001).

³⁰ Office of Management and Budget, *Enterprise Architecture Assessment Framework 3.0* (OMB: Washington, DC, 2008).

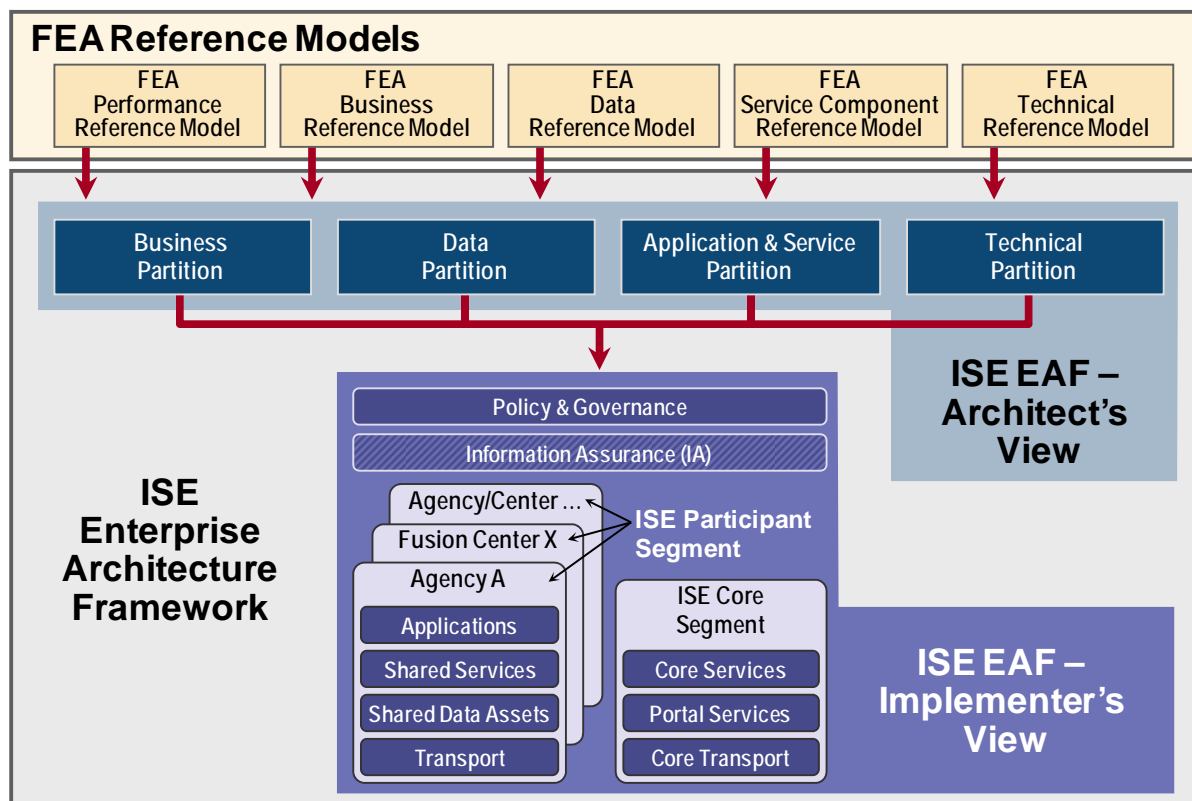


Figure 2-2. ISE EAF

The *ISE EAF* assists in coordinating activities and development of individual ISE participant enterprise architectures to drive the planning and management of those information resources that will physically define the nationwide ISE. As the maturity of the ISE continues to evolve, the *ISE EAF* will evolve and incorporate newly developed mission and service business processes, to include information flows, and additional requirements into future published versions.

An architecture is typically presented via multiple views or, in the ISE case, partitions. The ISE is described in terms of four partitions: Business, Data, Application and Service, and Technical. The table below, Table 2-2, briefly highlights the four partitions and offers an explanation of both the Implementer's and Architect's views. Each of these sections is explained in greater detail, along with architectural products, in subsequent chapters within this document.

Table 2-2. ISE EAF Partitions

EAF Partition	General Description
Business Partition	Identifies the performance drivers and desired outcomes, business functions, processes, and information flows that facilitate information sharing in the ISE.
Data Partition	Identifies and describes the data required to enable the ISE business processes through the functional standards of the CTISS. Defines universal core vocabulary and information exchange structures for sharing information across the various ISE business processes.
Application and Service Partition	Identifies and describes the software applications and service components that support the business processes. Includes Core Services and Portal Services used by all ISE participants, shared services provided by a participant for use by others, and the actual data assets (e.g., databases) to be shared.
Technical Partition	The technologies, technical standards of the CTISS, and patterns used to implement the applications and services.

2.2.1 ISE Implementer's View

The OMB has issued guidance on using architectural segments to define enterprise architecture. Enterprise, segment, and solution architectures provide different but related business perspectives by varying the level of detail and addressing related but distinct concerns. Just as enterprises are themselves hierarchically organized, so are the different views provided by each type of architecture. The components that make up the ISE can be seen as belonging to one of two views:

- The Architect's View is used to provide structural alignment of the ISE architectural components into the FEAF structure to ensure ISE strategic goals and objectives, business processes, investments, data, systems, services, and technologies are integrated and compatible with those across the Federal Government.
- The Implementer's View, shown in Figure 2-3, illustrates the major components that must be developed or integrated to implement the ISE at the segment and solution architecture levels. The Implementer's View is a useful view for planning and managing the development of ISE capabilities.

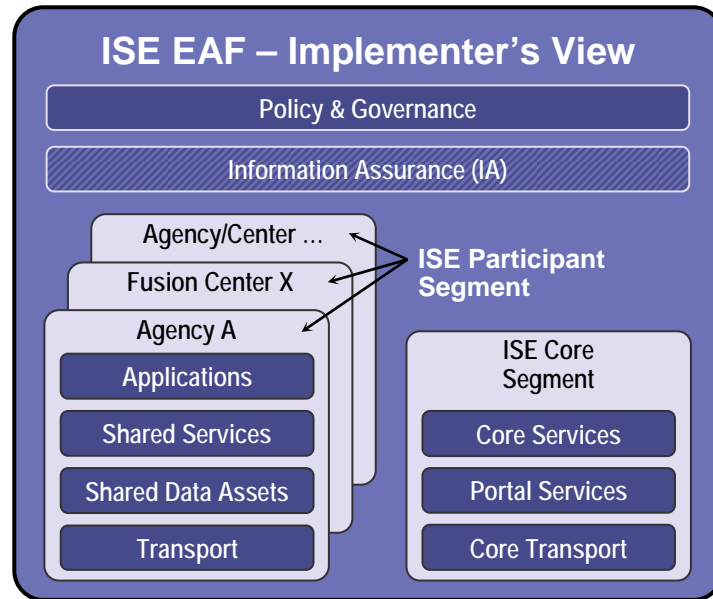


Figure 2-3. ISE Enterprise Architecture Framework: Implementer's View

Policy and Governance and Information Assurance (IA) span both the ISE Participants and ISE Core Segments. **Policy and Governance** provides the means for implementing and promulgating the necessary ISE directives and standards for establishing and evolving the ISE.

2.2.2 The ISE Core Segment

The **ISE Core** Segment can be viewed as the basic infrastructure that facilitates and/or supports the ISE environment at large. The **ISE Core** Segment provides Core Services, Portal Services, and Core Transport functions to all organizations that participate in the ISE.

- Core Services are those capabilities to enable the execution of ISE business processes across the ISE. These services are available for reuse and can be leveraged by all ISE participants (e.g., collaboration, security, storage, messaging, and discovery)
- Portal Services support the ISE Portal and ISE Management Portal functions and provide additional services (e.g., publish/subscribe, collaboration through a user interface (UI)) (These terms are further defined in Chapter 6)
- Core Transport includes the hardware, software, and transport media that support transmission and reception of information within and across the ISE

The ISE Core Segment will contain the core transport component that will be used to interconnect the separate ISE Shared Spaces of each ISE participant and allow exchange of information. It must also contain the necessary infrastructure components to implement service oriented architecture (SOA), as described further in Chapter 6.

The ISE Core is described as an independent entity; however, in practice it will be implemented as an extension to existing capabilities of one or more ISE Implementation Agents to provide these capabilities to all the ISE participants. These infrastructure components include Core Services such as directory and search capability, policies, and other resources that must be shared.

2.2.3 The ISE Participant Segments

The **ISE Participant** Segment shown on the left in Figure 2-3 (Agency A, Fusion Center X, Agency/Center ...) represents the components managed by an ISE participant or fusion center that uses or provides information for use within the ISE fabric. Applications developed or used may incorporate information and services provided by other participants through the ISE. Shared Data Assets are those information assets shared by participants via the ISE. These services typically provide other participants with access to data or capabilities “owned” by that organization. In the case of Suspicious Activity Reporting (SAR), Alerts, Warnings, and Notifications (AWN), and Terrorist Watchlist (TWL), this is where data is deposited.

Consistent with Presidential Guideline 2, State and major urban area fusion centers represent a valuable information-sharing resource and will be integrated into the national information-sharing infrastructure depicted through the *ISE EAF*. The State and major urban area fusion centers will become the focus, but not exclusive points, within the State and local environment for the receipt and sharing of terrorism information. The term “Collaborative Fusion Environment” refers to the fact that the environment will include State and major urban area fusion centers, a Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF)/Field Intelligence Group (FIG), a Department of Homeland Security (DHS) office, and a National Guard office. The ISE will also provide mechanisms to permit partner agencies at the Federal, State, and local levels (e.g., fusion centers) to share terrorism information based on common standards defined through the CTISS Program activity (explained in more detail in Chapter 7).

The Guideline 2 framework, depicted in Figure 2-4, illustrates a coordinated, collaborative structure through which terrorism information is shared between and among an example subset of participating Federal, SLT, and private sector organizations to support a variety of mission business processes. Individual agencies are identified to emphasize their current statutory responsibilities working with State governments in terrorism information sharing. Consistent with IRTPA, the ISE will leverage the National Counterterrorism Center (NCTC) that continues to serve as the central and shared knowledge bank on known and appropriately suspected terrorists and international terror groups. Also consistent with IRTPA, the NCTC ensures that agencies have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analyses. The NCTC and State and major urban area fusion centers are critical components in the ISE.

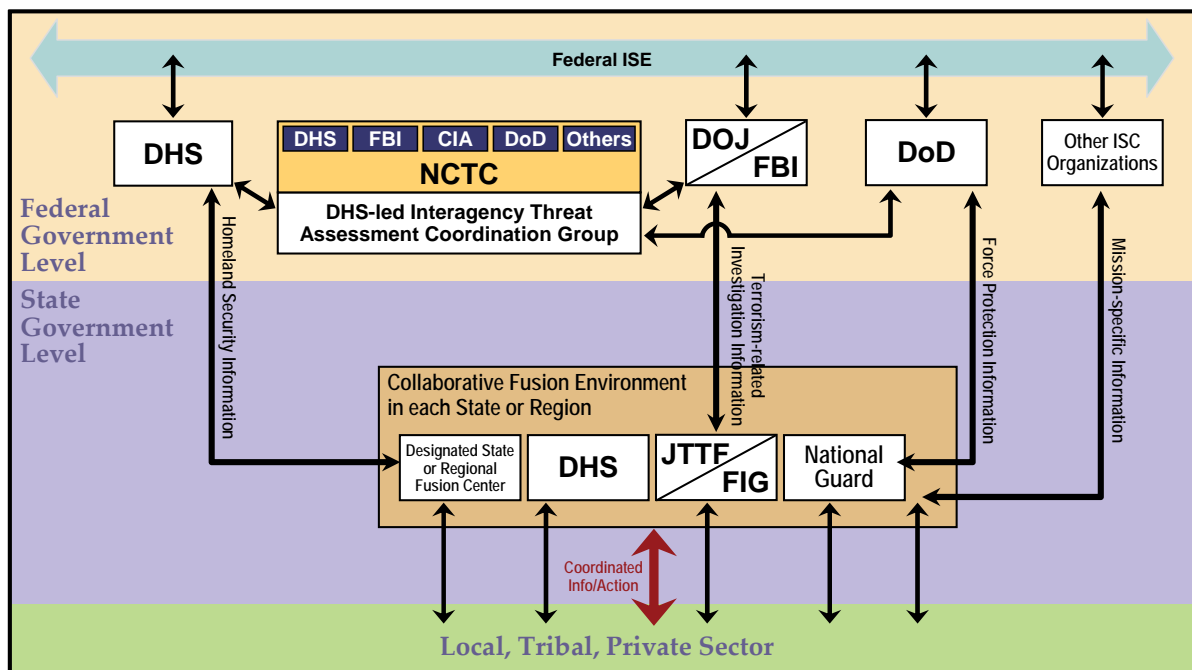


Figure 2-4. Approved Guideline 2 Framework³¹

The ISE derives desired capabilities by leveraging, to the maximum extent practicable, existing systems, processes, and policies. The ISE enables the sharing of information across three security domains, including Controlled Unclassified Information (CUI)/Sensitive but Unclassified (SBU),³² Secret/Collateral, and Top Secret (TS)/Sensitive Compartmented Information (SCI). Across these security domains, the ISE serves five communities: defense, foreign affairs, homeland security, intelligence, and law enforcement. There are many agencies within these communities including those in the Department of Treasury (DOTreas), Department of Interior (DOI), Department of Health and Human Services (HHS), Department of Commerce (DOC), Department of Justice (DOJ), Department of Energy (DOE), Department of State (DOS), Department of Homeland Security (DHS), Department of Defense (DoD), and Department of Transportation (DOT). There are also agencies from the Intelligence Community, as well as SLT governments, the private sector, and foreign governments. Each organization should have its own enterprise architecture (EA) that addresses its unique mission. The *ISE EAF* will not replace these existing architectures or ongoing agency architecture developments. Instead, the *ISE EAF* will provide strategic architectural guidance for developing and modifying existing architectures by identifying the interfaces and standards needed to facilitate information sharing between other organizations in the ISE.

³¹ Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Ibid., 71.

³² May 9, 2008, the President released the Memorandum for the *Heads of Departments and Agencies on the Designation and Sharing of Controlled Unclassified Information (CUI)*.

As depicted in Figure 2-5 below, the *ISE EAF* and *PAIS* provide linkage, at the enterprise architecture level, for terrorism information sharing capability across a broad spectrum of supporting communities and associated architectures. In particular, the *ISE EAF* helps to bridge the gap for information sharing across Federal civil systems, national security systems, and SLT and private sector architectures. While some of these architectures are individually isolated for supporting their communities' requirements, others have overlapping areas such as those information technology aspects associated with the DoD architecture that support both national security activities and non-national security activities (such as human resource, financial management, and other non-national security business areas for the department). Other overlapping areas include national assets such as the National Communications System (NCS) and the National Command and Coordination Capability (NCCC) having infrastructure and services provided by the private sector as well as from other Federal departments and agencies. Overall, the *ISE EAF* provides a common thread of information technology and their architectures for integration and interconnection across the spectrum of these Federal, SLT, foreign, and private sector partners supporting terrorism information sharing.

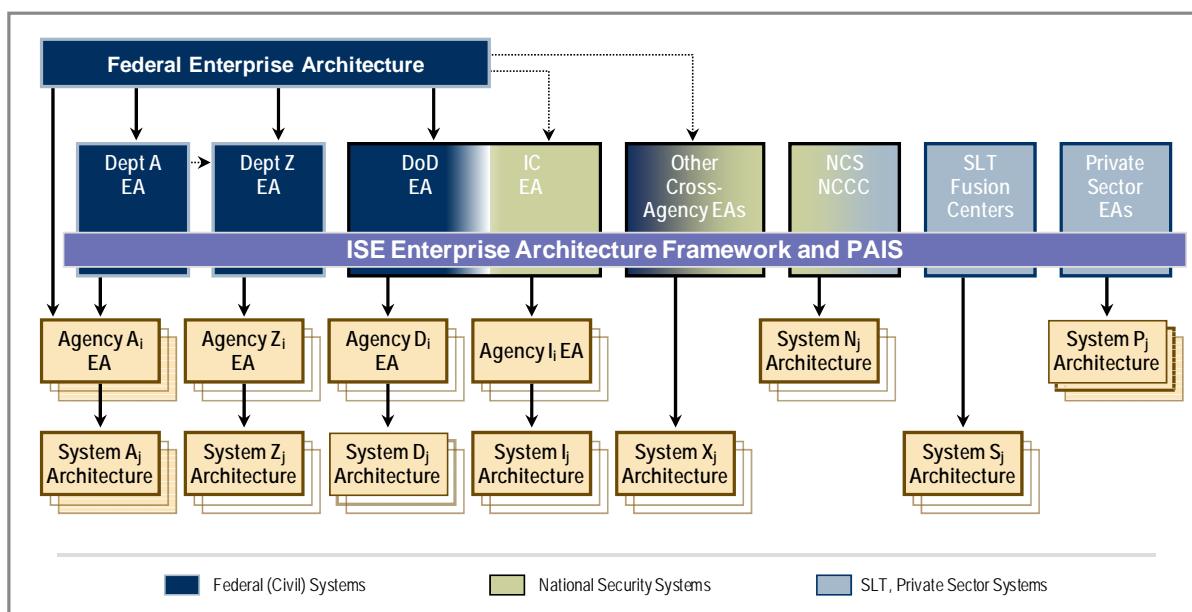


Figure 2-5. ISE EAF Bridging the Community Spectrum

2.3 ISE Implementation Agents Roles and Responsibilities

As the ISE Core and Transport services are developed, identified roles and responsibilities of ISE Implementation Agents will provide ISE participants the ability to post/share their information. An ISE Implementation Agent refers to an organization responsible for providing infrastructure and services in the Core Segment. The bulleted list below addresses the responsibilities for an ISE Implementation Agent within each *ISE EAF* Partition (Business, Application and Service, Data, and Technical) that must be performed to ensure integration within the ISE.

Business Partition:

- ISE Implementation Agents must be able to align, discover, search, and apply similar cross agency initiatives to support reuse, leverage, and other cost savings initiatives
- ISE Implementation Agents will analyze their business processes and establish the ISE common risk management governance process to balance the access of information with risks among all Federal, SLT, private sector and foreign partners
- ISE Implementation Agents shall identify and categorize candidate assets for sharing
- ISE Implementation Agents must ensure overall business process and implementation comply with ISE policies and guidance (at the highest level)
- ISE Implementation Agents shall deploy integrated and expanded plans of actions and milestones (POA&M) across all the various ISE participants
- ISE Implementation Agents must be mindful of opportunities to add capabilities or features to their service or core capabilities that further the general goals of the ISE
- ISE Implementation Agents will begin by preparing and executing a detailed performance evaluation plan and collecting and tracking performance metrics in parallel with the conduct of daily operations tasks such as maintenance of service, security monitoring, on-going privacy evaluation and protection, user/access management, etc.
- ISE Implementation Agents must balance investment priorities and strategies to support the ISE programmatic guidance and overall CPIC process

Application and Service Partition:

- ISE Implementation Agents must incorporate all ISE shared services for ISE Shared Spaces implementation and interconnection
- ISE Implementation Agents shall implement SOA by exposing critical services used with the ISE Shared Spaces concepts
- ISE Implementation Agents shall implement access authorization controls to protect shared data assets in accordance with the ISE Identity and Access Management Framework
- ISE Implementation Agents shall audit and monitor the security controls put in place to protect shared data on which assets are hosted
- ISE Implementation Agents shall implement a training program for the services they provide

Data Partition:

- ISE Implementation Agents must incorporate NIEM and U/CORE data exchange models as appropriate
- ISE Implementation Agents must adhere to CTISS Program standards and guidance

Technical Partition:

- ISE Implementation Agents must apply and align departments' and agencies' technical services to comply with those technical standards determined by the ISE
- ISE Implementation Agents must apply the RMF and principal IA and Core Transport standards within ISE Shared Spaces and EA/Information Sharing Segment Architecture (ISSA) efforts
- ISE Implementation Agents must provide ongoing monitoring and reporting of mission critical ISE systems
- ISE Implementation Agents must identify and make explicit for others to see the goals and objectives of each organization participating in the ISE
- ISE Implementation Agents must collaborate with the ISC to ensure that shareable assets are integrated into the ISE Core and Portal and internal agency transport can connect to the ISE Core Transport
- ISE Implementation Agents shall determine how data assets shall be shared (expose as a service is preferred)
- ISE Implementation Agents shall implement security controls to protect shared data assets

2.4 Coordination, Integration, and Re-use

OMB requires each organization to design and implement segment architectures. A segment architecture is defined as individual elements of the enterprise describing core mission areas and common or shared business services and enterprise services. Segment architectures drive decisions for a business case or group of business cases supporting a core mission area or common service. Within the ISE, SAR, AWN, and TWL are identified as three of the nine ISE core mission processes that ISE participants must incorporate or demonstrate progress toward within agency EA development. In each ISE participant's information sharing segment architecture (ISSA), common ISE attributes, services, standards, and other ISE tools will become apparent and allow for opportunities to re-use (fostering 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. As an example, many ISE participants have begun or completed developments of an ISSA based on mission needs. The Department of Justice (DOJ), Department Homeland Security (DHS),

Director of National Intelligence (DNI), Department of Defense (DoD), Health and Human Services (HHS), and the Environmental Protection Agency (EPA), for example, have developed or have started developing their EA or ISSAs using common ISE attributes. Another agency, for example the Department of Health and Human Services, intends to use the *ISE EAF* and *ISE PAIS* as models for implementation of a nationwide health information network. Likewise, the combined efforts of the Department of Defense, Global Maritime Domain Awareness (MDA) community, the Intelligence Community (IC), and the Department of Transportation (DOT) supporting both the military and commercial maritime environment are other examples of intended reuse and leveraging capabilities using ISE architectural products.

This page intentionally blank.

Chapter 3 – Policy and Governance, Drivers and Requirements

3.1 Policy and Governance

In accordance with the *Intelligence Reform and Terrorism Prevention Act*, the President will determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE. In consultation with the Information Sharing Council, the Program Manager, Information Sharing Environment (PM-ISE) is responsible for planning for, overseeing the implementation of, and managing the ISE to include monitoring and assessing progress. The PM-ISE is also responsible for assisting in “the development of policies, as appropriate, to foster the development and proper operation of the ISE”³³ Achieving the target state of the ISE will likely require changes in policies, a governance process suitable for a broad range of organizations and jurisdictions, and processes for establishing and maintaining trust among participants.

The existing ISE governance structure is depicted in Figure 3-1 below. Further explanation of ISE governance is outlined in Chapter 4 of the *ISE Implementation Plan*.

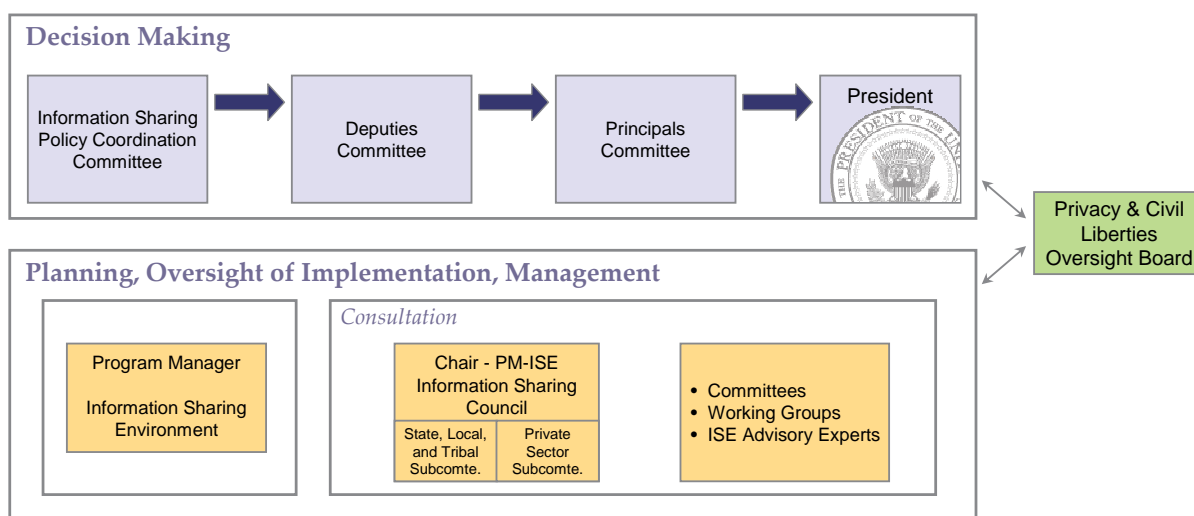


Figure 3-1. ISE Governance

3.1.1 Decision Making

Given the complexity of managing ISE implementation, it is critical to establish a governance structure by which activities are executed and appropriate mid-course corrections can be made. The ISE governance structure is based on the principle that ISE issues are resolved at the lowest organizational level wherever possible. In the event an unresolved scenario exists, an organized process is in place to elevate these issues for resolution, up to and including the Cabinet level and the President.

³³ 6 U.S.C. § 485(f)(2)(A)(ii).

As currently defined in the *Information Sharing Environment Implementation Plan*, Chapter 4, the ISE governance structure will consist of the following:

PM-ISE – Acts as the central agent to improve terrorism information sharing among ISE participants by working with them to remove barriers, facilitate change, and ensure that ISE implementation proceeds efficiently and effectively.

Information Sharing Council (ISC) – Chaired by the PM-ISE, advises the President and PM-ISE on developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE. Additionally, it works to ensure coordination among the Federal departments and agencies participating in the ISE and recommends means by which the ISE can be extended to allow interchange of information between the Federal Government and appropriate authorities of SLT governments.

ISC Subcommittees and Working Groups – Address and resolve important issues requiring specific expertise. Business process, architecture, and standards working groups and committees have already been established.

Privacy and Civil Liberties Oversight Board – Ensures and protects individual privacy and civil liberties as highlighted in the Privacy Act of 1974. Provides advice and counsel to the President or to any Executive department or agency senior leader on the development and implementation of policies related to efforts to protect the Nation from terrorism, to include development, adoption, and implementation of the ISE.

ISE policy and governance is described in more detail in the *Information Sharing Environment Implementation Plan*.

3.2 The Federal Transition Framework Catalog

OMB's *Federal Transition Framework (FTF) Catalog*, published at least annually, is a single information source for clear and consistent information describing government-wide information technology (IT) policy objectives and cross-agency IT initiatives using a simple, familiar, and organized structure. The development of agency target architectures that can be used by agencies to ensure that the Federal transition strategy is reflected in their own EA transition strategies and budget submissions will be facilitated by the *FTF Catalog*. Consistent with ISE goals, this action will assist agencies with aligning information and technology management programs with appropriate inter-agency initiatives. Furthermore, ISE participants will be able to use the *FTF Catalog* to discover similar cross-agency initiatives to make better informed decisions concerning agencies' IT investment to realize service improvements and potential cost saving opportunities.

In addition, the development of Federal agency target architectures supporting the ISE will be facilitated by the FTF. Using updates in the FTF with the business, data, and services outlined in the *ISE EAF*, agencies can ensure that the Federal Transition

Strategy is reflected in their own EA transition strategies and budget submissions. The goal is to assist ISE participants with alignment of IT programs with relevant cross-participant initiatives.

3.3 Drivers and Requirements

The *ISE Drivers and Requirements Document*³⁴ describes the authoritative mandates (e.g., Executive Orders, Public Laws) that direct the ISE. These ISE drivers and requirements are strategic in nature and establish direction to bring about ISE specific results.

The Presidential Guidelines direct that “the ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively “resources”) used for the sharing and integration of and access to terrorism information, and shall leverage those resources to the maximum extent practicable, with the objective of establishing a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information.”³⁵ This Presidential direction resulted in the PM-ISE’s developing the *ISE EAF* to further define the ISE specific drivers and requirements. The ISE and supporting Common Terrorism Information Sharing Standards (CTISS) Program will facilitate information sharing practices, reduce barriers to sharing, and institutionalize sharing by providing a new construct for planning, installing, and operating nationwide information resources within the fabric of the ISE.

More specific than drivers, ISE requirements are defined as the specific capabilities necessary for establishing the usability of the ISE and focus on meeting the goals of the ISE. Each ISE requirement is traceable to an authoritative source that is posted at www.ise.gov. However, some source documents are not specifically focused on the ISE and may contain certain exemptions. For example, the Federal Information Security Management Act (FISMA) is one source document that pertains to security of information systems of Federal departments and agencies, but it is not directly applicable to national security, State, local, and tribal information systems.³⁶ Such requirements are not mandates but are recommended requirements so that as the ISE evolves organizations (e.g., State, local, tribal) will be able to connect to the ISE.

³⁴ ISE Drivers and Requirements Document – www.ise.gov.

³⁵ *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements In Support of the Information Sharing Environment* (2005), Section (1).

³⁶ See 44 U.S.C. § 3543(b).

This page intentionally blank.

Chapter 4 – Information Security and Assurance

4.1 Introduction

The Information Security and Assurance chapter identifies the particular standards, technologies, and frameworks that will support a secure implementation of the ISE, focusing on the “TO-BE” information security architecture. This Chapter includes five detailed sections: an Information Security and Assurance Overview, Policy and Governance, Risk Management, an ISE Information Security and Assurance Model, and the Identity and Access Management Framework.

4.2 Information Security and Assurance Overview

Information security³⁷ is the protection of information and information system(s) from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Information security covers all aspects of information systems (people, processes, and technology) and all actions necessary (protect, detect, and respond) to adequately mitigate negative impacts to the organization, individuals, other organizations, or the Nation resulting from use of the information systems. Information security includes use of management and operational and technical safeguards and countermeasures including access control; identification and authentication; auditing and accountability; system and communications protection; incident response; contingency planning; system and information integrity; physical and environmental protection; personnel security; risk assessment; certification, accreditation, and security assessment; configuration management; awareness and training; maintenance; systems and services acquisition; planning; and media protection.

Effective information security and assurance within the ISE requires consistent policies and standards, effective governance, a common risk management framework, trustworthiness of information system(s), and appropriate training.

4.3 Policy and Governance

The artifacts of governance arrangements and activities are policies, rules, guidelines, recommendations for changing laws, and decision making that affects all aspects of the ISE. A more detailed discussion of governance and risk management is outside the scope of this chapter, but a brief discussion is included here because of its crucial impact on the IA approach for the ISE. Further information on ISE governance and risk management processes can be found in the *ISE Implementation Plan* and the *Information Sharing Environment PAIS*.

³⁷ Information security (or information system(s) security) is the term most widely used in the public and private sectors with the equivalent term within the national security community being “Information Assurance” (IA). Within this document the term “information security and assurance” is used, understood to be essentially equivalent to IA as defined in Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, Revised June 2006.

IA is a key capability in the ISE to support business process-driven exchanges, such as Suspicious Activity Reporting (SAR), where data elements may include those of a sensitive nature (such as privacy protected information or intelligence sources and methods) requiring strong protection.

A basic risk management approach should identify the following:

- Threats, vulnerabilities, and impacts (which combined constitute an initial level of risk)
- Measures to mitigate risk
- Determination of residual risk (remaining level of risk after IA controls are applied)
- Determining whether residual risk is acceptable or additional protective measures are required

Progressing through this process ensures a known and acceptable level of risk is identified so that a risk-based decision is made by the appropriate governance bodies and accrediting authorities for the ISE. This risk-based decision shall be commensurate with mission requirements focused primarily on the “responsibility to provide” rather than to simply share or protect information. There are numerous risk management models in use within the Federal Government and across all of the ISE communities.

Determination of an appropriate risk management model will occur as governance bodies and decision making processes are established for the ISE.

4.4 Risk Management

The ISE manages the risk associated with the sharing of information among ISE participants by employing a *Risk Management Framework (RMF)*. The RMF provides ISE participants with a disciplined, structured, flexible, extensible, and repeatable process for achieving agreed-upon degrees of trustworthiness for ISE information system(s) (see Section 2.1.3 in the *ISE PAIS, Version 1.0* for the definition of information system(s) trustworthiness). The RMF, which operates within the context of the architecture development life cycle, can be applied to both new and legacy information system(s) that are part of the ISE. The RMF incorporates well-defined information security standards and guidelines to facilitate the sharing of information and to demonstrate compliance with the ISE information security requirements. The plug-and-play nature of the RMF allows other entities (e.g., SLT governments, and the private sector) to use the framework either with National Institute of Standards and Technology (NIST) and/or Committee on National Security Systems (CNSS) security standards and guidelines. This may also include equivalent national or international standards approved by the appropriate ISE information security governance function(s) using standard criteria and categories.

The RMF depicted here graphically and further defined in the *ISE PAIS*, illustrates the specific activities in the ISE RMF based on the National Institute of Standards and Technology (NIST)³⁸ security standards and guidelines associated with each activity and consisting of the following steps:

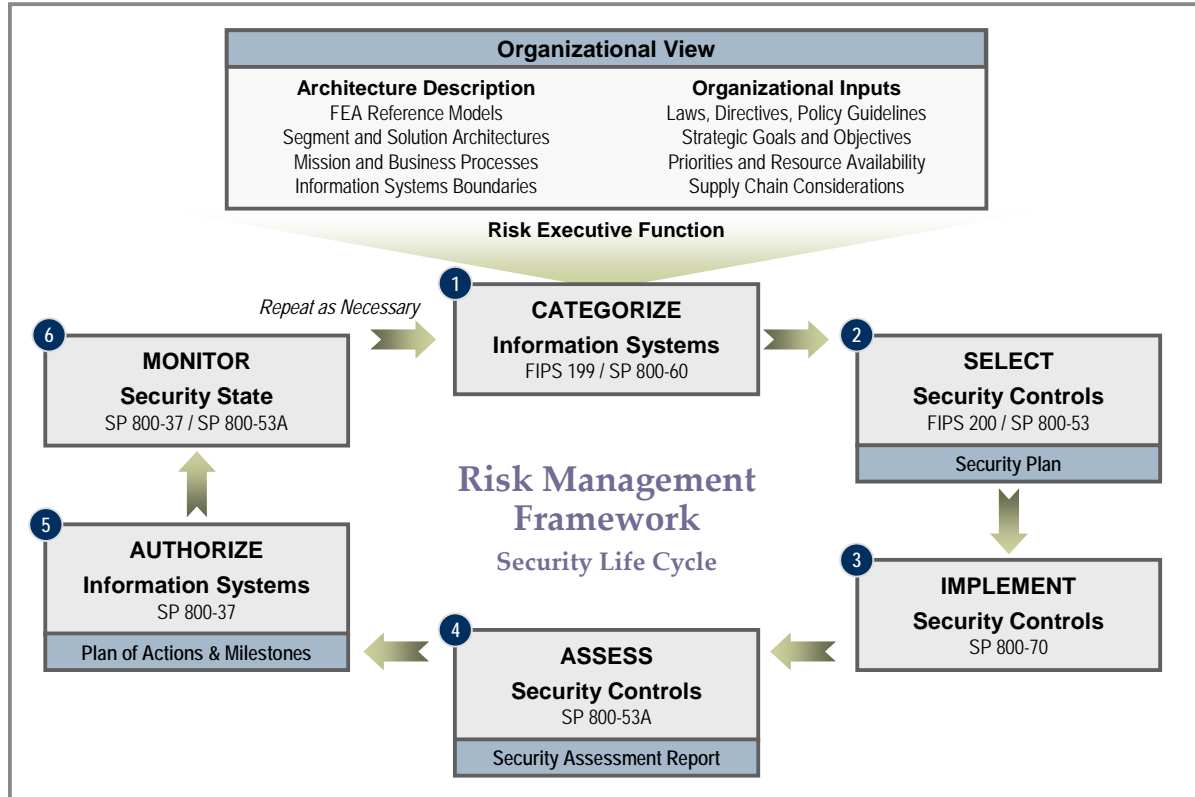


Figure 4-1. The ISE Risk Management Framework

4.5 ISE Information Security and Assurance Model

Information security and assurance for the ISE relies on overarching governance and risk management processes based on an IA model encompassing six IA categories: Information Sharing, Integrity/Non-Repudiation, Mission Management, ISE Defense, Availability, and Confidentiality. These categories are cross-referenced to the four *ISE EAF* partitions (Business, Data, Application and Service, and Technical). Finally, this is all threaded together as IA Controls and Countermeasures commonly grouped into three focus areas: People and Training; Policy and Practices (or Operations); and Technology.

The next section provides the perspective of the IA model in relation to the four partitions

³⁸ The Risk Management Framework is available at the National Institute Standard and Technology (NIST) website at <http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf>.

4.5.1 Four Partitions of the ISE EAF Architect's View in Relation to IA Capabilities

The ISE IA model identifies those Information Security and Assurance implications within each of the four partitions of the ISE EAF Architect's view. Figure 4-2, below depicts a graphic representation of the IA implication on all four of the ISE EAF partitions. The graphic further depicts the method used to analyze those IA implications and needs in each of these partition areas. The IA three-dimensional model is shown in the center because of the relationship to the other partitions. The next section describes the ISE IA Model, and explains the IA capabilities and controls with respect to the ISE.

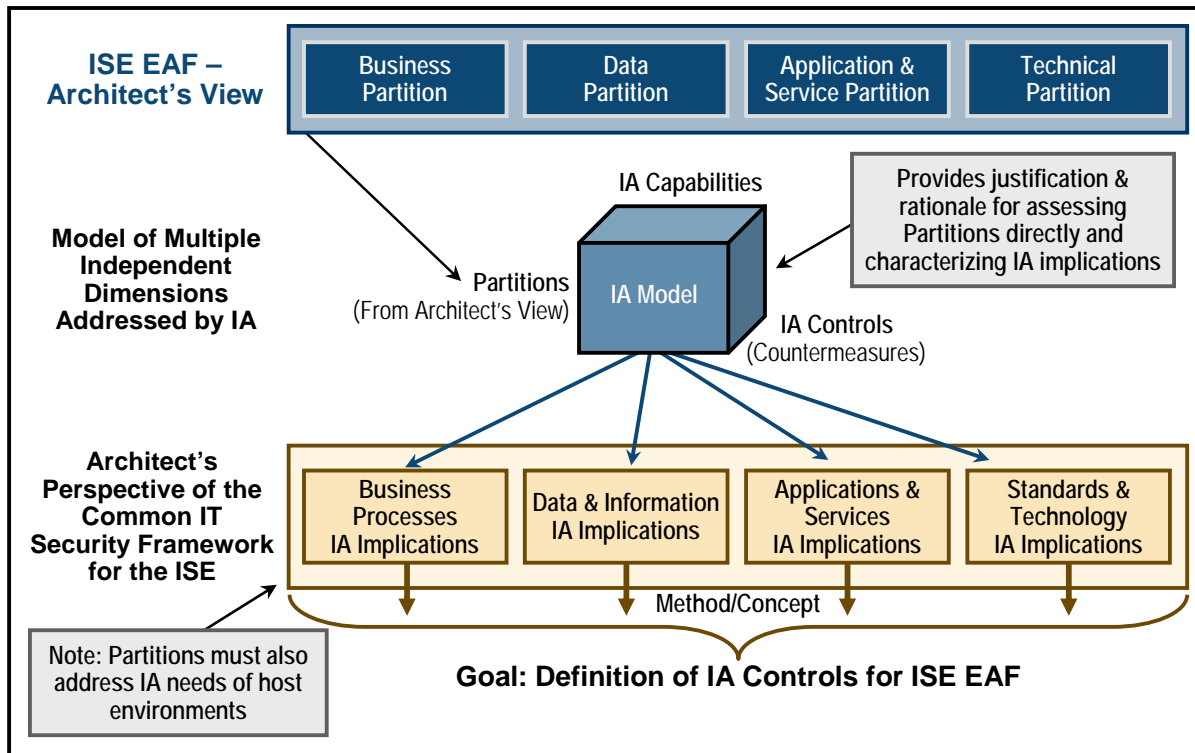


Figure 4-2. IA Relative to Four Partitions of the ISE Architect's View

4.5.2 ISE IA Model

The IA Model for the ISE incorporates all three critical dimensions of IA Categories, ISE EAF Architect's View Partitions, and IA Controls. Each dimension can be divided into principal elements, the intersection of which will identify IA controls to apply to ISE partitions in order to support capabilities in the IA categories. This ISE IA Model matrix is illustrated in Figure 4-3.³⁹ Descriptions of the elements of the IA dimensions follow.

³⁹ Office of the PM-ISE, ISE Information Assurance Model and Common IT Security Framework, Draft Version 0.6 (August 2007).

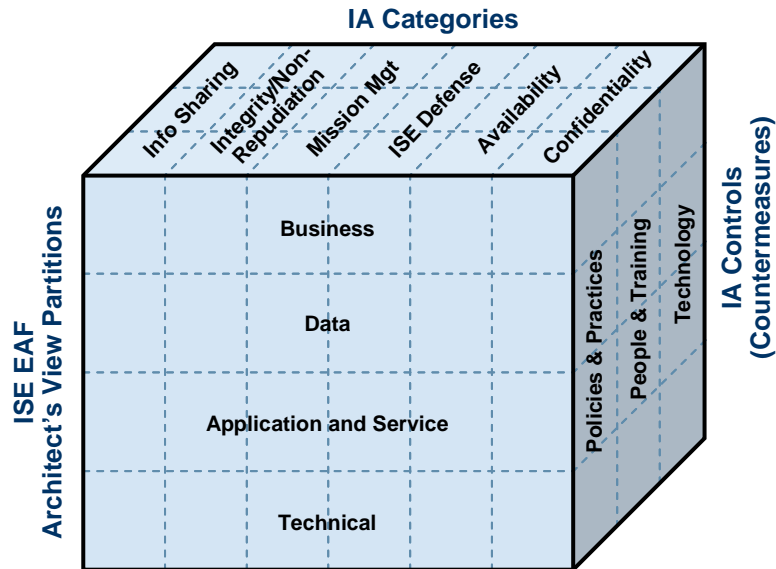


Figure 4-3. IA Model

The focus of the IA Model is to define it such that it

- Encompasses the IA Categories: Assured Information Sharing, Assured Integrity/Non-Repudiation, Assured Mission Management, Assured ISE Defense, Assured Availability, and Assured Confidentiality
- Demonstrates relationships to the four partitions of the *ISE EAF* Architect's View
- Includes categories of IA controls that address policies and practices, people and training, and technology

The model comprehensively includes all major elements providing justification and rationale for assessing partitions directly with the respective IA categories of capabilities.

4.5.3 Information Assurance Categories⁴⁰

Table 4-1 lists the categories of information assurance (IA) standards and technologies applicable to the ISE. The descriptions for each of these categories provide a brief understanding of what each category entails. Instructions and guidelines regarding the adoption and implementation of specific technologies and standards will be forthcoming in CTISS issuances.

Security mechanisms, tools, practices, policies, management processes, ISE Core Services, and features of service-based architecture combine to provide information

⁴⁰ Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Ibid., Section 5.3.1. See also, Global Information Grid (GIG), Information Assurance (IA) Initial Capabilities Document (ICD), National Security Agency (March 2006).

assurance in each of these categories. The following sections describe several security approaches used in each IA category.

Table 4-1. IA Categories

IA Category	Description
Assured Information Sharing	This is the most critical IA capability for the ISE because the primary function of the ISE is to share information. The challenge will be to provide the ability to securely and dynamically share information across security domains while simultaneously ensuring the security and privacy appropriate to that information.
Assured Integrity/Non-Repudiation	The ISE must assure the integrity/non-repudiation of data, at rest, during processing, in transit, and across systems during normal, degraded, disconnected operating modes, and in low bandwidth environments. This requirement refers primarily to measures that ensure data is not inadvertently or maliciously modified.
Assured Mission Management	The ISE must provide the ability to assign, prioritize, modify, and revoke user and system roles, access rights, and Community of Interest (COI) membership.
Assured ISE Defense	The ISE, its information, systems, and infrastructure must be defended against a variety of cyber threats. Defensive capabilities will include physical security measures, personnel security measures, configuration control, intrusion detection, virus and mal-ware control, monitoring, auditing, disaster recovery, and continuity of operations planning (COOP).
Assured Availability	The ISE must assure a level of availability consistent with stated requirements.
Assured Confidentiality	The ISE must not reveal information to unauthorized users. This will be accomplished by first ensuring that only authorized users have access to the ISE, and, second, that even if an unauthorized user does get access, the user cannot leverage that access to view ISE information.

4.5.3.1 Assured Information Sharing

Security Domains: The ISE has three security domains:

- Top Secret/Sensitive Compartmented Information
- Secret/Collateral
- Controlled Unclassified Information (CUI)/Sensitive But Unclassified

All users with access to a specific security domain and ISE relevant information must have a personal clearance level equivalent to the level of security in that domain. However, all users within a specific security domain may not have access to all information available in that domain. Role-based access controls may limit access to specified information based on the user's identity and/or role. Agencies, fusion centers, and the NCTC should share information that derives from or resides in all three

domains. However, State and major urban area fusion centers will primarily have access to the Secret/Collateral and CUI/SBU domains.

Cross-Domain Solutions: The ISE vision to make terrorism information available, accessible, and usable by all ISE participants and centers is complicated because of current technologies that do not enable efficient exchange of information from one security domain to another. This inability causes proliferation of assets ranging from multiple desktop machines for end-users to multiple server racks and associated networking equipment in back-office server rooms. This trend will continue for the foreseeable future.

There still exists a requirement in the ISE to pass information among security domains where terrorism information in one domain may be fused with information in a domain of a different security and classification level. In practice, this requirement dictates that terrorism information must pass both ways, i.e., from a lower-classification domain to a higher-classification domain and from a higher-classification domain to a lower-classification domain. This does not imply the intent to transmit unencrypted, classified information over an unclassified network, nor does it imply transmitting information classified at a higher level to a lower classification domain. Likewise, it does not imply that suspect information, possibly containing malicious code or viruses, will be allowed to corrupt protected networks.

In the near term, cross-domain exchange of information should be the responsibility of ISE participants. Information exchanged from one security domain to another should occur internally; therefore placing responsibility on the ISE participant. These near-term solutions for cross-domain information exchange will likely be in the form of policies, practices, and procedures for passing properly inspected and properly classified material from one security domain to another.

The long-term, cross-domain exchange of information will be conducted through automated processes offered as ISE Core Services. An evolved ISE should provide core services for sanitizing and inspecting information. These automated services will depend on proper security labeling of information and strict rules regarding distribution and declassification of information. The algorithms, taxonomy, and rules for cross-domain solutions can be found at the Unified Cross Domain Management Office (UCDMO).⁴¹

Each ISE security domain should be connected by one or more trusted, cross-domain solutions. When used, these solutions exist within an ISE participant and enable movement of data across security domains. They allow information to flow between security domains, adhering to the policies and constraints that protect classified information. Trusted cross-domain solutions require all information be appropriately

⁴¹ The UCDMO published a Cross Domain Inventory list version 2.2. Electronic copies of this and other documents pertaining to cross domain solutions can be found at www.ucdmo.gov.

tagged with trusted security labels. Trusted cross-domain solutions should support assured information sharing that transcends multiple security domains.

CTISS Tearline Standards: The CTISS will designate functional standards for tearlines leveraging standards from national security organizations. Tearline standards define practices and technologies for segregating data into separate parts corresponding to different security domains. This segregation facilitates computer-assisted and automated processes for passing information between domains.

4.5.3.2 Assured Integrity and Non-Repudiation

Authentication: The ISE must take measures to ensure only authorized users can access ISE resources. Exclusively allowing authorized users to access the data in the ISE will help to assure that data is not subject to unauthorized modification. Authentication is further addressed in section 4.6 (Identity and Access Management Framework).

Strong Authentication: Access to all ISE resources should be protected by strong authentication. Each potential user will be required to present a logon name (something that only that user possesses) and a password, personal identification number, or pass phrase (something that only that user knows) and token or biometric data (second authentication factor). All ISE accounts should be attributed to a specific individual, disallowing un-attributed accounts such as ADMIN or GUEST. Strong authentication also contributes to integrity and non-repudiation by allowing the ISE to properly audit actions by individual accounts.

Public Key Infrastructure (PKI): The ISE should accommodate one or more PKIs as PKI is used within communities such as Defense. It is desirable that there be one PKI supported across all three ISE security domains; however, if this is not feasible, there will be at least one PKI across each of the three security domains. The PKI will provide identity validation through a Certificate Authority, certificates for strong authentication, certificates for digital signature, and certificates for public/private (asymmetric) encryption. The PKI contributes to non-repudiation and integrity through digital signature and is further addressed in section 4.6 (Identity and Access Management Framework).

4.5.3.3 Assured Mission Management

Network Management Function: The ISE should be managed via a network management function whose responsibility will be establishing, monitoring, and enforcing service level agreements with public and private telecommunication service providers for assured availability; planning, exercising, and implementing disaster recovery and continuity of operations for assured availability; real-time ISE defense; ISE operations; and assured mission management of the ISE.

4.5.3.4 Assured ISE Defense

Trusted Infrastructure: Each security domain will employ trusted infrastructure. The TS/SCI and Secret/Collateral domains will apply security controls consistent with Director of Central Intelligence Directive (DCID) 6/3 and DoD Instruction (DoDI) 8500.2. The CUI/SBU domain will employ security controls specified in the *Federal Enterprise Architecture Security and Privacy Profile* and *Recommended Security Controls for Federal Information Systems* as well as Federal Information Processing Standards (FIPS) and NIST Special Publications, to include *FIPS Publication 199 (Standards for Security Categorization of Federal Information and Information Systems)*, *FIPS Publication 200 (Minimum Security Requirements for Federal Information and Information Systems)*, and *Special Publication 800-53 (Recommended Security Controls for Federal Information Systems)*.

For certification and accreditation, the CUI/SBU domain shall adhere to guidance provided in NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004. The Secret/Collateral and TS/SCI domains will be certified and accredited using DoD 8510.bb, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) or equivalent.

Authorization: The ISE must take measures to ensure that authorized users can perform only those functions permitted by their identity and role. A user must be authenticated to the ISE, and each action that an authenticated user attempts to perform must be compared to the list of permitted actions for that user and role, i.e., the actions must be authorized. Assuring that only authorized users are permitted to execute authorized actions aids in defending the ISE. This concept is further addressed within section 4.6 (Identity and Access Management Framework).

Public Key Infrastructure: The PKI contributes to defense of the ISE through strong authentication.

Network Management Function: Network management personnel will be responsible for real-time defense of the ISE.

4.5.3.5 Assured Availability

High-Availability Design: The ISE will be designed for high availability consistent with the requirement for availability and the trade-offs between availability, usability, and cost. High-availability design may include redundancy of capabilities and facilities, appropriate levels of information assurance to avoid or mitigate attack, appropriate design for graceful degradation of capabilities, provision and maintenance of accessibility to required information in any environment (stable to austere), and provision of flexible allocation of resources based on demand and mission needs.

Network Management Function: The ISE should be managed on a real-time, on-going basis for high availability. Network management personnel should be responsible for

management of the ISE for high availability. These activities will include implementing patch management; monitoring the status of ISE assets; and detecting, diagnosing, responding, and correcting problems.

4.5.3.6 Assured Confidentiality and Privacy

Encrypted Communications: All communications leaving an enclave at any security domain level should be encrypted. This encryption ensures that all communications between enclaves are encrypted, assuring confidentiality of messages transmitted across the ISE.

Public Key Infrastructure: The PKI contributes to confidentiality through encryption.

Privacy Enhancing Technology: Applicable privacy laws and regulations should be assured via technologies such as permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.⁴²

For example, with the SAR business process, information assurance considerations include those needed to purge SAR records when required and those affecting Privacy Impact Assessments (PIA).

4.6 Identity and Access Management (IdAM) Framework

Based on the requirements set forth in the National Strategy for Information Sharing, in order for terrorism information sharing to take place, a common and collaborative Identity and Access Management (IdAM) Framework is required. This IdAM Framework will link disparate IdAM technologies and implementations to assure appropriate authorization and access in order for ISE participants to share terrorism information.

4.6.1 The ISE IdAM Framework

The ISE IdAM Framework incorporates the law enforcement, defense, homeland security, intelligence, and foreign affairs communities' IdAM efforts. This Framework includes all Federal, and SLT government agencies that agree to abide by a set of technical and functional standards, policies, business rules, and agreements that serve to make identity and information access portable across the ISE. The ISE IdAM Framework includes Identity Providers, Service Providers, the Assurance Level Certification process, the Brokered Identity Enforcement process, the Attribute Based Access policy enforcement process, and program management. The Identity Provider provides local authentication services. The Service Provider provides access to services and applications that facilitate the sharing of terrorism information to all ISE participants as appropriate given information security considerations. The Assurance Level

⁴² Office of the 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* (December 2006), <http://www.ise.gov/docs/PrivacyGuideline.pdf>.

Certification Process provides guidance on how an Identity Provider or Service Provider is certified at an e-authentication assurance level. The Brokered Identity Enforcement Process provides guidance and polices for establishing the brokered trust relationships. The Attribute Based Access policy enforcement process provides guidance and policies for establishing an attribute based access control policy for the ISE. Finally, the program management will oversee the development and implementation of the technical, policy, and business interoperability standards, agreements, and this Framework.

The ISE IdAM Framework shall incorporate available voluntary consensus standards that are used to provide interoperability of the IdAM services to the ISE. The ISE IdAM Framework will support the coexistence of multiple federated identity schemes and provide an IdAM Framework for the management of brokered trust between those schemes. Furthermore, the ISE IdAM Framework provides ISE participants an opportunity to contribute to the collection, development, and implementation of the policies and standards it encompasses. Implementation of these policies and standards will provide each ISE participant with a capability to quickly, efficiently, and securely access data or systems in other ISE participants' networks and enclaves. This standard provides the means for information sharing to take place and the associated capabilities to be developed. It will ensure ISE participants have access to the information they need when they need it while limiting the effect on legacy systems and networks by incorporating existing IdAM technologies.

The ISE IdAM Framework requires a commitment from each ISE participant to abide by the technical and functional standards, policies, business rules, and agreements acknowledged, developed, and implemented. The success of the ISE IdAM Framework is dependent on all ISE participants working together in concert to ensure enhanced information sharing while protecting the security of data and systems.

4.6.2 IdAM Functionality

This section provides information on IdAM functionalities and interoperability requirements to allow for information sharing among ISE participants.

4.6.2.1 Credential Adjudication Mechanisms

Credential adjudication mechanisms are required in the ISE in order to negotiate the various identity credentials presented by ISE participants for access to services. In turn, the Service Providers present these same credentials to the adjudication mechanism for identity assurance validation. These mechanisms will be based on a brokered trust model that transcends the various ISE participants and are coordinated with the Federal Identity Credentials Committee under the Federal CIO Council. Without this brokered trust, terrorism information sharing cannot take place.

Credentialing technologies, defined by HSPD-12 and FIPS 200-1, are among those recommended for use by ISE participants. These technologies will be included as acceptable standards for the ISE IdAM Framework. Therefore, the brokered trust model

must allow for, accept, and adjudicate these credentials presented by ISE participants for access to Service Provider services in order to provide identity assurance for the Service Provider.

4.6.2.2 Attribute-Based Authorization Mechanisms

Attribute-based authorization technology will be required in the ISE. In order for shared terrorism information to be accessed by the appropriate authorized personnel, attributes assigned to them in conjunction with their identity credentials will facilitate the access.

A set of attributes may include

Name: [First, Middle, Last]

Unique Identification Number: [a hash taken from this set of minimum attributes + Random Number]

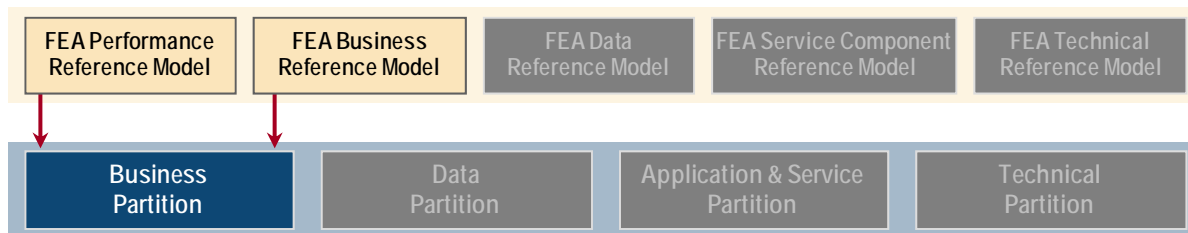
Basic Role: [Law Enforcement, Defense, Homeland Security, Intelligence, Foreign Affairs]

4.6.2.3 Biometrics

The ISE IdAM Framework guidance will use national level biometrics standards for assuring personal identity and physical presence while accessing shared terrorism data.⁴³

⁴³ For more information regarding the national level biometrics standards visit <http://www.biometrics.gov/NSTC/Publications.aspx>.

Chapter 5 – Business Partition



5.1 Introduction

The *ISE EAF* Business Partition provides an organized, structured view into existing business policies, processes, and practices and is the cornerstone to ensure alignment with overarching ISE mission and strategic goals. The *ISE EAF* Business Partition uses the FEA PRM and FEA BRM as input models to ensure ISE participants' EAs and segment architecture developments are driven by core mission/business goals and strategic outcomes. This partition sets the overarching enterprise strategic drivers and business priorities and outcomes that enable executable agency-wide EAs and ISSA development. These overarching ISE performance goals and objectives allow ISE participants to create a culture of sharing, reduce barriers to sharing, improve sharing practices, and institutionalize sharing within and across the Federal Government and with SLT government partners. Using established ISE performance goals, ISE participants will be able to perform a comprehensive analysis of their "TO-BE" business and information requirements to identify ISE mission modernization opportunities based upon the enterprise and strategic business requirements.

5.2 Performance Management Overview

Performance management is the widely accepted management process of developing a results-oriented approach to monitor progress against goals, enhance mission outcomes, promote accountability, and strategically allocate resources based on performance.⁴⁴ Within the FEA's federated approach, the PRM dictates the methodology and means to manage IT performance across the entire IT life cycle.⁴⁵ As it relates to the national capability to share information, performance management is used to optimize the relationships between people, processes, and technology to achieve ISE mission outcomes.

⁴⁴ See Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62, § 3 (codified as 5 U.S.C. § 306; requiring agencies to adopt mission statements, strategic plans, and measures of both program outputs and outcomes) see also OMB's Program Assessment Rating Tool (PART) (OMB's FY05 PART guidance provides "PART is a vehicle for achieving the goals of GPRA.").

⁴⁵ See OMB, FY07 Budget Formulation – FEA Consolidated Reference Model Document, May 2005, p.4; OMB – The Federal Enterprise Architecture Program Management Office, How to Use the Performance Reference Model, Version 1.0, and September 2003.

The PRM is a framework that “allows agencies to better manage the business of government at a strategic level, by providing a means for using an agency’s EA to measure the success of IT investments and their impact on strategic outcomes.”⁴⁶ Since the *ISE EAF* is a “framework,” rather than a standalone EA, the purpose of this section is to guide agencies, in accordance with the PRM, in their efforts to manage their particular IT resources. To accomplish this, the *ISE EAF* provides ISE participants a common vision and set of overarching principles to align their performance management efforts and establish a clear “line of sight” to desired results for the ISE. For example, ISE participants will use CTISS artifacts while developing agency level EAs and Segment Architectures aligned to *ISE EAF* principles to align with ISE shared mission processes and performance outcomes.

5.3 FEA and ISE EAF

5.3.1 The FEA BRM

The BRM is the second layer of the Federal Enterprise Architecture and is the main viewpoint for the analysis of services components, data and technology. The subsequent reference models (i.e., Service Component Reference Model (SRM), Data Reference Model (DRM), and Technical Reference Model (TRM) to be covered in later chapters) are derived from mission business processes within the BRM. Business-led architectures that support performance outcomes are more successful in meeting strategic goals, reacting to changing mission needs, and serving citizens’ expectations, and, overall, drive accurate investments to reach key decisions rather than technology or budget-driven architectures. Business-led architectures will continue to motivate ISE participants to be more proactive vice reactive by building from established business needs and requirements based on targeted outcomes. Based on this approach, ISE participants are encouraged to work closely with all relevant stakeholders to include business/mission owners and security, segment and solutions architects, as appropriate, to define and design a suitable architecture. This document includes the mission processes for SAR, AWN, and TWL. Continued development for all the ISE mission processes detailed in Section 5.4 is key to developing the complete *ISE EAF* Business Partition.

5.4 ISE Business Process Framework

The ISE Business Process Framework, illustrated in Figure 5-1, shows the three types of ISE business processes and links the ISE Mission Drivers to the ISE Mission Processes.

⁴⁶ OMB, FY07 Budget Formulation – FEA Consolidated Reference Model Document, May 2005, pp.4-5 (The PRM focuses on three main objectives: (1) Help produce enhanced performance information to improve strategic and daily decision making; (2) Improve the alignment and better articulate the contribution of inputs to outputs, thereby creating a clear “line of sight” to desired results; and (3) Identify performance improvement opportunities that span traditional organizational structures and boundaries).

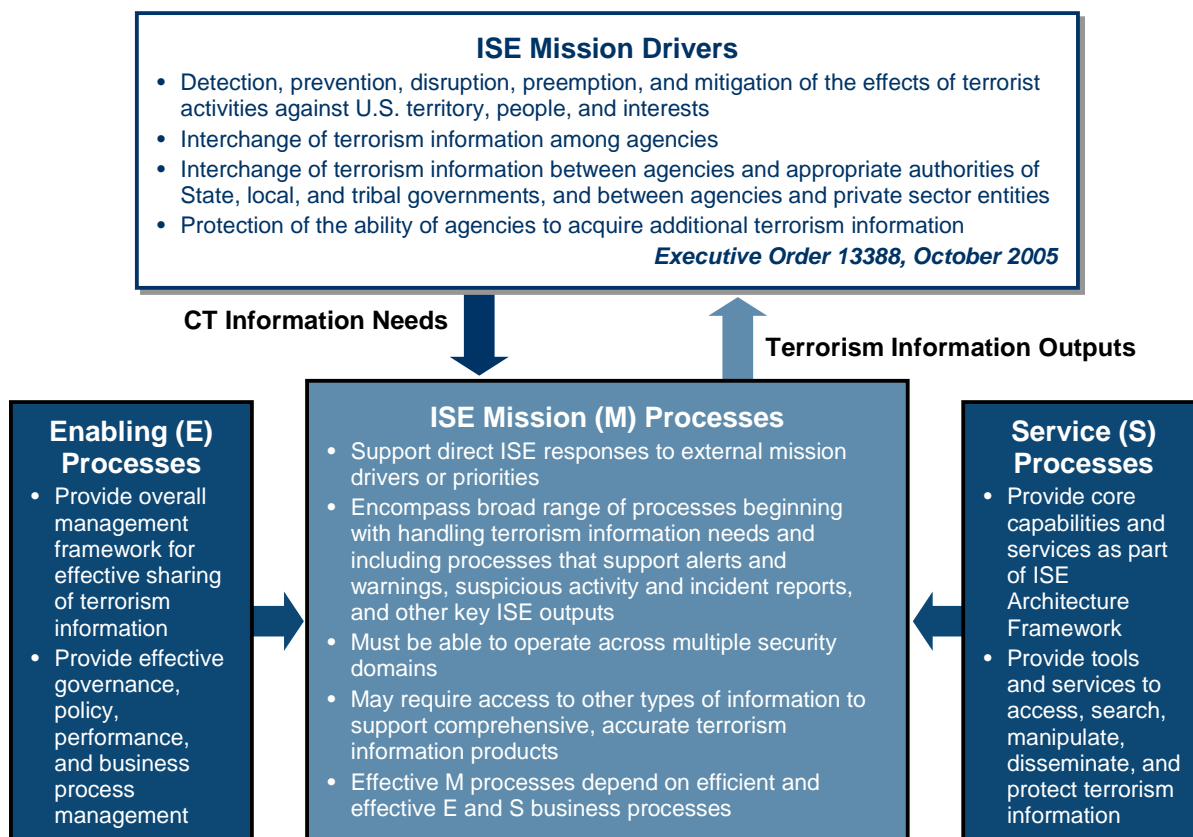


Figure 5-1. ISE Business Process Framework

Business processes address the Office of the PM-ISE requirements and ISE participant requirements. To accomplish this, the ISE Business Processes are grouped into three general categories:

- **ISE Mission Processes:** A key factor in the success of the *ISE EAF* is the alignment of the architecture to the mission requirements, which enable the participants in the ISE to achieve their mission objectives. This *ISE EAF* version specifically focuses on the SAR, AWN, and Identification and Screening (TWL Component) mission process areas, recognizing that similar efforts are underway for the remaining ISE mission processes. Defining these processes helps ISE architects identify and understand the specific mission needs and thereby derive the business requirements that ISE development will ultimately address. These processes represent the actual use of information via the ISE to support counterterrorism missions. ISE Mission Processes include Information Requirements and Roles, Analysis, Operations, Policy and Decision Making, Response, and Protection

- **ISE Enabling Processes:** The PM-ISE uses enabling business processes to establish and manage the ISE. These processes are the programmatic activities identified in the *ISE Implementation Plan* for which the PM-ISE is responsible.
- **ISE Service Processes:** Service processes are those recurring supportive activities that directly affect the mission processes of the various ISE participants. These are services that provide access, collaboration, discovery and search, manipulation and storage, directory services, dissemination capability, and information protection.

ISE Core Services depicted below in Figure 5-2 enable the execution of ISE business processes across information sharing systems in the ISE. Detailed descriptions of the ISE Core Transport, ISE Core Services, and ISE Portal Services are found in Chapter 6.

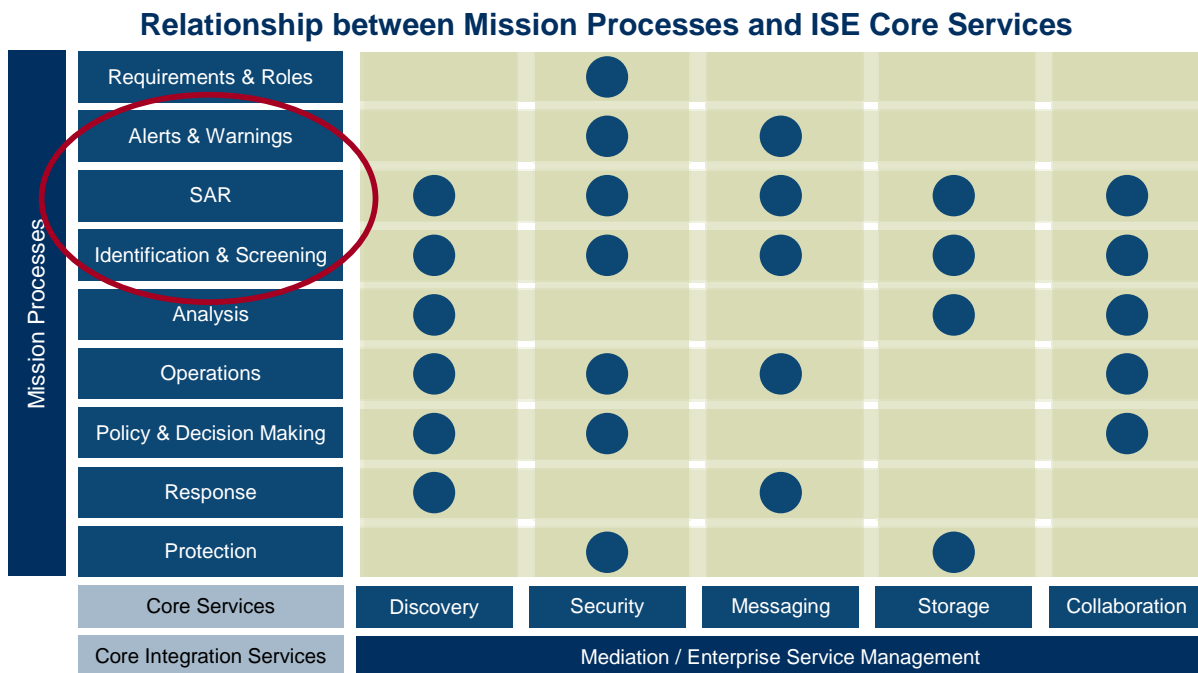


Figure 5-2. Relationship Mapping of Mission Processes and ISE Core Services

5.4.1 Target Business Processes

For the target *ISE EAF* Business Partition, additional detail will be added to the baseline partition incorporating reengineered ISE business processes. The target partition will show the business process information flows using the organizations and capabilities described in the *ISE EAF*. The identified business process information flows will then be used to determine the required data exchanges for each type of information flow.

ISE targeted mission business processes have been identified. By documenting ISE mission business processes and information flows, ISE participants are able to determine appropriate information based upon mission requirements.

5.4.2 The ISE Business Partition

The *ISE EAF* Business Partition lays the foundation for resolving key decisions to determine if current business and information efforts prohibit or promote progress within the ISE. Modifying current business and information processes, practices, and policies is essential to allow for enhanced exchange/sharing of ISE related information to provide interoperability and portability of data from other ISE mission processes (such as Suspicious Activity Reporting (SAR), Identification and Screening (TWL component), and Alerts, Warnings and Notifications (AWN)) across counter-terrorism communities. As an example to show linkage and interrelationship within these three mission processes, an ISE goal is to use the ISE-SAR information as an input that could lead to a closer analysis of potential terrorist information. This new discovery (i.e., critical information) would later be shared with other terrorist information repositories (e.g., NCTC/TIDE or the Terrorist Screening Database {TSDB}) following CTISS standards to match identities and show patterns or trends in behaviors to alert, warn, or notify of potential terrorist plots. The 9/11 Commission Report repeatedly documents crucial pre-9/11 information kept in disparate databases and posits that if information had been combined and analyzed, the Nation would have been better able to thwart or stop the attacks.⁴⁷ Using proven business and information architecture practices and methodologies provides an ability to link trends in behavior and activity to prevent future attacks and enables ISE participants to quickly execute decisions in a timely manner.

Transitioning from the Business Partition to the Application and Service, Data and then Technical partitions, ISE participants will begin to understand the adjustments required within current business and information environments (usual day-to-day operations) in order to achieve ISE target performance driven architecture.

The *ISE EAF* Business Partition describes a hierarchical list of the business areas, lines of business, sub-functions, and processes within the scope of the ISE that are taken from the Federal Enterprise Architecture BRM. The BRM sub-function 262, *Information Sharing*, is described as relating to any method or function, for a given business area, facilitating data being received in a usable medium by one or more departments or agencies as provided by a separate department or agency or other entity; and data being provided, disseminated, or otherwise made available or accessible by one department or agency for use by one or more separate departments or agencies, or other entities, as appropriate.⁴⁸ Figure 5-3 represents where this sub-function is placed within the FEA BRM.

⁴⁷ National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, (U.S. Government Printing Office: Washington, DC, 2004), 416, 417.

⁴⁸ OMB, FEA Consolidated Reference Model Document, Version 2.2 (OMB: Washington, DC, 2007), 45.

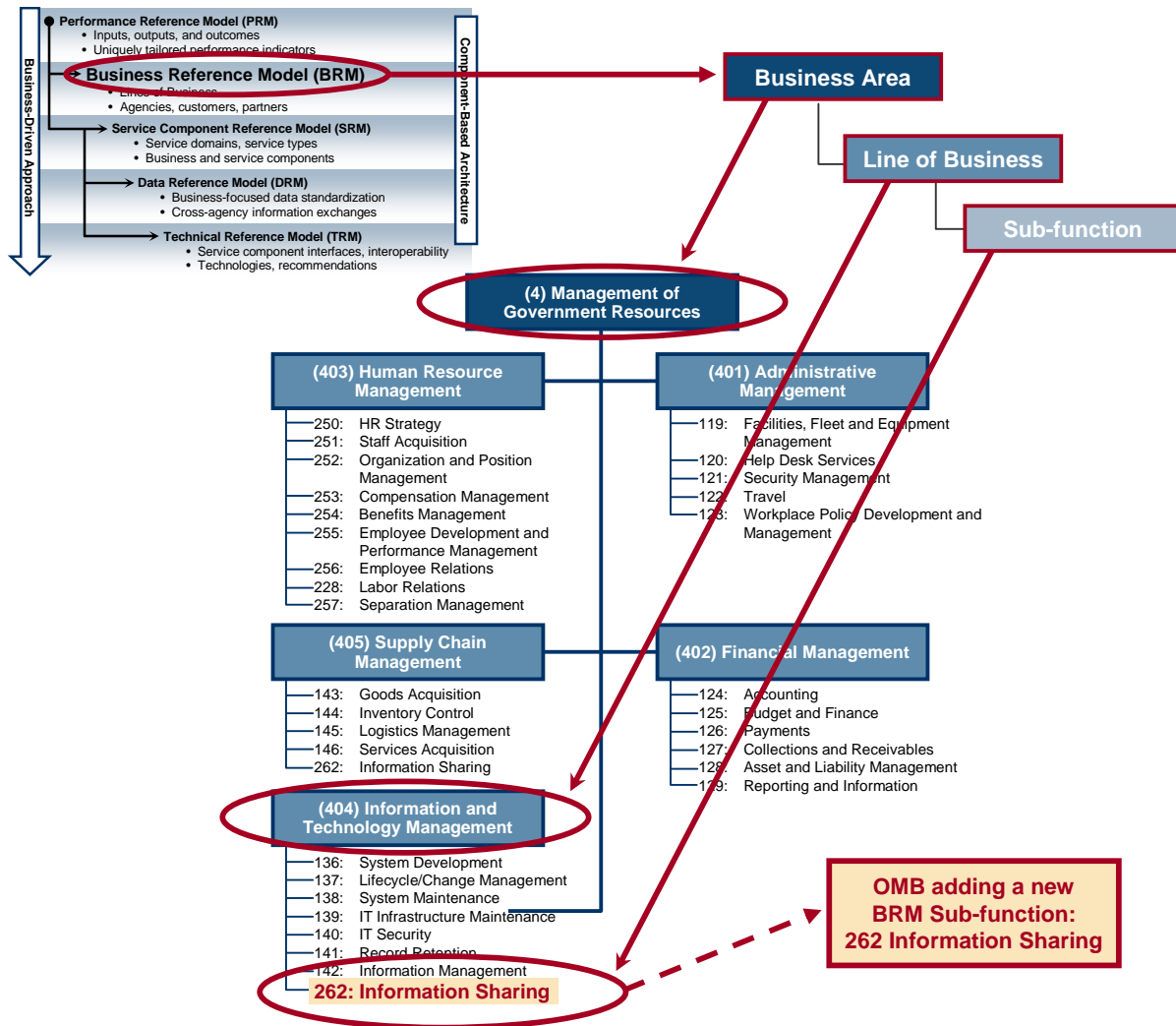


Figure 5-3. The BRM Sub-Function Added to the FEA BRM

The FEA BRM sub-function is not meant to describe the mapping of an agency's mission-related activities for collecting and processing information. It provides a budget/planning bin for the components necessary and related to SAR, AWN, and TWL to build and allow access to organization-hosted ISE Shared Spaces. ISE participants need to determine how they will build ISE Shared Spaces, a secured and trusted physical space outside of internal networks to expose data and provide appropriate access to available reusable shared services. Further, the FEA BRM sub-function provides a single, distinct code for budgeting information sharing investments. This sub-function makes it possible to easily identify ISE investments (among other agency investments in information sharing) and establish performance metrics for ISE deployment. This sub-function also aids ISE participants in identifying cost savings because it allows them to leverage cross agency initiatives more readily. By leveraging the *FTF Catalog*, ISE participants will be able to bridge common initiatives and enhance reuse and leveraging opportunities. In the case of SAR, AWN, and TWL, along with other ISE mission process areas, an ISE participant would identify this sub-function in

the organization investment portfolio to support cross-community SAR, AWN, and TWL investment planning initiatives.

Figure 5-4, below, depicts the FEA BRM with ISE attributes that represents alignment to ISE core mission processes (SAR, AWN, and TWL) consistent with the ISE expanded *FTF Catalog* inputs.

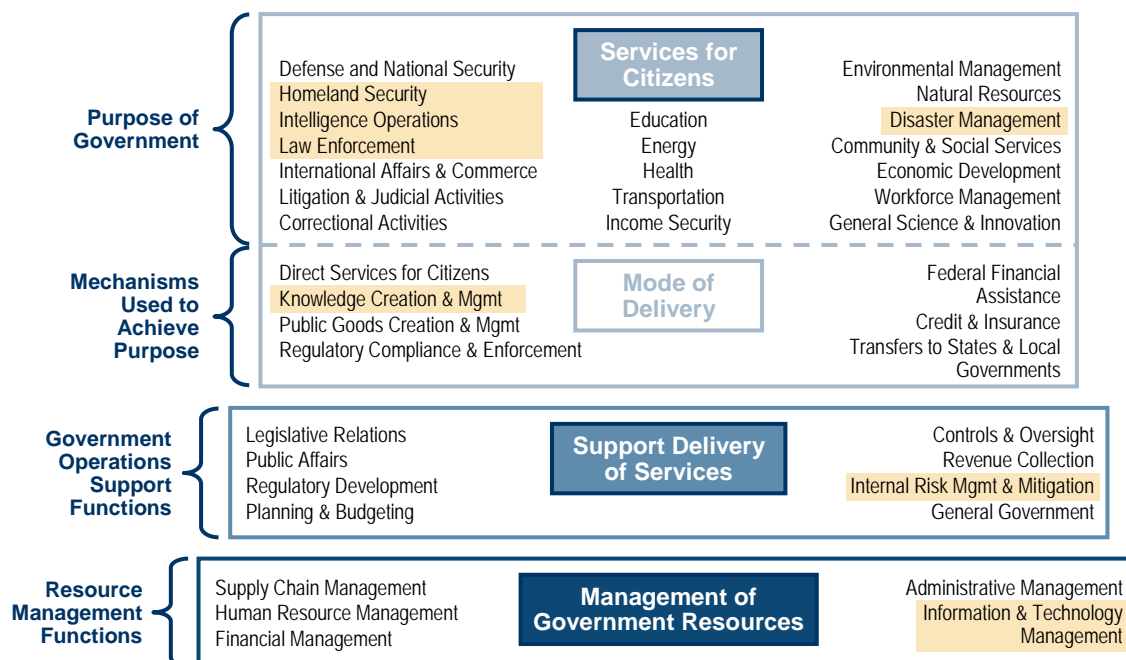


Figure 5-4. The FEA BRM Highlighting ISE Attributes

For example, in the case of implementing **suspicious activity reporting (SAR)** capability into an ISE participant's EA, the organization would identify an appropriate mapping to the BRM that includes the sub-functions of "Intelligence Analysis and Production – 215" and "Intelligence Collection – 214" under the Intelligence Operations line of business, the sub-function "Criminal Investigation and Surveillance – 045" and "Criminal Apprehension – 044" under the Law Enforcement line of business, and the sub-function "Information Sharing – 262" under the Information and Technology Management line of business.

Similarly, for implementing alignment of **identification and screening as it relates to TWL** within the ISE, ISE organizations would identify the following BRM sub-function mappings: "Intelligence Analysis and Production – 215" under the Intelligence Operations line of business, "Border and Transportation Security – 033" and "Key Asset and Critical Infrastructure Protection – 034" within the Homeland Security line of business, "Criminal Apprehension – 044" BRM sub-function under the Law Enforcement line of business, and "Information Sharing – 262" BRM sub-function under the Information Technology Management line of business.

Finally, for implementing **alerts, warnings, and notification**, ISE organizations would identify within their EAs, the following BRM sub-function mappings: “Key Asset and Critical Infrastructure Protection – 034” within the Homeland Security line of business, Disaster Preparation and Planning – 008” and “Disaster Repair and Restore – 009” “Emergency Response – 010” within the Disaster Management line of business, “Criminal Investigation and Surveillance – 045” BRM sub-function under the Law Enforcement line of business, “Knowledge Dissemination – 072” BRM under the Knowledge Creation and Management line of business, “Continuity of Operations – 095” under the Internal Risk Management and Mitigation line of business, and “Information Sharing – 262” BRM sub-function under the Information Technology Management line of business.

ISE participants can show and align organization-level EA development to the ISE by identifying some of the above attributes within their EA implementations. Figure 5.5 shows the interdependencies of the SAR, AWN, and TWL mission processes to the FEA BRM sub-functions.

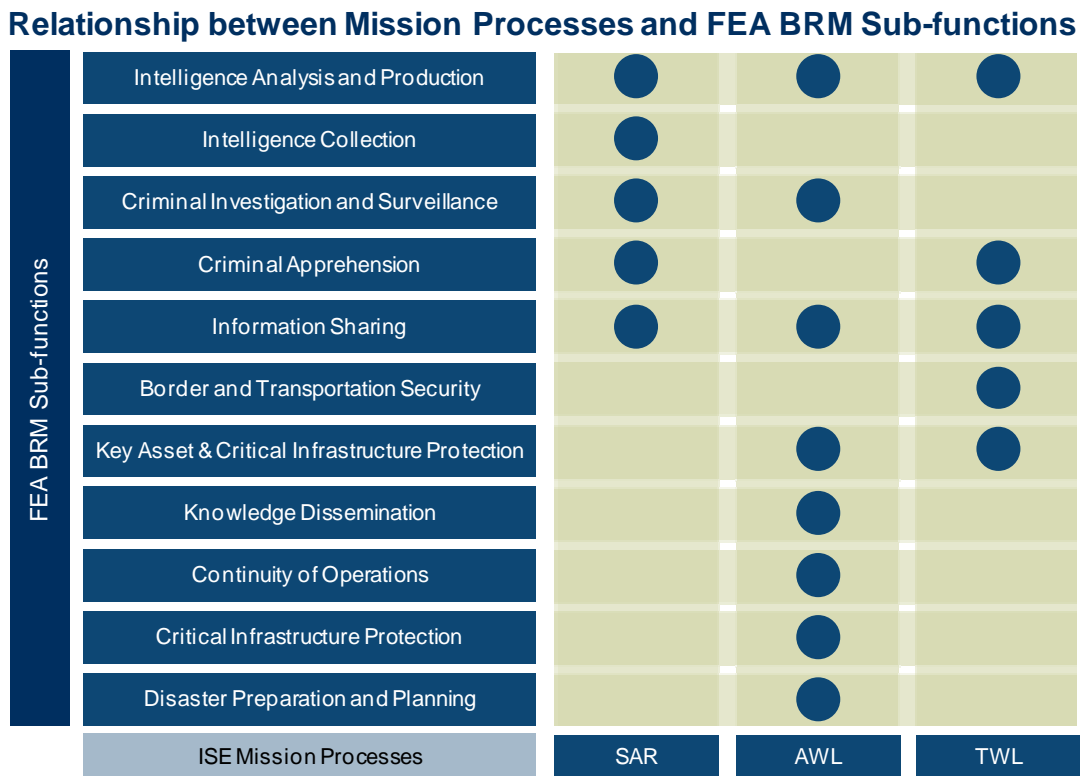


Figure 5-5. Interdependencies of Mission Process to FEA BRM Sub-functions

5.5 Core Business Process Analysis and Information Flows for ISE Mission Business Processes

5.5.1 ISE Business Process Modeling Methodologies

The *ISE EAF* Business Partition defines business processes at two levels of detail:

- Business Process Descriptions – a brief description in the ISE business process
- Business Process Models – an information flow diagram highlighting descriptive process steps and ownership of the activities performed

ISE Business Process Descriptions

The “Business Process Description” provides the name of the ISE business process and a brief description of the process purpose. Definitions for listed ISE Business Processes are provided in Appendix C. The identification and implementation of clearly defined business processes reduce future ISE gaps.

ISE Business Process Model

Business process models provide additional detail to the information flows for an actual ISE business process, and this includes the types of information required for sharing (records, databases, documents, etc.). Each event, activity, responsible party, and its interactions can be described for a set of terrorism information sharing business processes. Boundaries and responsibilities within and between participating organizations can also be highlighted.

5.5.2 Information Flows

Information flows are derived from overarching ISE mission and service business processes and provide the interrelationships and interfaces between ISE participants for sharing information packages across the ISE. These flows provide the next level of detail from the business processes and provide key inputs into the information exchanges that are the basis for identifying areas of CTISS functional standards.

The ISE overarching missions’ information flows show continuous interrelationships and dependencies that significantly affect the ISE. The critical path identified within the accompanying Information Flow Narratives, (see Appendix D for ISE-SAR, Appendix E for TWL, and Appendix F for AWN) requires the mission, applications and services, and enabling functions to carry out key programmatic activities. As an example, the ongoing ISE-SAR Evaluation Environment (EE) will assess and improve proposed ISE-SAR processes, and further AWN and TWL to identify the requirements and processes needed to ensure information is discoverable and available to State and major urban area fusion centers. A national ISE outcome will be the ability to route and exchange

critical information to the people on the ground supporting national counterterrorism efforts.

5.6 Business Process Application Example

To demonstrate the application of the *ISE EAF* by an ISE participant throughout this document, examples will map the ISE-SAR, AWN, and TWL mission process across the four *ISE EAF* partitions.

5.6.1 ISE Suspicious Activity Report (ISE-SAR)

The SAR Process steps represent the national SAR information flow and identify those actions taken by various ISE participants in the nationwide SAR Process. As is depicted in Figure 5-6, this process flow lays the foundation for describing what additional business process analysis should be done to ensure all stakeholders have access to appropriate and relevant information when needed. Further detail of this National SAR Process may be found in *the National SAR Initiative Concepts of Operations*.⁴⁹

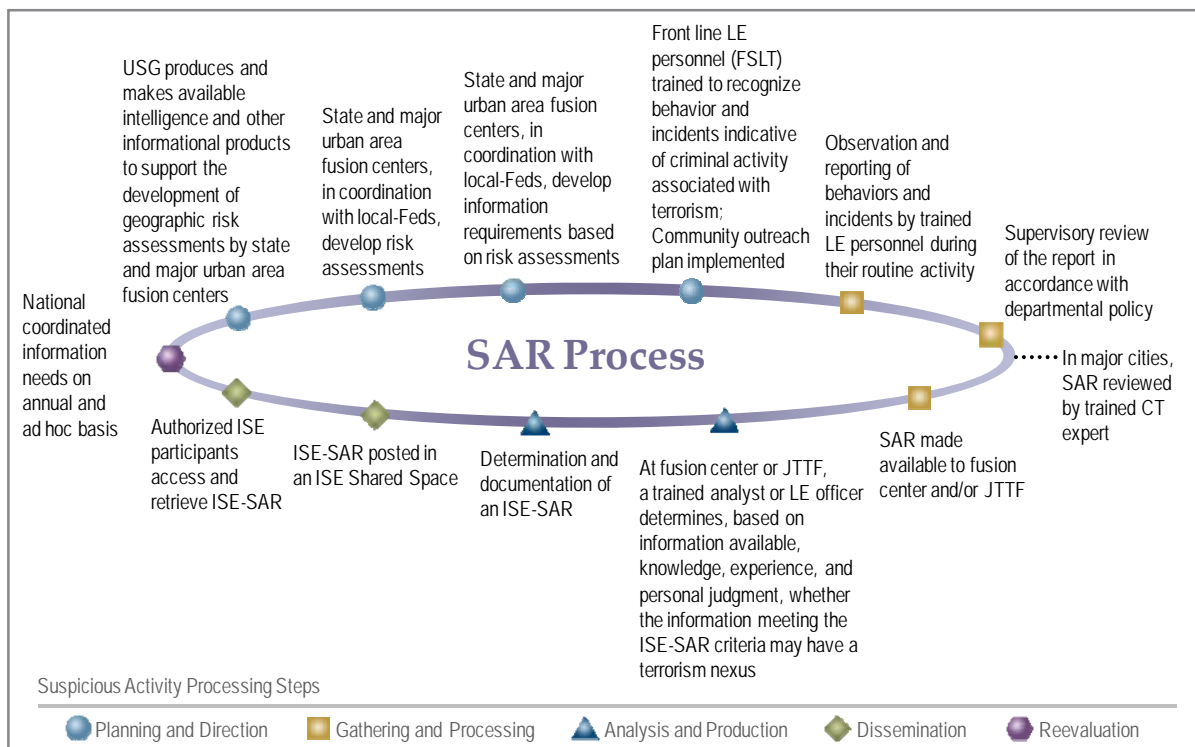


Figure 5-6. National SAR Process Steps

The ISE-SAR mission process further provides an official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, or criminal or other illicit intentions that have been determined,

⁴⁹ The National SAR Initiative Concepts of Operations (CONOPS) is available from the Office of the PM-ISE.

5.6.2 Identification and Screening (TWL Components)

The Identification and Screening mission process supports the counterterrorism (CT) community's efforts to identify and screen personnel and material. 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 select public and private sector services, and for law enforcement (LE) actions. This includes updates to terrorist watchlist (TWL) components and making them available, discoverable, and accessible to ISE participants. The terrorist watchlist mission process is a component of the identification and screening mission process and encompasses the receiving and sharing of reported information and the nomination, export, screening,⁵⁰ encounter, redress, and updates to the Terrorist Screening Database or TSDB (See Appendix E for complete Business Process Analysis {BPA} to support this mission process). HSPD-6, which was signed on 16 September 2003, required the creation of the Terrorist Screening Center (TSC) to integrate the existing U.S. Government terrorist watchlists in order to facilitate information sharing, protect the Nation and the international community, and provide 24-hour, 7-day a week responses for agencies that use the watchlisting process to screen individuals. HSPD-11, Comprehensive Terrorist-Related Screening Procedures (27 August, 2007), builds upon HSPD-6 and requires the Secretary of Homeland Security—in coordination with the heads of appropriate Federal departments and agencies—to outline a strategy to enhance the effectiveness of terrorist-related screening activities and develop a prioritized investment and implementation plan for detecting and interdicting suspected terrorists and terrorist activities. The ISE supports and aligns its Identification and Screening mission process with these overarching HSPDs.

Figure 5-8, below, illustrates that the process begins when reported **information** is received and/or shared that prompts the need for a **nomination** to the consolidated terrorist watchlist (see Appendix E on the detailed steps in the information flow with a step-by-step narrative to support the figures below). Information that would trigger the need for an individual to be nominated to the watchlist could originate from a variety of sources. For example, engaging in suspicious activity reporting (SAR) or other criminal activities such as money laundering could identify an individual or individuals engaged in terrorism or supporting terrorism activities.

⁵⁰ The screening process spans Federal, SLT governments, the private sector, and U.S. Government partnerships with those organizations among the international community that have terrorist-related screening functions.

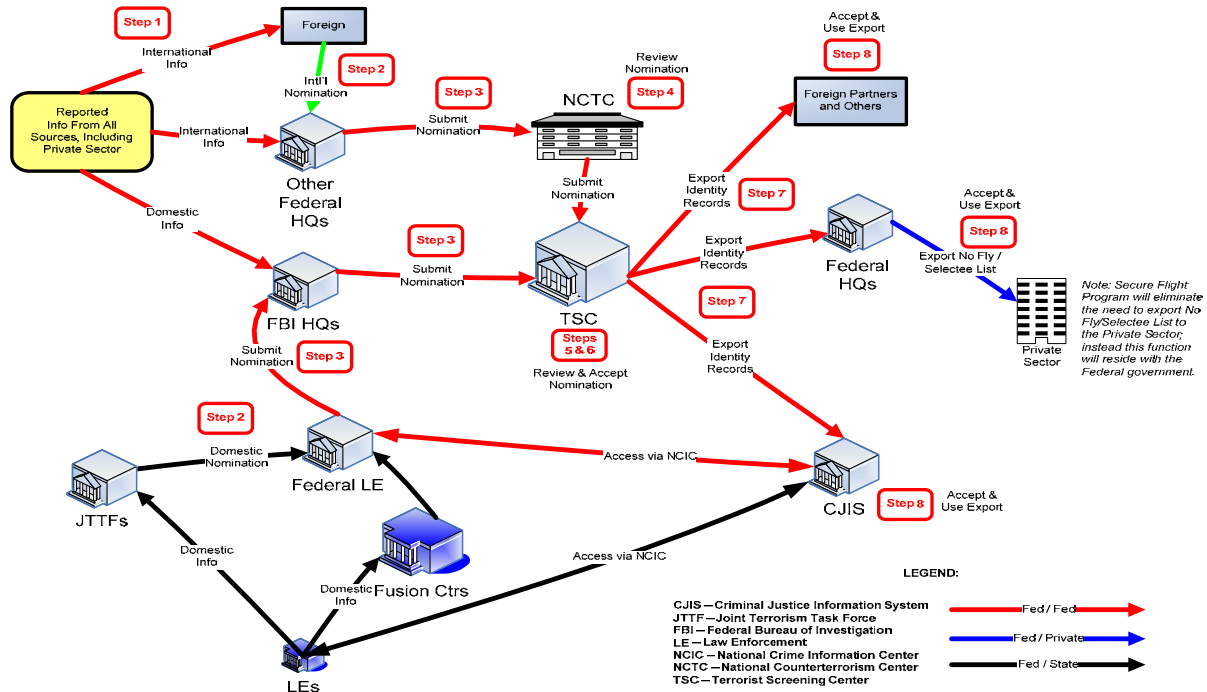


Figure 5-8. Consolidated TWL Nomination and Export Information Flow

The **screening** community spans Federal, State, and local governments, the private sector, and U.S. Government partnerships with those organizations among the international community that have terrorist-related screening functions. TSC provides this information directly to Federal and selected foreign governments and others through various methods (e.g., e-mail, database export). Individuals may initiate the **encounter** process when they seek a particular service or encounter law enforcement (ISE-SAR encounter) or homeland security personnel. For example, when an individual is stopped by State or local law enforcement within the U.S or makes an airline reservation, enters a port of entry, applies for a U.S. visa/passport, the frontline screening agency or official conducts a name-based search of the individual against applicable terrorist watchlist records.

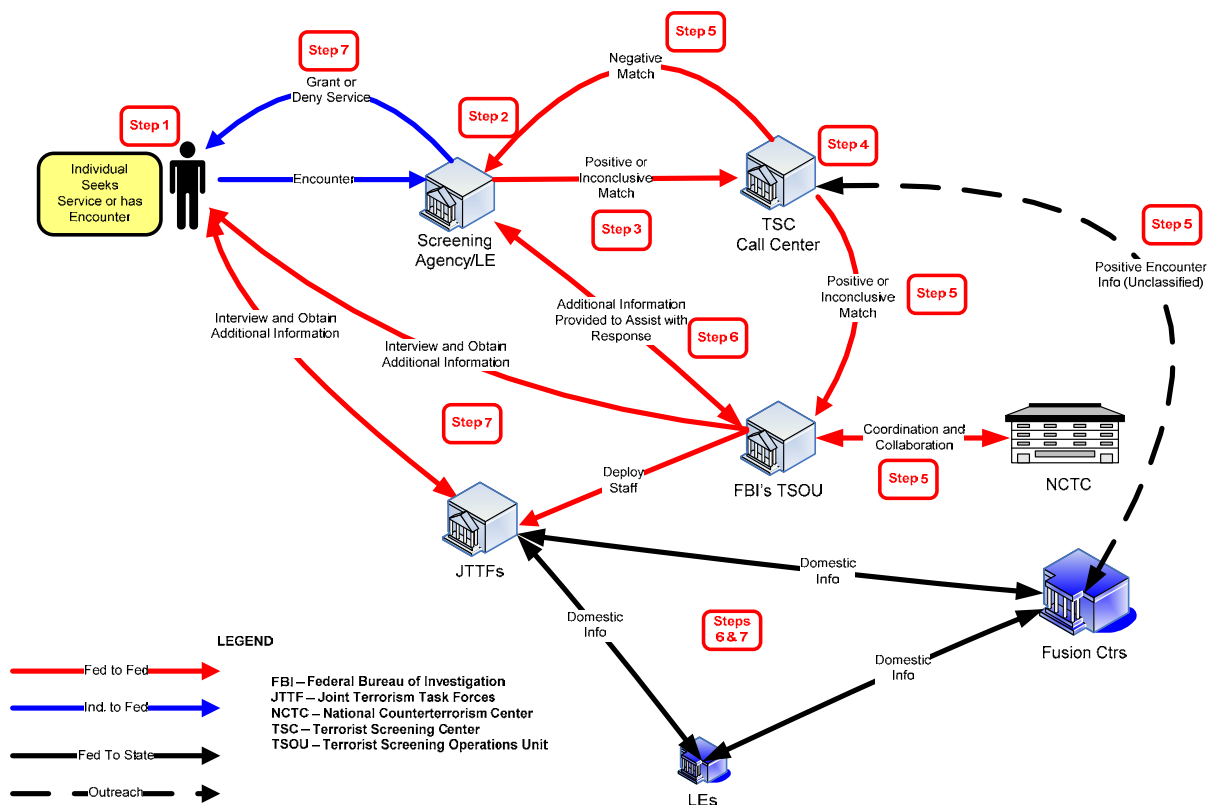


Figure 5-9. Consolidated TWL Screening, Encounter Management, and Quality Assurance Information Flow

5.6.3 Alerts, Warnings and Notifications (AWN)

The AWN mission process supports the preparation of and ensures timely dissemination and handling of terrorism alerts and warnings among ISE participants at appropriate security levels. The Federal ISE AWN process applies to threats with either a foreign or a domestic terrorism nexus. The ISE AWN process activities can be grouped into four phases: (1) **analysis** of information by Federal agencies; (2) **coordination** among key ISE AWN producers and production of federally coordinated ISE AWN products; (3) **dissemination** of those products to Federal, SLT, private sector partners, and foreign partners; and (4) **follow-up** activities. Leveraging the *ISE-SAR Functional Standard* and other CTISS program efforts, once an observation or a behavior is determined to have a terrorism nexus, ISE participants will be able to use common processes and rules to coordinate and produce federally coordinated ISE AWN products. (See Appendix F for complete Business Process Analysis (BPA) to support this mission process).

Federal agency departments have begun efforts to define AWN for the ISE; these efforts helped set expectations for what an ISE AWN should encompass and meet overarching ISE goals and objectives. Additionally, National Security Presidential

Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20, establishing a comprehensive national policy on the continuity of Federal Government structures and operations, identifies important relationships between the ISE and continuity operations and communications particularly in supporting National Essential Functions (NEFs) and interfaces and plans with SLT governments, systems, and architectures. This effort includes interfaces between the *ISE EAF* and the *Continuity Communications Architecture* developed by the National Communications System. The information flow, depicted below in Figure 5-10 provides a high level view of how AWN information is analyzed, coordinated, and disseminated by various organizations.

(See Appendix F for more details on the steps in the information flow to support the figure below. Appendix F also includes a time sensitive AWN information flow diagram with step-by-step narrative.)

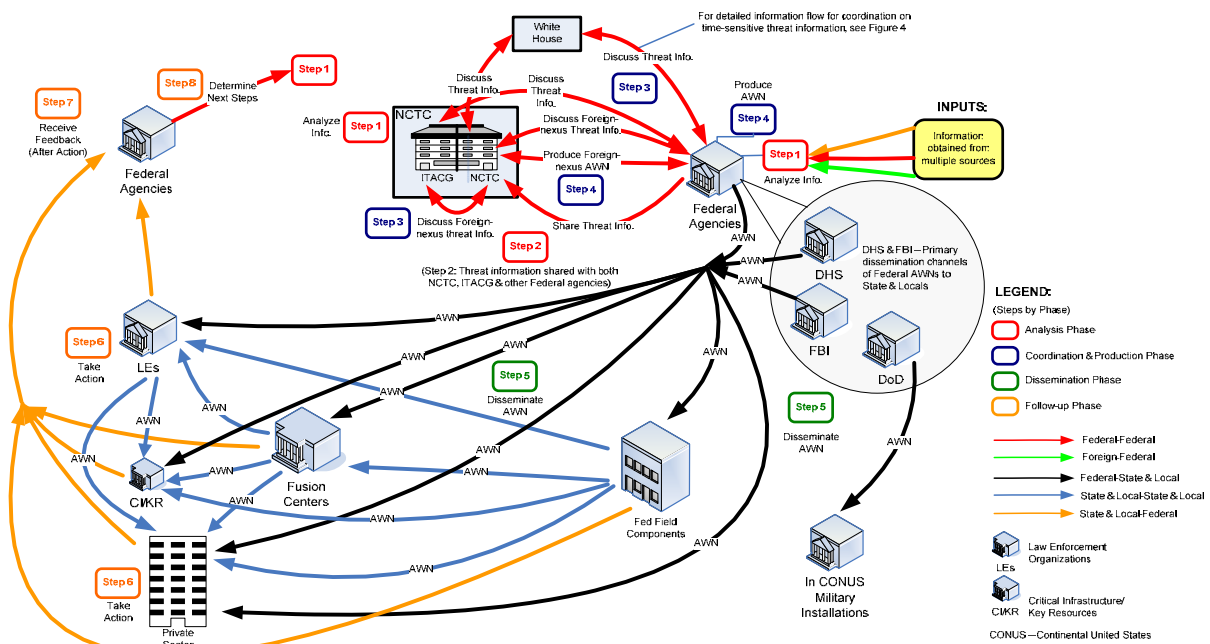
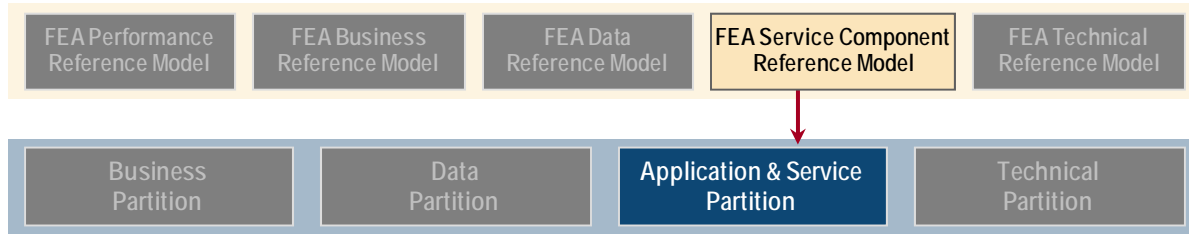


Figure 5-10. ISE AWN Information Flow

This page intentionally blank.

Chapter 6 – Application and Service Partition



6.1 Introduction

6.1.1 Overview

Similar to the Business, Data, and Technical Partitions, the Application and Service Partition of the *ISE EAF* describes the components of the architecture that provide operating capabilities to facilitate information sharing. Initially, the Application and Service Partition will leverage existing Government assets to promote reuse of existing capabilities across the ISE community. In order to orchestrate these applications and services into a unified, logical picture, a Service Oriented Architecture (SOA) approach using services as described below in Section 6.1.2. and further in Chapter 8 will be employed.

The major components of the Application and Service Partition are the ISE Core Segment and the ISE Participant Segment. The Core Segment consists of Portal Services, ISE Core Services, and Core Transport. The ISE Participant Segment consists of Applications, Shared Services, Shared Data Assets (e.g., databases), and Participant Transport. These components are supported by common technologies, including a secure implementation of the IT infrastructure needed to implement SOA.

6.1.2 An Introduction to Service Oriented Architecture

SOA is a paradigm for organizing and using distributed capabilities that may be 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. The *ISE EAF* aligns to the FEA Practical Guide Framework Service Oriented Architecture (PGFSOA) model, and SOA provides a powerful framework for matching needs and capabilities and for combining capabilities to address those needs by leveraging other capabilities. This architecture model is useful within the ISE to ensure common services are available.

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. This group of conventions is often referred to as an Architecture Description Language (ADL). Several other normalized artifacts are also used to facilitate a shared understanding of the structure of a system, its major components, the relationships between them, and their externally visible properties.

In order for SOA to meet these challenges, **services** must have accompanying **service descriptions** to convey the meaning and real world effects of invoking the service. These descriptions must additionally convey both semantics and syntax for both humans and applications to use.

6.1.3 Terminology

One of the constructs used to organize the Application and Service Partition is the FEA Service Component Reference Model (SRM).^{51 52} The SRM uses the word “service” to indicate activities performed by an enterprise on behalf of its customers. These activities are either fully automated, software-driven processes or a combination of human-driven activity and automated processes.

The SRM is organized across horizontal service areas, independent of the business functions, providing a viable foundation that promotes the reuse of applications, application capabilities, components, and business services. It is structured hierarchically around service domains, service types, and service components, as depicted in Figure 6-1, FEA Service Component Reference Model.

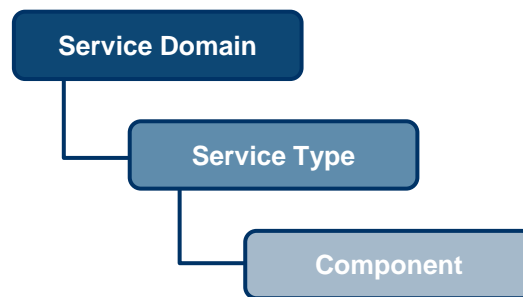


Figure 6-1. FEA Service Component Reference Model

The SRM Service Domains provide a high-level view of the services and capabilities that support enterprise and organizational processes and applications. Service Domains consist of Service Types that further categorize and define the capabilities of each Domain. Finally, each Service Type includes one or more Service Components that provide the building blocks to deliver the Component capability to the business. A Component is defined as a “self contained business process or service with

⁵¹ OMB, *FEA Consolidated Reference Model Document, Version 2.2*, Ibid., 46-63.

⁵² The Application and Service Partition also includes items other than services that are not defined by the SRM. This partition defines actual software applications and databases as well as services.

predetermined functionality that may be exposed through a business or technology interface.”⁵³ The ISE Core Services, ISE Portal Services, and Shared Services map to this reference model.

The Application and Service Partition target architecture is based on service oriented principles, as stated above. SOA refers to “line-of-business services” as those services that automate a unique portion of a business process typically not reusable by others. SOAs refer to “core services” as services required by a majority of developers and users and are generally provided by ISE Implementation Agents. Further, services can be split into two primary groups: legacy services and contemporary services. Many legacy services originate from already existing applications that can be modified and exposed via the ISE, often using middleware technology. Contemporary services, in contrast, are newly developed services that encapsulate business processes for exposure via the ISE.

6.2 FEA Service Component Reference Model Mapping

The FEA Service Component Reference Model, shown in Table 6-1, contains seven Service Domains. Each domain represents a top-level service category within the ISE. Each Service Domain contains multiple Service Types, as shown in the table. Likewise, each Service Type contains a set of SRM Service Components. These SRM Service Components map to the ISE Core Services and ISE Portal Services.

⁵³ Office of Management and Budget, *Ibid.*, 46.

Table 6-1. FEA Service Component Reference Model Alignment to ISE Core Mission Process

Service Domains	Service Types	ISE Mission Process
Customer Services	Customer Relationship Management Customer Preferences Customer Initiated Assistance	AWN TWL
Business Management Services	Management of Process Organizational Management Investment Management Supply Chain Management	AWN SAR TWL
Digital Asset Services	Knowledge Management Records Management Content Management Document Management	AWN SAR TWL
Business Analytical Services	Analysis and Statistics Visualization Business Intelligence Knowledge Discovery Reporting	AWN SAR TWL
Back Office Services	Data Management Human Resources Financial Management Asset/Materials Management Development and Integration Human Capital/Workforce Management	AWN SAR TWL
Support Services	Security Management Search Communication Collaboration Systems Management Forms Management	AWN SAR TWL
Process Automation Services	Tracking and Workflow Routing and Scheduling	AWN SAR TWL

Table 6-2 shows the mapping of ISE Portal Services and ISE Core Services to SRM Service Domains and Service Types. The ISE Portal Services and ISE Core Services are defined in the sections that follow.

Table 6-2. Mapping of ISE Core and Portal Services to SRM Service Domain and Type

ISE Core and Portal Service Categories	SRM Service Domain: Type
Collaboration	Support Services: Collaboration
User Interface	Customer Services: Customer Preference
Portal Hosting	Support Services: Collaboration
User Assistance	Customer Services: Customer Initiated Assistance
Mediation	Back Office Services: Data Management
Security	Support Services: Security Management
Discovery	Support Services: Search
Enterprise Service Management	Support Services: Systems Management
Storage	Digital Asset Services: Content Management
Messaging	Support Services: Communications

6.3 Baseline Application and Service Partition

The baseline ISE Application and Service Partition consists of current IT assets developed over time by ISE participants. Terminology varies among organizations; however, it includes systems, applications, databases, and services. For the purpose of this document, systems are defined as a set of resources including people, software, hardware, and networks that provide comprehensive capability. Applications are defined as software collections that provide specific functionality within a system (e.g., an accounts payable function in an accounting system). Applications can include services when invoked, and provides specific capabilities (e.g., determine the current account balance for a vendor). Systems and applications may include data assets such as databases, documents, video files, or other digital data resources. As defined by the FEA DRM, a Data Asset is a collection of Digital Data Resources that is managed by an organization, categorized for discovery, and governed by a data steward.⁵⁴

Numerous existing systems and data assets in the Federal Government contain useful information that could be leveraged for terrorism information sharing. However, information is kept in disparate databases (silos) or follows incompatible standards that make it difficult to address/solve terrorism nexus-related concerns. Further, an effort is underway to review OMB Exhibit 300 and Exhibit 53 entries from ISE participants to identify information assets relevant to the ISE. This review will be used to form a more comprehensive list.

⁵⁴ OMB, The Data Reference Model Version 2.0, Ibid.

6.4 Application and Service Target Partition – ISE Core Segment

The foundation for information sharing employs enterprise-level applications and services including discovery (search and metadata registration), security (authentication and appropriate access controls), mediation, messaging, enterprise management, storage (e.g. directory services), collaboration, and others. An important principle is for data, applications and services to be loosely coupled and interoperable with one another. Therefore, neither the application and services nor data is dependent on the physical implementation and location of the underlying information technology infrastructure.

6.4.1 Overview

Figure 6-2 shows the target state of the ISE Application and Service Partition. Three separate instances of the configuration shown in the figure support the three security domains: CUI/SBU, Secret/Collateral, and TS/SCI. The major components of ISE Core Services, ISE Portal Services, and Core Transport are shown in relation to each other. Core Transport and Core Services constitute the “ISE Core,” which is illustrated by the blue, dotted boundary surrounding the portion called the ISE. ISE Portal Services are represented by the ISE Portal and the ISE Management Portal (IMP). The ISE Portal provides the primary ISE interface to human end users. Its functions are described in Section 6.4.5. The IMP is the primary management and administration interface to the ISE. Its functions are described in Section 6.4.6. The Core Transport must contain provisions for network management, as described in Section 6.4.3 The ISE Core Services are provided to the majority of ISE users. The Core Services are described in further detail in Section 6.4.7.

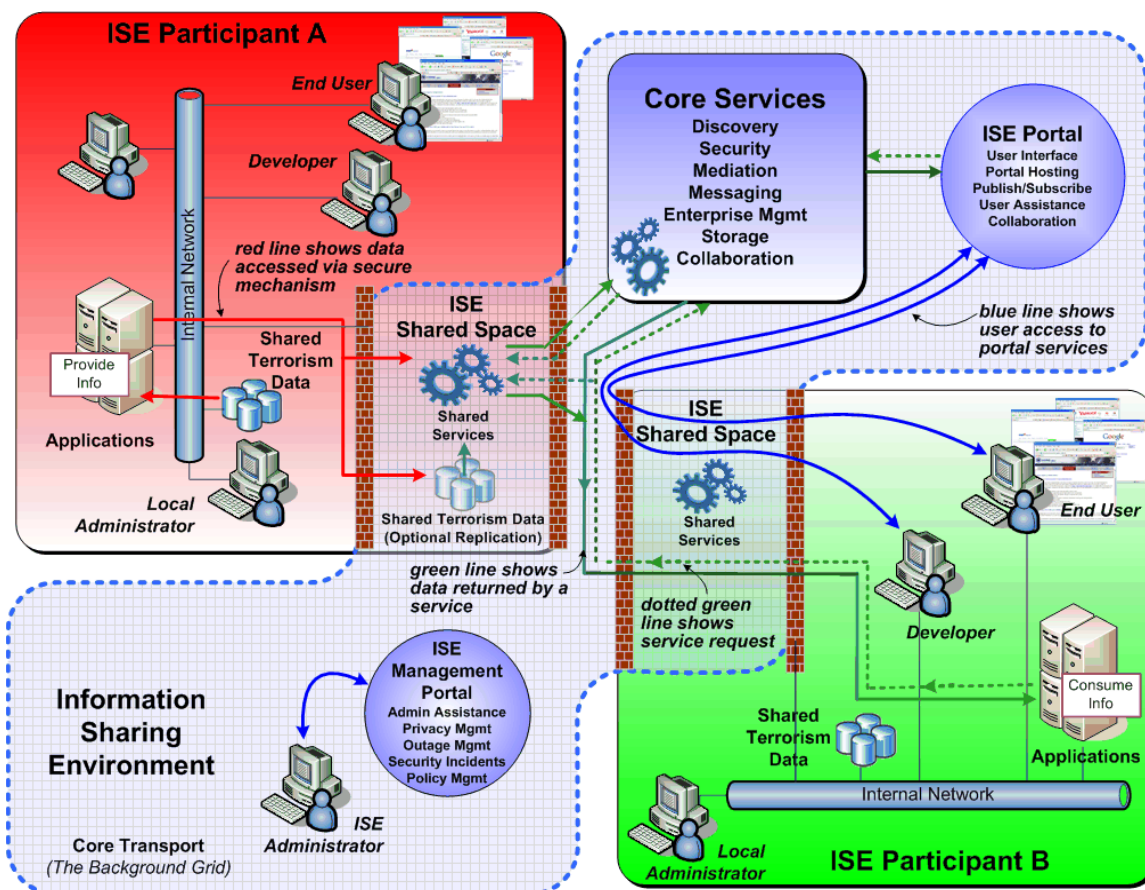


Figure 6-2. Application and Service Partition of the ISE TO-BE Architecture.
This configuration exists at three security levels: CUI/SBU, Secret/Collateral, and TS/SCI.

Note that the ISE Core is described herein as an independent construct. However, in practice it will be implemented as an extension to an organization's existing capabilities provided to ISE participants. For example, network management capabilities may be an extension of an existing service provided by an ISE participant such as DHS, DoD, or the NCTC.

6.4.2 ISE Shared Spaces

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 and applications and services accessible to all ISE participants (across the law enforcement, intelligence, homeland security, foreign affairs, and defense communities). ISE Shared Spaces are accessible in each of the three ISE security domains (CUI/SBU, Secret/Collateral, and Top Secret/SCI).

Achieving the objectives of an ISE Shared Space will require ongoing coordination of planning, governance, requirements, implementation, and testing efforts across all ISE

participants. Thus an incremental approach is necessary to ensure an orderly and effective transition to the desired operational environment.

ISE Shared Spaces rely on a suite of services accessing data regardless of its location. There may be multiple ISE Shared Spaces, each under the management, control, and resourcing responsibility of an ISE participant. This responsibility includes ensuring information security, data integrity, use, retention, and other data stewardship requirements are met and that the ISE Shared Space capability supports established ISE mission processes. As discussed in Section 4.6.1, a key concept of ISE Shared Spaces is that ISE participants with varying identity and access management capabilities will be accommodated but their access to information may be limited.

Therefore, the following principles need to apply to participation and implementation using an ISE Shared Space:

- Data and services are available and interoperable across the ISE by following standards for information sharing
- Infrastructure interoperability is achieved through definition and enforcement of standards, interface profiles, and implementation guidance
- Data assets, applications and services are visible, accessible, understandable, and trusted to authorized (including unanticipated) users
- ISE Core services document and advertise their performance characteristics through service level agreements

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 to be considered:

- Information flow-driven model
 - *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.
 - *Entity:* These information flows would be based upon mission business processes of an individual organization (i.e., "entity").
- Logical view model (or system-independent operational descriptions)
 - *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, search, and directory services for access and use.
- *Web Services*: Exposing terrorism information, services, and applications via Web services that interface with other ISE participant Web portals.
 - *Hybrid*: Allowing direct access, with appropriate access management safeguards, to selected applications within an ISE participant's infrastructure.
 - **Hosting and implementation model**
 - *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 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.
 - *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. 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.

These models support ISE participants in their development of enterprise, segment, and solution architectures that clearly identify the structure and attributes of the organization's ISE Shared Spaces. They also provide sufficient detail to support fiscal year programmatic plans to ensure business case justification, acquisition, installation, operations, and management requirements are met and that the ISE Shared Space capability supports established ISE mission processes. A more detailed description of ISE Shared Spaces is provided in Appendix G.

6.4.3 Transport

Information sharing between ISE participants requires a means to connect those organizations to one another. The Core Transport infrastructure connects Federal agencies (including the NCTC), State, and major urban area fusion centers (typically

one or two per State), private sector entities, and foreign government partners. Generally, each agency houses three separate networks corresponding to three security domains: CUI/SBU, Secret/Collateral, and TS/SCI. The State and major urban area fusion centers and private entities typically will not include an SCI network. The network management function, which is described in more detail in Section 6.4.4, should have a connection to each security domain to be managed.

ISE Core Transport indicates the underlying telecommunications infrastructure (e.g., copper and optical cables, routers, switches, etc.) that move ISE message traffic from one location to another. Classified messages are required to be passed on protected public infrastructure in appropriately encrypted text. These requirements are met by encrypting all messages above the unclassified level prior to transmission across the ISE Core using an approved encryption standard.

A key decision for the ISE Core is determining a provider of the described transport infrastructure. The fundamental options are (a) leverage existing Wide Area Networks (WANs) to support information sharing in the ISE, or (b) develop new WANs for the ISE. An ISE Implementation Agent should have current transport capabilities that can be leveraged for the ISE. As mission processes and requirements are better understood, the ISE Implementation Agent should develop additional transport capability.

The initial transport capability exists within agencies. However, as the ISE mission processes become better defined, new transport capabilities should be created to support the changing mission processes. At present, no organization can provide a single, unified transport service supporting all security levels. However, various WANs do exist in each security domain.

The second option is for an agency serving as an ISE Implementation Agent to develop the ISE transport infrastructure. This option would entail WANs in one or more of the security domains or development of some type of unified core network. In practice this means that, whether ISE transport exists for a specific security domain or is unified for all security domains, the core of this transport is secure. Therefore the telecommunications services required to support an ISE network would be procured from an existing, public telecommunications service provider. Multiple full-service providers can supply the underlying telecommunications infrastructure (cables, switches, routers, etc.), the necessary links between national and international service providers, the "last-mile" connections from the ISE to the agencies, and the management functions including security and information assurance as a turnkey capability.

Procuring telecommunications and WAN services is a typical Federal Government activity. Such contracting is a detailed, domain-knowledge-intensive process, involving subject matter expertise in telecommunications technology, information assurance, service-level-agreements, telecommunications laws and statutes, among other expertise. In choosing this approach, the PM-ISE would consider one of the Federal agencies skilled in such contracting to execute this task. For SAR, interfacing to the ISE

Core Transport would require State and major urban area fusion centers to identify who needs access to ISE data—such as first responders, investigators, and security personnel. State and major urban area fusion centers would be required to identify what internal networks are in use, such as investigative, case management, and alerting systems. Role-based security functions and Access Control Lists determine what services are available to the individual user. Finally, State and major urban area fusion centers would need to identify their policy guidance approach to transport including identification of requirements documented using standard operating procedures, system administrator instructions, and other policy guidance documentation.

6.4.4 Network Management Function

A network management function will be provided by the same ISE Implementation Agent organization that provides the Core Transport service. The organization would leverage existing network operations capability to support this function. The network management function should include capabilities to permit engineers and technicians to monitor, manage, and troubleshoot problems on the network. The administration function supports oversight of problems, configuration and change management, network security, performance and policy monitoring, reporting, quality assurance, scheduling, and documentation by using sophisticated network management, monitoring, and analysis tools. It provides a structured environment that effectively coordinates operational activities with all ISE participants and vendors related to the function of the network.

The network management function must be implemented with built-in redundancy to support survivability, availability, and continuity of operations requirements. Services must be provided for in all security domains: CUI/SBU, Secret/Collateral, and TS/SCI. The number and physical distribution of the administrative support functions should be determined by trade-study analysis. The service provider should be selected based on its ability to support industry best practices in the configuration and operation of a WAN.

6.4.5 ISE Portal Services

A central feature of the ISE target architecture is the ISE Portal. The ISE Portal is the primary delivery mechanism for the ISE Portal Services component of the ISE Core. The ISE Portal makes extensive use of the ISE Core Services to provide capabilities. In some cases, the ISE Portal is simply a user interface to underlying ISE Core Services. For example, the ISE Portal activity of discovering a service is primarily a human user interface to the ISE Core Service “Discovery.”

The ISE Portal is implemented using commercial portal technology and may vary for each of the three security domains. The ISE Portal provides the user access to the functions described below

User Interface: The ISE Portal provides the primary user interface to ISE capabilities. A user or application developer can visit the ISE Portal for the following services:

- A user or developer can discover available services.
- An application developer can visit the ISE Portal to register a service. Through predefined ISE Portal processes, the Service Provider will describe the service and register it in the Universal Description, Discovery, and Integration (UDDI) registry. The description should include any special considerations for or limitations to the use of the service and a point of contact.

Portal Hosting: The ISE Portal provides the capability for any ISE participant to provide access to a specific participant portal. For example, ISA Participant A may elect to provide a separate portal to information and capabilities relative to its mission process area. That participant portal can be viewed as a “sub-portal” of the ISE portal. This portal provides ISE Portal users the ability to reach the participant portal from the ISE Portal, providing ISE users with a convenient one-stop destination for ISE capabilities.

Publish/Subscribe: The ISE Portal provides capability for users to publish information and to subscribe to already published information. This service includes the following:

- **Post an Alert:** Users and automated processes can post alerts to the ISE. Alerts can take several forms including Administrative Alerts, informing ISE users of changes in content or status of the ISE (e.g., the addition of a new service or a service interruption); and Operational Alerts, informing ISE users of a change in terrorist information (e.g., an emerging threat).
- **Subscribe to Alerts:** Both users and automated processes can subscribe to alerts. Subscription processes can be tailored in terms of delivery, priority, and distribution.⁵⁵
- **Advertise Information Feeds:** Providers can advertise information feeds. Information feeds are automated information delivery services (e.g., list servers) dedicated to a particular topic area.⁵⁶
- **Subscribe to Information Feeds:** Users can subscribe to information feeds. Subscription can be tailored in terms of delivery, priority, and distribution.
- **Subscribe to information about ISE Status:** Includes events such as planned outages, problems, and resolutions.

User Assistance: The ISE Portal provides the primary point of access for user assistance. The ISE Portal provides general user assistance for features and capabilities of the ISE and with problem resolution. There are three types of user assistance:

- Automated self help provides “how to” information, usually called Frequently Asked Questions (FAQ) documents.

⁵⁵ Office of the PM-ISE, *Ibid.*, Section 5.2.

⁵⁶ *Ibid.*, Section 5.2.

- The ISE Knowledge Base provides both “how to” and problem resolution information.
- ISE real-time support is available via an on-line instant messaging/chat.

User Assistance offers automated “helper” capabilities for service providers, consumers, and end users of the ISE via resources, such as tutorials that provide on-demand help for user profiling and customization and portal presentation/foundation for integration of ISE Core Services and capabilities. User Assistance services also include Section 508 accessibility validation tools.

Collaboration: The ISE Portal provides users with collaboration services. Unlike other ISE Portal services, collaboration spans both the ISE Portal and the ISE Core. The underlying services that enable collaboration exist at the Core level. The services visible to the typical ISE user via user interfaces are categorized with ISE Portal Services. Some of these capabilities include whiteboards, blogs, wikis, and online chat/instant messaging.

6.4.6 ISE Management Portal (IMP)

The IMP is intended to provide a central interface for ISE management and administration activities. The IMP is implemented over commercial portal technology and may vary for each of the three security domains. The IMPs may be implemented as sub-portals of the ISE Portal(s). It is shown and discussed separately for clarity. The IMP provides administrator access to the functions described below.

Interact and Collaborate: Allows ISE support staff to share and discuss information related to ISE management and administration in real-time chat and asynchronous discussion groups. In addition to chat and discussion, ISE Portal collaboration also provides white-board and application sharing capability.

Report Outages or Resolutions: Both administrator and automated processes can report ISE service outages or resolutions and initiate relevant alerts. An outage is defined as a loss of an ISE capability or service. A resolution is defined as the repair of an outage.

Subscribe to Outages and Resolutions: Both administrators and automated processes can subscribe to ISE service outages and resolutions. This function allows ISE status to be reflected in local reporting locations, and allows users and processes to implement alternate service choices and return to normal processing following a resolution.

Subscribe to Information Feeds: Users can subscribe to information feeds concerning ISE management and administration. This function allows local administrators and managers to remain informed in real-time.

Manage ISE Policy: Managers and administrators can develop, store, disseminate, and retrieve ISE policy information. This function includes authentication and authorization information. Portions of this policy information are used internally by the ISE to govern privacy, security, and trust.

Respond to ISE Security Incidents: The IMP provides a central point of collaboration to respond to security incidents with real or potential impact on the ISE. Security administrators use the IMP to share security information and coordinate response to incidents.

Get User Assistance: The IMP provides expert ISE manager and administrator assistance through four sources:

- Automated self help provides “how to” information
- The ISE Knowledge Base provides both “how to” and problem resolution information. This information is provided both by ISE central management and by the administrator and manager forum
- ISE real-time support is available through on-line chat
- ISE points of contact are provided for electronic mail and telephone contact

The ISE Management Portal is a primary administration and management interface to the ISE. Other capabilities may be added as the ISE evolves.

6.4.7 ISE Core Services

The ISE Core Services represent the common capabilities for ISE participants to develop plans for implementing and exploiting SOA, leveraging and shaping ongoing development, modernization, and enhancement activities within their agency to leverage, support, and use cross agency initiatives. The top drivers defining the requirements of the ISE Core Services are directly derived from several authoritative source documents. The Intelligence Reform and Terrorism Prevention Act of 2004 mandates the ISE build upon existing systems’ capabilities. This requirement promotes reuse of architectural elements as well as minimization of unnecessary duplicated system capability.

Core Services provides core software infrastructure in support of the ISE’s service oriented architecture. Core Services provides a toolkit of capabilities that can be used by application developers to greatly simplify the process of developing a new application in support of new or improved business processes. Not only do they provide reusable services (i.e., functional capabilities) directly, they permit discovery of other reusable services and access to shared terrorism data.

The seven top-level ISE Core Services categories are

- Discovery
- Security
- Mediation
- Messaging
- Enterprise Service Management
- Storage
- Collaboration⁵⁷

All of these ISE Core Services would be leveraged into systems that support AWL, SAR, or TWL business process implementation. The following sections describe the capabilities offered by each Core Service.

Discovery

Discovery allows a user to search for and locate existing ISE services and data that can be accessed via the ISE Portal. ISE participants will publish data and services metadata in a registry to enable all users to find and understand data. Discovery plays a critical infrastructure role and comprises services that

- Allow for publishing/advertising of service definitions, descriptions, metadata, and accessibility. Information producers may include services, data repositories, devices, and business functions
- Support discovering service information as advertised by producers
- Permit discovery, retrieval, and publishing of services without interrupting normal business operations
- Enable fault recovery via discovery of redundant copies of services
- Permit discovery services to be integrated at design or run-time to create other composite services

These capabilities are summarized in Table 6-3.

⁵⁷ The NCES lists nine categories of core services. The *ISE EAF* has allocated the Application Sharing and User Assistant categories to ISE Portal Services.

Table 6-3. Discovery Service Capabilities

Capability	Description
Metadata Discovery	Metadata is data used to describe other data. Metadata services provide the ability for enterprise systems to discover and manage (publish, make visible, and access) various metadata products. Services provide the following capabilities: categorizes items into one or more taxonomies, searches for data by multiple criteria (e.g., key words, date, time, submitter), enables communities and users to retrieve and review data based on rankings, provides notification of changed items, allows namespace managers to identify preferred data for their communities, and serves as a clearinghouse for official standards and documents.
Person Discovery	Provide methods for locating people and information within the ISE using a set of common attribute definitions. Enables users to discover others based on roles, availability, knowledge, skills, or other characteristics and to dynamically establish a conference based on the capabilities of the network and devices being used.
Service Discovery	Provides the capability to enable enterprise to COI replication and discovery for publishing, finding, and invoking ISE services/applications registered and categorized in an enterprise information store. Provides integration with other technical capabilities in the foundation, including Enterprise Services Management (ESM) and Security, to support the secure discovery of these COI services/applications and invokes their use.
Content Discovery	This capability provides a way to perform federated searches for enterprise content (i.e. functional standards, data assets) across federated search-enabled data sources. This capability not only indexes the enterprise content for search, but also provides the ability to search other federated content repositories and exposes the enterprise catalog via a federated search application program interface. It provides the ability to automatically index public content and to establish and search catalogs of tagged information. The catalog entries can serve as pointers to current database contents. This capability also supports migration of COI-specific data sources to support federated search.

Security

Security Services provide protection mechanisms to ISE participants (known and unanticipated) users by supporting authentication, authorization, and access control processes to discover data and services on all networks. To secure interactions among enterprise service consumers and providers, the Security Services are defined as services that are standards-based, platform-independent, technology-neutral, and vendor-agnostic. The Security Services category includes components that

- Allow authorized users to access services
- Enable access control policies to be managed and enforced at the enterprise level
- Provide developers a mechanism to protect deployed services

- Include business processing rules that are necessary for enforcing access to protected enterprise service components
- Leverage existing industry standards and specifications from standards bodies

Table 6-4 below summarizes the capabilities offered by the Security Services category of the ISE.

Table 6-4. Security Services Capabilities

Capability	Description
Policy Decision Service (PDS)	Accepts authorization queries and returns authorization decision assertions, conforming to the Security Assertion Markup Language (SAML) Protocol.
Policy Retrieval Service (PRS)	Exposes security policies in Extensible Access Control Markup Language (XACML) format and can be used for service providers to retrieve policies for their resources.
Policy Administration Service	Used by management applications to add, update, and delete authorization policies stored as Policy Sets.
Certificate Validation Service (CVS)	Revocation status checking is performed by allowing clients to delegate the certificate validation tasks.
Principal Attribute Service	Provides query and retrieval interfaces to access attributes for users.
Public Key Infrastructure (PKI)	PKI is a service that provides and manages X.509 certificates for public key cryptography. Certificates identify the individual named in the certificate and bind that person to a particular public/private key pair. PKI provides the data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption, and digital signature services for programs and applications.

Mediation

Data and services in an enterprise environment are represented in a variety of formats. Mediation services help bridge information exchange between data producers and consumers having disparate systems. Mediation services include data transformation and adaptation.

Table 6-5 below describes the capabilities offered by mediation services.

Table 6-5. Mediation Service Capabilities

Capability	Description
Protocol Adaptation	Allows entities in the enterprise to interoperate without either party having to conform to the other's protocols or technologies.
Data Transformation	Facilitates transforming data from one form to another. It also enables translating data between COIs and various formats and supports legacy data throughout the enterprise.

Messaging

Messaging services provide a federated, distributed, and fault-tolerant enterprise messaging capability. These use multiple message brokers, including publish and subscribe, peer-to-peer, and queuing for delivering high performance, scalable, and interoperable asynchronous event notifications to both applications and end users. Messaging also supports the configuration of Quality of Service (QoS) parameters for a published message, including the priority, precedence, and time-to-live (TTL). In addition, it assures message delivery to disconnected users or applications. Messaging services are built on a message-oriented middleware that supports both asynchronous and synchronous modes of information exchange. Alerts, Warning, and Notification applications are specific examples that are built on top of Messaging services.

Table 6-6 below briefly describes specific capabilities offered by Messaging services.

Table 6-6. Messaging Service Capabilities

Capability	Description
Notification Services	Provides an application interface and the underlying infrastructure to provide users the ability to publish, subscribe, and receive notifications. Notifications are triggered by the Discovery Service when a predefined event occurs.
Alerts by topic	Provides an application interface and the underlying infrastructure to provide users/systems the ability to publish, subscribe, and receive alerts by topics. Alerts are triggered when a new message is posted to a topic or channel by a user or system (asynchronous information exchange).
Enterprise Messages	Provides an application interface and the underlying infrastructure to provide machine-to-machine messaging. The enterprise service/application subscribes to enterprise messages by topics or queues. The enterprise service/application can also publish and receive enterprise messages using this service.

Enterprise Service Management (ESM)

ESM is a continuous process of managing, measuring, reporting, and improving the QoS of systems and applications. ESM is the component that provides service management. As the number of services deployed increases, the ability to effectively manage them becomes critical. Monitoring enterprise services allows service providers and service management administrators to collect and evaluate mission critical vital signs such as service performance metrics and QoS data. ESM will integrate with several other service management offerings to provide extensive situational awareness. ESM offers the following capabilities as listed in Table 6-7.

Table 6-7. ESM Service Capabilities

Capability	Description
Monitoring and ensuring QoS of critical components	Generates a report about service health and notifies Service Providers about any unusual signs.
Monitoring Service Level Agreements (SLAs) compliance	Assists service providers in achieving service promises by monitoring service-level objectives and alerting service providers when service-level objective indicator value gets close to threshold.
Providing detection and handling of exceptions	Enables defining exception conditions, detecting and alerting exceptions, and automatically taking corrective actions to handle exceptions in real-time.
Providing insight into the usage of services	Captures usage data such as service throughput and Service Consumer information, helping with the evaluation of whether a service is useful, worthwhile to continue supporting, and if more services or forwarded staging are needed.
Providing distributed management of services	Offers IT asset managers and service providers the ability to configure, manage, and track distributed services remotely.
Accepting and responding to customer feedback	Provides a means to receive customer feedback and input, and to monitor and resolve issues.

Storage

Storage services include capabilities to achieve content delivery and discovery via backup/mirror data stores to support disaster recovery, smart cache methods, and content staging. Table 6-8 summarizes the capabilities offered by the Storage services.

Table 6-8. Storage Service Capabilities

Capability	Description
Data Source Integration	A set of guidelines and specifications that describe how to create ISE enterprise data sources for access via the ISE Federated Search.
Enterprise Content Delivery Network	Provides services to store, cache, and forward-stage information for fast access.

Collaboration

Collaboration enables communication and file-sharing among users via the ISE. It includes voice, text (e.g., instant messaging/chat rooms), video, file-sharing, and manipulated visual representation (e.g., whiteboard, slide presentation). Collaboration provides a full range of accessible, hosted, and managed services using identity management and content storage services, involving one-to-one, one-to-many, and many-to-many interactions. Collaboration enables users to discover others based on

availability, knowledge, and skills and then establish a conference based on the capabilities of the network and devices being used. Table 6-9 describes the capabilities offered by the Collaboration service.

Table 6-9. Collaboration Services Capabilities

Capability	Description
Conferencing	Supports one-to-one and one-to-many conferencing sessions. Allows white-boarding and annotation for all session participants (e.g., image-sharing and image annotation).
Person Discovery	Securely allows use of a global directory service to find people and devices on the network.
Integrated Voice over Internet Protocol Services	Enables voice and video conferencing over Internet Protocol (IP) networks.
Collaborative Workspaces	Provides a place where a group of users can publish, manage, retrieve and share information of all file types.
Application Sharing	Allows authorized users the ability to share an application running on a user's computer simultaneously with other users.
Application Broadcasting	Allows users to select either an application or a portion of their desktop that they can broadcast to all members of the collaboration session.

6.4.8 Mission Processes Usage of ISE Core Services

6.4.8.1 Alerts, Warnings, and Notifications

ISE AWN are terrorism-related AWN produced as a result of interagency coordination and disseminated to ISE participants. ISE AWN also includes urgent AWN developed with only internal agency coordination but disseminated to ISE participants.⁵⁸ The purpose of sharing AWN data is to ensure the analysis and integration of information leading to the disruption of terrorist activities and initiate protection or response efforts as necessary. The Federal Government currently uses processes that enable coordination on the production of ISE AWN for threat information of both foreign and domestic origin. The ISE AWN process activities include (1) **analysis** of information by Federal agencies; (2) **coordination** among key ISE AWN producers and **production** of federally coordinated ISE AWN products; (3) **dissemination** of those products to Federal, SLT, private sector partners and foreign partners; and (4) **follow-up** activities.⁵⁹

The objectives of the ISE AWN process include the ability and mechanisms to

⁵⁸ Based upon input from key Federal AWN producers, "urgent" signified timeframes that precluded interagency coordination.

⁵⁹ Coordination among Federal AWN producers, development of federally coordinated AWN products, dissemination of those products to SLT and private sector partners, and follow-up from SLT to the Federal Government, are key requirements of the NSIS. See NSIS, pp. A1-7 and A1-8.

- *Conduct Analysis* – Once information is received, it should be documented, stored, and analyzed to assess the reliability and credibility of the source. Approximately seven (7) major line organizations and other separate specialty elements are capable of producing information related to threats to the homeland. This analysis provides a broad based, presumably all inclusive input thread for producing ISE AWN. ISE AWN processes should have the ability to determine whether a threat is of domestic or foreign origin. Information is also analyzed to determine relevancy to SLT and private sector partners.
- *Coordinate and Produce AWN*– Threat information relevancy is determined through coordination by ISE AWN producers. If threat information is determined to be of foreign origin or related to foreign entities, the ISE AWN coordination and production should follow expanded Interagency Intelligence Committee on Terrorism (IICT) guidelines. Once completed, this type of AWN should be reviewed for relevancy to SLT entities. The ISE AWN coordination and production process will also serve as the classification mechanism for AWN. Through interaction and discussion, Threat Matrix coordination meetings will serve as the primary mechanism used by the CT community to examine AWN and qualify their significance and potential as a threat. Finished ISE AWN should be stored on ISE databases and systems. ISE AWN stored in ISE Shared Spaces allow authorized ISE participants the ability to review and retrieve AWN based on classification levels (highest to lowest) and relevancy (to IC, Federal, SLT entities). This function allows ISE participants the ability to search and discover appropriate information as needed.
- *Disseminate AWN* – ISE AWN information will be distributed to Federal agencies, State, and major urban area fusion centers, SLT (law enforcement) officials, and private sector partners. ISE AWN producers use secure communication channels to provide threat information to applicable IC and law enforcement AWN recipients. ISE AWN information can be distributed to consumers through a variety of communication mechanisms, which can be as simple as voice/e-mail notification of ISE AWN availability and as complex as fusion center/IC entity interaction and data transfer.
- *Provide AWN Process Follow-up* – Once AWN information is disseminated to applicable parties through ISE Shared Spaces, ISE participants should have the ability to monitor threat-related intelligence; make recommendations on additional ISE AWN products and threat related intelligence; and issue AWN updates, retractions, or escalation notices. Follow-up also involves providing avenues for SLT and private sector partners to provide feedback to AWN, report actions taken in response to ISE AWN issuance, and make recommendations on future ISE AWN products. All feedback should be reviewed by AWN providers for applicability and viability for inclusion in future ISE AWN products.

As shown in Table 6-10, AWN information and processing can be directly correlated with ISE Core Services and FEA SRM Service types.

Table 6-10. Mapping of AWN Information Flow to ISE EAF Core Services and FEA SRM

ISE AWN Information Flow Process Steps	ISE EAF Core Services	FEA SRM Service Type
Information	Storage: Database Collaboration Security	Data Management Collaboration Security Management
Analysis	Collaboration Storage: Database Security	Collaboration Data Management Security Management
Coordination and Production	Storage: Database Collaboration: email Security	Data Management Collaboration Security Management
Dissemination	Storage: Database Discovery; Search	Data Management Search
Follow-Up	Storage: Database Discovery; Search Collaboration: Messaging	Data Management Search Collaboration

This table illustrates the interdependency and relationship of common service types and service elements to support ISE AWN core mission processes.

Affected ISE EAF Core Processes

- *Discovery/Search* – Discovery would assist users in identifying the location of pertinent AWN analysis and reports. This process would also allow ISE participants to search for and locate existing ISE AWN products and monitor threat information that can be accessed via the ISE Portal. The ability to discover and search in an ISE Shared Space allows all IICT products to be disseminated across the Federal Government.
- *Security* – Security services provide protection mechanisms to the users in the ISE through support of control processes. This service would provide the necessary protections for controlling accesses to ISE AWN databases and the stored information. Security mechanisms, controls, and classifications also ensure that all AWN products will be distributed at the appropriate security levels across multiple security domains, through IC agencies, and by the IC agencies to their identified constituent recipients. The “system” must ensure information protection consistent with National Fusion Center guidelines, and ISE standards requirements.
- *Mediation* – Data and services must be stored in a location and manner accessible to and compatible with the applicable agencies’ dissemination tools. Data and services in an enterprise environment are represented in a variety of formats. Mediation services help bridge information exchange between data producers and consumers. Mediation services include data transformation and adaptation. If an AWN is warranted, Federal agencies coordinate the production

of ISE AWN to the extent that time and operational priorities allow. This service would accommodate the interfacing of disparate AWN dissemination systems between different ISE participants.

- *Messaging* – ISE participants could be alerted via the Messaging services that a new AWN report has been published and is being disseminated. This newly disseminated published AWN could trigger analysis that identifies a viable threat. The newly identified threat would be communicated back to ISE participants via Messaging services. Messaging services would also allow ISE participants to receive feedback on actions taken in response to ISE AWN. Feedback is invaluable when developing future AWN products.
- *Enterprise Service Management (ESM)* – ESM is the continuous process of managing, measuring, reporting, and improving the Quality of Service of ISE AWN systems, applications, and services. ESM monitoring and status alerts will provide users with notifications of failures, i.e., the inability to access any ISE Shared Spaces, including knowledge and AWN product repositories.
- *Storage* – Storage services would include capabilities to store AWN and achieve content delivery via ISE data stores. This process would be applicable to the storage of information and AWN according to the data formats outlined in ISE Functional Standards as appropriate.
- *Collaboration* – With AWN, collaborative workspaces would provide the ISE Shared Spaces environment for sharing and analyzing information gathered by ISE participants. In some instances, agencies may not have identical analytical capabilities; information sharing, coordination, and collaboration allows the appropriate agency to lead the threat assessment effort and then disseminate any required information and/or ISE AWN through the proper channels.

Once the threat information has been compiled and analyzed, Collaboration enables communication and file-sharing among users via the ISE. In the AWN process, collaboration between information gatherers could entail threat evaluation, validation, escalation, monitoring, etc. Collaboration uses a full range of accessible, hosted, managed, and content storage services, involving various levels of interaction.

6.4.8.2 Suspicious Activity Reports (SAR)

The overall purpose of sharing SAR information is to ensure the analysis and integration of information leading to the disruption of terrorist activities. This purpose can be achieved by successfully locating SAR-related data in any participating ISE Shared Space.

Table 6-11 shows the mapping of the ISE SAR Top-level Business Process to ISE Core Services and SRM Service Types.

Table 6-11. Mapping of ISE SAR Top-level Business Process to ISE EAF Core Services and FEA SRM

ISE SAR Top-level Business Process	ISE EAF Core Services	FEA SRM Service Type
Information Acquisition	Discovery: Search Security Messaging Storage: Database Collaboration	Knowledge Discovery Search Data Management Security Management Collaboration
Organizational Processing	Discovery: Search Security Messaging Storage: Database Collaboration	Knowledge Discovery Data Management Security Management Collaboration
Integration/ Consolidation	Storage: Database Discovery: Search Mediation Collaboration: Email Messaging Security	Knowledge Discovery Data Management Security Management Collaboration
Data Retrieval/ Distribution	Storage: Database Discovery: Search Collaboration Messaging Security	Knowledge Discovery Search Data Management Security Management Collaboration
Feedback	Storage: Database Collaboration Messaging Security	Search Data Management Security Management Collaboration

The objectives of SAR in ISE Shared Spaces include the ability to

- *Search participating ISE Shared Spaces* – SAR data in participating ISE Shared Spaces should be accessible and searchable through an integrated, federated process. The search capability should be able to identify needed information through flexible queries. This tool should allow a user to find known data as well as to discover information previously unknown to the requestor.
- *Search/Query Participating ISE Shared Spaces* – The SAR search capability must be able to query participating ISE Shared Spaces. ISE Shared Spaces should be configured to use an internal search tool. The federated search function must be capable of querying the internal database tool and receiving the resulting information.

- *Selectively Query ISE Shared Spaces* – The tool should be capable of searching or querying one or more selected ISE Shared Spaces as well as performing broad area searches of all relevant ISE Shared Spaces.
- *Search Unstructured/Semi-Structured (Non-Database) Data in ISE Shared Spaces* – Some data are in non-database formats, (i.e., documents, reports, various free text formats). The search capability must be able to conduct word searches in such formats.
- *Maintain Maximum Availability* – The search tool should be usable across a broad spectrum of users, within the constraints of the ISE.
- *Integrate Results (Federated Search)* – The search tools should be capable of providing a consolidated presentation of the search results, be they from a single ISE Shared Space or the results of queries from multiple ISE Shared Spaces.
- *Enable Data Screening or Preview* – The initial results list shall display submitting organization, contact information, and sought information. The search capability should be able to sort the initial search results based on the categories of information displayed.
- *Display needed data from participating ISE Shared Spaces* – Once found, the information should be viewable from participating ISE Shared Spaces by any authorized requestor.
- *View Information* – Any authorized user should be able to view all SAR data in participating ISE Shared Spaces to which the user is authorized.
- *Accurately Display Information (distribution)* – The search results must accurately reflect the data extant in the database, displayed without unintended alteration or introduced errors on the user's computer desktop.
- *Failed Contact Indicator* – The search capability should indicate any failures to access ISE Shared Spaces.
 - Prevent, while conducting the search function, inadvertent or unauthorized release of sensitive information.
- *Protect Sensitive Information from Unauthorized Access* – Sensitive information within the ISE Shared Spaces shall be protected, consistent with public law and guidelines pertaining to protection of sensitive information.
- *Provide Audit Tracking* – The search capability shall collect and document not only the originator of the search request but also the reason for the search.

Affected ISE EAF Core Processes

- *Discovery/Search* – Allows ISE participants to search for and locate existing ISE services that can be accessed via the ISE Portal. Discovery also provides a way for the user to perform federated searches for enterprise content across federated search-enabled data sources. Discovery would assist users in identifying the location of pertinent SAR databases. Discovery would allow all ISE participants to

query data elements stored within SAR records, i.e., perform a federated search. A federated search allows an ISE participant to search all available data repositories for which they are authorized on the ISE for specific information via a single search interface. The single federated search interface should allow an ISE participant the ability to formulate a query based on a set of parameters and subsequently narrow the search through more specific parameter refinement.

- *Security* – Security services provide protection mechanisms to the participants in the ISE through support of control processes. This service would provide the necessary protections for controlling accesses to ISE-SAR databases and the stored information.
- *Mediation* – Data and services must be stored in a location and manner accessible to and compatible with the search tool. Data and services in an enterprise environment are represented in a variety of formats. Mediation services help bridge information exchange between data producers and consumers. Mediation services include data transformation and adaptation. Regarding SAR, this service would accommodate the interfacing of disparate SAR systems between different ISE participants.
- *Messaging* – ISE participants could be alerted via the Messaging services that a new SAR has been published. This newly published SAR could trigger analysis that identifies a viable threat. The newly identified threat would then be communicated back to SAR originators and broadcast to ISE participants via Messaging services.
- *Enterprise Service Management (ESM)* – ESM is the continuous process of managing, measuring, reporting, and improving the Quality of Service of ISE-SAR systems, applications, and services. ESM monitoring and status alerts will provide users with notifications of failures, i.e., the inability to access any ISE Shared Space, including knowledge and SAR product repositories.
- *Storage* – Storage services would include capabilities to achieve content search, and delivery, and delivery via ISE-SAR data stores. This process would be applicable to the storage of information according to the data formats outlined in the *ISE-SAR Functional Standard*.
- *Collaboration* – With SAR, collaborative workspaces would provide the ISE Shared Spaces environment for collaborating SAR information gathered by ISE participants. Collaboration enables communication and file-sharing among users via the ISE. Collaboration uses a full range of accessible, hosted, managed, and content storage services, involving various levels of interaction. Collaboration enables users to discover others based on available capability.

6.4.8.3 Terrorist Watchlist (TWL)

One of the most important tools in the fight against terrorism is the U.S. Government's consolidated terrorist watchlist (TWL). The overall purpose of sharing TWL information is to ensure U.S. Federal departments, agencies, SLT entities, and foreign and private

sector partners all have access to a consolidated, accurate TWL to aid in controlling and protecting the Nation's borders. Information sharing is also critical to the success of the U.S. Government's terrorist-related screening programs.

As shown in Table 6-12, TWL information and processing can be directly correlated with ISE Core Services and FEA SRM Service types.

Table 6-12. Mapping of TWL Information Flow to ISE EAF Core Services and FEA SRM

ISE TWL Information Flow	ISE EAF Core Services	FEA SRM Service Type
Information	Storage: Database Collaboration Security	Data Management Collaboration Security Management
Nomination	Collaboration Storage: Database Security	Collaboration Data Management Security Management
Export	Storage: Database Collaboration Security	Data Management Collaboration Security Management
Screening	Storage: Database Discovery: Search	Data Management Knowledge Discovery
Encounter	Storage: Database Discovery: Search Collaboration	Data Management Knowledge Discovery Collaboration
Redress	Storage: Database Discovery: Search Collaboration	Data Management Knowledge Discovery Collaboration
Update TSDB	Enterprise Service Management Collaboration Storage: Database	Systems Management Collaboration Data Management
Quality Assurance	Enterprise Service Management Mediation Storage: Database	Systems Management Data Management

TWL provides the ability to

- *Access TWL information that has been exported by the TSC to Federal Government databases used by agencies that conduct terrorism screening - Consumers of TWL data should have the ability to access the data and have the data sent directly to them.*
- *Accept and use the TSDB export. Search Unstructured/Semi-Structured (Non-Database) TWL Data - Some data is in non-database formats, (e.g., documents, reports, various free text formats). The search capability must be able to conduct word searches in such formats.*

- *Search/query TWL applicable databases and data* – During the TWL screening process, the expanded user interface (UI) would allow all ISE participants to conduct terrorist and non-resident stay-related queries. During the encounter process, frontline database queries against watchlist records could be performed. Terrorist and terrorism-related queries should return information detailed enough to assist with the travel screening process, entry into the U.S., passport/visa issuance or denial, detainment at a U.S. port of entry, arrest, etc.
- *Search Unstructured/Semi-Structured (Non-Database) Data in ISE Shared Spaces* – Some data are in non-database formats, (e.g., documents, reports, various free text formats). The search/query capability must be able to conduct word searches in such formats.
- *File an appeal or complaint via TWL screening officials* – Any individual whose credentials are questioned or who is subjected to screening may file an appeal. Complaint forms should be readily available and data in participating ISE Shared Spaces should be in a format that is accessible and searchable.
- *Provide database updates when applicable to the TSDB* - Updates may be necessitated by the results achieved in any portion of the TWL process. Database updates are performed in collaboration with NCTC and all other screening agencies.

Affected ISE EAF Core Processes

- *Search/Discovery* – Allows the ISE participant to search for and locate existing ISE services that can be accessed via the ISE Portal. Discovery also provides a way for the user to perform TWL-applicable searches across federated search-enabled data sources.

Discovery would assist ISE participants in identifying the location of pertinent TWL databases. Discovery would also allow all ISE participants to query data elements stored within TWL records. During the screening and encounter processing, the users would have the ability to search the TSDB, which is an extraction of the TIDE database or specific information via a single search interface. This single search interface should allow a user the ability to formulate a query based on a set of parameters (name, date of birth (DOB), etc.) and subsequently narrow the search through more specific parameter refinement.

User interface capabilities will allow TWL information receipt, form completion and processing, and data sharing. The user interface will also allow collaboration between TWL participants as the nomination is being evaluated by NCTC for evaluation/acceptance or evaluation/rejection.

- *Security* – Security services provide protection mechanisms to the participants in the ISE through support of access control processes. This service would provide the necessary protections for controlling accesses to the TSDB and TIDE databases and the information within. The “system” must ensure information protection consistent with National Fusion Center guidelines.

- *Mediation* – Data and services must be stored in a location and manner accessible to and compatible with the search tool. Data and services in an enterprise environment are represented in a variety of formats. Mediation services help bridge information exchange between data producers and consumers.

Mediation services include data transformation and adaptation. In the case of TWL, this service is spearheaded by TSC's adherence to a detailed set of standard operating procedures (SOP) for uploading from NCTC's TIDE information into the TSDB and NCTC's work with stakeholders to implement a standardized, electronic terrorist nomination form that will enable easy ingest into applicable databases.

- *Messaging* – TWL exports, encounters, and redresses all process ISE participant alerts via messaging services. TSC exports pertinent TWL records to Federal authorities and select others via data export and e-mail. The encounter and redress processes use e-mail to send/forward and develop/file complaints, respectively.
- *Enterprise Service Management (ESM)* – ESM is the continuous process of managing, measuring, reporting, and improving the Quality of Service of TWL systems and applications. Based on various process results (screening results, encounter, redress inquiry), TSDB updates may result in other external partners' databases. ESM is performed in conjunction with NCTC, FBI, TSC, and screening agencies and is documented in quality assurance records.

The Encounter Management Application (EMA) also provides quality assurance (QA) through management of possible "hits," or matches vs. the TWL and by storing records of all incoming encounters.

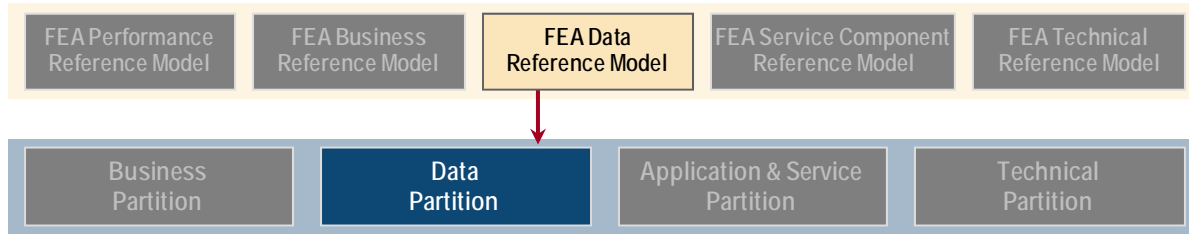
- *Storage* – Storage services would include capabilities to achieve content search and delivery. This process would be applicable to the storage of information according to the data formats outlined in a Functional Standard as appropriate.
- *Collaboration* – With TWL, TSC's export of watchlist information provides the collaborating and sharing of TWL information gathered by ISE participants. Collaboration enables communication and file-sharing among users via the ISE. TSDB contains biographical information from the TIDE database, which provides a direct export to the majority of the watchlist community via database uploads, various applications, and e-mail. Collaboration uses a full range of accessible, hosted, managed, and content storage services involving various levels of interaction.

6.5 Target Application and Service Partition – ISE Participant Segment

The target Application and Service Partition of the ISE Participant Segment must be developed by each organization participating in the ISE. The Office of the PM-ISE will work to coordinate inputs from each participant as the ISE definition evolves. Each ISE participant will provide descriptions of its target environment for agency Applications, Shared Data, and Shared Services. The process for developing the ISE participant

target architecture will be an integral part of the EA and Capital Planning and Investment Control (CPIC) process performed by each in accordance with OMB guidance.

Chapter 7 – Data Partition



7.1 Introduction

The Data Partition of the *ISE EAF* describes the vocabulary, data model, functional standards, and information exchange structures necessary to support the ISE mission, vision, and performance goals.

The PM-ISE has designated the CTISS Committee as the primary body for developing and harmonizing ISE common standards. The CTISS identifies relevant standards categories, standards defining bodies, and core standards for developing business process-driven functional standards and technical standards. These standards are necessary to establish an integrated, nationwide enterprise of information sharing organizations and resources.

The National Information Exchange Model (NIEM) and the Universal Core (UCORE) Interagency Initiative are complimentary efforts that are both leveraged under the CTISS to provide the ISE Data View. Harmonization with other ISE participants not conformant to NIEM / UCore exclusively for terrorism information sharing will be through the CTISS process. NIEM complies with directives specified in the Homeland Security Presidential Directive-5 (HSPD-5),⁶⁰ the Homeland Security Act of 2002,⁶¹ and Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. NIEM is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. NIEM enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations and data formatted in a semantically consistent manner. NIEM will standardize content (actual data exchange standards), provide tools, and manage processes.

The UCORE is an interagency information exchange specification and implementation profile. It provides a framework for sharing the most commonly used data concepts of

⁶⁰ Bush, President George W., "Management of Domestic Incidents, (Homeland Security Presidential Directive-5 (HSPD-5)," (February 2003), found at Internet site <http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html>.

⁶¹ Homeland Security Act of 2002, Pub. L. No. 107-296.

“who, what when, and where”. UCORE serves as a starting point for data level integration and permits the development of richer domain specific exchanges. UCORE was developed in concert with NIEM program office, and is a collaborative effort between DOD, DOJ, DHS and the Intelligence Community.

7.1.1 Functional Standards

As defined further in Section 7.3, functional standards will contain the business context and information exchanges, and provide implementation guidance. Based on the information provided in these standards, ISE participants may be able to implement the exchange as is or may be able to extend it into agency processes to suit their needs. For example, with the SAR mission process, examples of the types of data to be gathered in the standard and transferred to an ISE Shared Space are data derived from Field Interview Cards, existing SAR records, 911 reports, and other observation data sources from first responders and security personnel. A structured format supports the gathering, blending, and sharing of information while helping to ensure that privacy and civil liberties are adequately protected and that necessary security features and assurances are present. Similar examples may be found in both AWN and TWL mission processes. The *ISE-SAR Functional Standard* was issued on 25 January 2008. It contains artifacts including a SAR Exchange Data model, a Component Mapping Template, “information exchange” schemas, and XML Instances.

7.1.2 Linkage Between Business and Data Partitions

The Functional Standards are intended to provide instructions to ISE participants when implementing a specific exchange of data. The business requirements and information flows between ISE participants are described by business processes as defined in the *ISE EAF Business Partition*. Ultimately, the linkage between the Business Partition and the Data Partition must exist for the *ISE EAF* to be effective.

It is important to note that the definition of ISE mission business processes will provide the requirements for shared data that will ultimately be documented in a Functional Standard. These processes will examine/analyze ISE participants’ data source (authoritative or not, types of structure, semi-structured, and unstructured) and identify counter terrorism-related data assets to improve data context and specify query point(s) to retrieve data assets to enhance data sharing. Furthermore, these mission processes will be used to derive additional data requirements consistent with the information exchange development life cycle, as described in Section 7.3. In addition, the same process may help define the concept of data asset management (data steward).

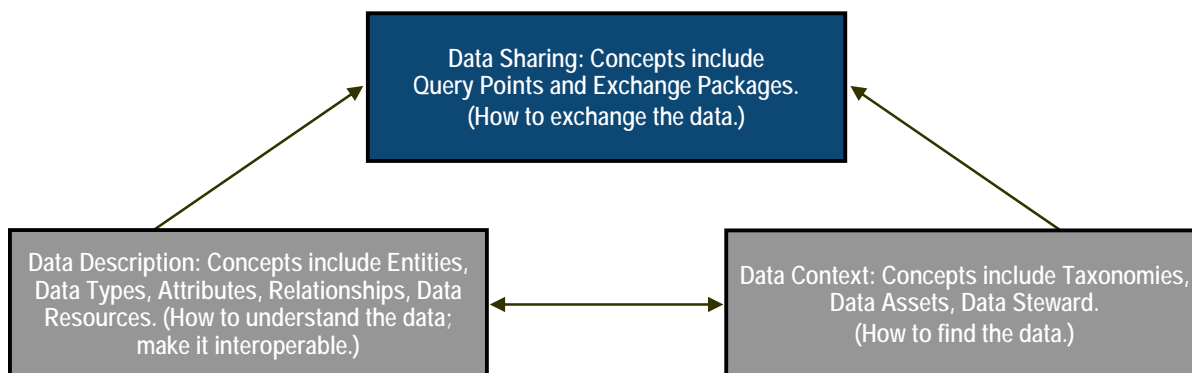
7.2 “TO-BE” Data Partition

7.2.1 Compliance with the FEA Data Reference Model

An objective of the ISE is to use metadata in a way that conforms to the Federal Enterprise Architecture Data Reference Model (DRM). The DRM is an abstract model allowing multiple implementations. The primary purpose of the DRM is to enable information sharing and reuse across agencies. It achieves its purpose through a standards-based approach to data description and categorization, discovery of common data and how to access it, and the promotion of uniform data management practices. The model is designed to optimize an organization’s data architecture for information integration, interoperability, discovery, and sharing and may be used to establish a common language within a Community of Interest (COI). The model covers three standardization areas:

- Data Description
- Data Context
- Data Sharing

An overview of the DRM and the abstract model can be seen in Figure 7-1.



“The DRM is a framework to enable information sharing and reuse across the Federal Government via the standard description and discovery of common data and the promotion of uniform data management practices”

Figure 7-1. DRM Overview

The **Data Description** standardization area captures the syntax and semantics of the data to be shared. A uniform description enables comparison of metadata for data harmonization, reuse, discovery, sharing, and exchange. One of the key concepts in this area is the **Data Schema**. Data schema is a representation of structured data; it represents metadata and is often in the form of data products as logical data models. Another concept in the Data Description area is a **Digital Data Resource** that represents a digital container (file) of information. There are three types of Digital Data Resources: structured, unstructured, and semi-structured. Structured data is formatted according to a defined structure that can be expressed in a data model. The most

common example is a database containing repeated, structured records, each containing well defined fields. Unstructured data is a collection of data that does not follow a pattern of defined fields, for example, a text or image file. Semi structured data is a mix of both these types, for example, an e-mail record that contains structured fields in the header but unstructured text in the body.

The purpose of the **Data Context** standardization area is to discover data and provide linkages to the other FEA reference models. More than one context (perspective, view) may be identified. Data Context provides additional information about data to relate it to the purposes for which it was created and used. A concept in this area is the **Data Asset**, a managed container for data, e.g., a document repository, a relational database, or a Web site. Another concept is the **Data Steward**, a person or organization responsible for managing a Data Asset.

The purpose of the **Data Sharing** standardization area is to provide a reference for describing services offered by a COI to enable access to and exchange of data. The exchanges may be ad hoc requests or scheduled requests and exchanges. The Exchange Package provides a description of a specific recurring data exchange between a Supplier (Provider) and a Consumer. It contains metadata relating to the exchange and a reference to the Payload (content) of the message. A Query Point is a means to access and query a Data Asset.

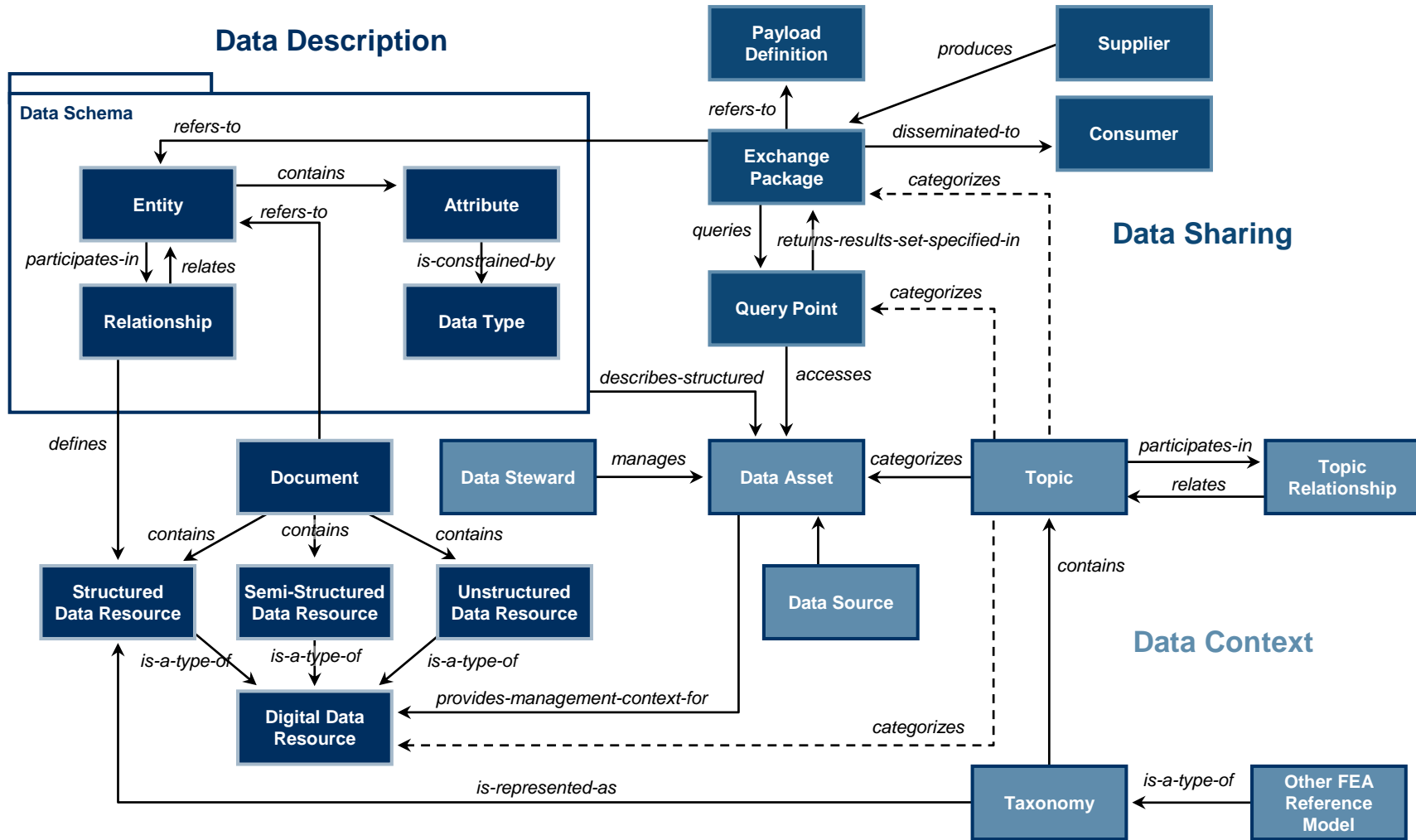


Figure 7-2. DRM Abstract Model⁶²

⁶² Office of Management and Budget, The Data Reference Model, Version 2.0 (OMB: Washington, DC, 2005), found at Internet site http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf.

7.3 Common Terrorism Information Sharing Standards

On October 31, 2007, the PM-ISE established the Common Terrorism Information Sharing Standards (CTISS) program consistent with the direction provided by the President in Guideline 1 of his December 2005 Memorandum and consistent with Section 1016(g) (4) of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004.

The *ISE Administrative Memorandum (ISE-AM) 300* sets forth roles and responsibilities for the administration and implementation of the CTISS program. CTISS are business process-driven, performance-based “common standards” for preparing terrorism information for maximum distribution and access to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. Two categories of common standards are formally identified under CTISS: Functional Standards and Technical Standards.

ISE Functional Standards constitute detailed mission descriptions, data, and metadata on focused areas that use ISE business processes and information flows to share information. *ISE Technical Standards* identify specific technical methods and techniques to implement information sharing capability into ISE affiliated systems.

The CTISS focus, driven by business processes derived from ISE operating concepts, is to further expand the sharing capability of terrorism information across the Federal Government into functional and integrated support areas. The CTISS also expands the information sharing capability among Federal, SLT governments, and private sector entities and foreign partners.

A baseline set of core standards was established for CTISS. The CTISS baseline is founded on the following assumptions:

- ISE common standards should not be classified
- ISE common standards should be considered throughout all phases of the intelligence cycle
- The functional standards implementation approach should leverage existing standards to enable information sharing
- The functional standards implementation approach should support development of standards to enable information sharing
- Structured and unstructured information sharing standards apply to data, documentation, related business processes, and respective production methods
- The CTISS should not be precluded from supporting the sharing of other information types (i.e., beyond terrorism information such as emergency response)

- Standards improvement should be a continuous process
- Metadata should ensure that terrorism information is understandable, searchable, and accessible based on common characteristics across the ISE
- Metadata tags should provide accuracy and relevancy indicators of the information
- XML is the chosen markup language to facilitate information sharing within the ISE
- ISE common standards should provide necessary guidance for access controls
- Standardizing CUI/SBU definitions across the ISE should be included in future standards implementation activity
- User training (initial and ongoing) should be provided to support a successful implementation of standards.

A common standards framework, the *CTISS Framework*, provides a common lexicon for defining, structuring, and guiding existing and future information resource planning and investment acquisition processes.

The *CTISS Framework* provides a relational, hierarchical mapping and programmatic structure that identifies standards types, standards defining bodies, and core standards for leveraged use across the ISE community. As depicted in Figure 7-3, the highest level of the Framework identifies the terrorism information domains, or affected interest areas, influenced by standards for information sharing, intelligence, law enforcement, homeland security, foreign affairs, and defense.⁶³

Each information domain spans all levels of the Government including Federal and SLT governments as well as foreign partners and the private sector. Consistent with the *ISE Implementation Plan*,⁶⁴ security domains affecting ISE supporting networks also span the Framework with three broad domains addressed for information sharing (Controlled Unclassified Information (CUI)/Sensitive but Unclassified {SBU}, Secret, and Top Secret/Sensitive Compartmented Information {SCI}).⁶⁵

⁶³ The five annotated terrorism information domains depicted in Figure 7-3 correspond to the five ISE communities.

⁶⁴ The *ISE Implementation Plan* may be found at www.ise.gov.

⁶⁵ For the purposes of this document, consistent with 50 U.S.C. § 435a(f)(5), Sensitive Compartmented Information or "SCI" is defined as the "classification for information in such material concerning or derived from intelligence sources, methods, or analytical processes that requires such information to be handled within formal access control systems . . ." As set forth in Executive Order 12958, as amended, the term "Top Secret" refers to "information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe." As further set forth in Executive Order 12958, as amended, the term "Secret" refers to "information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe." Finally, Controlled Unclassified Information, or "CUI" is described in detail in the May 9, 2008, President Memorandum for the *Heads of Departments and Agencies on the Designation and Sharing of Controlled Unclassified Information (CUI)*.

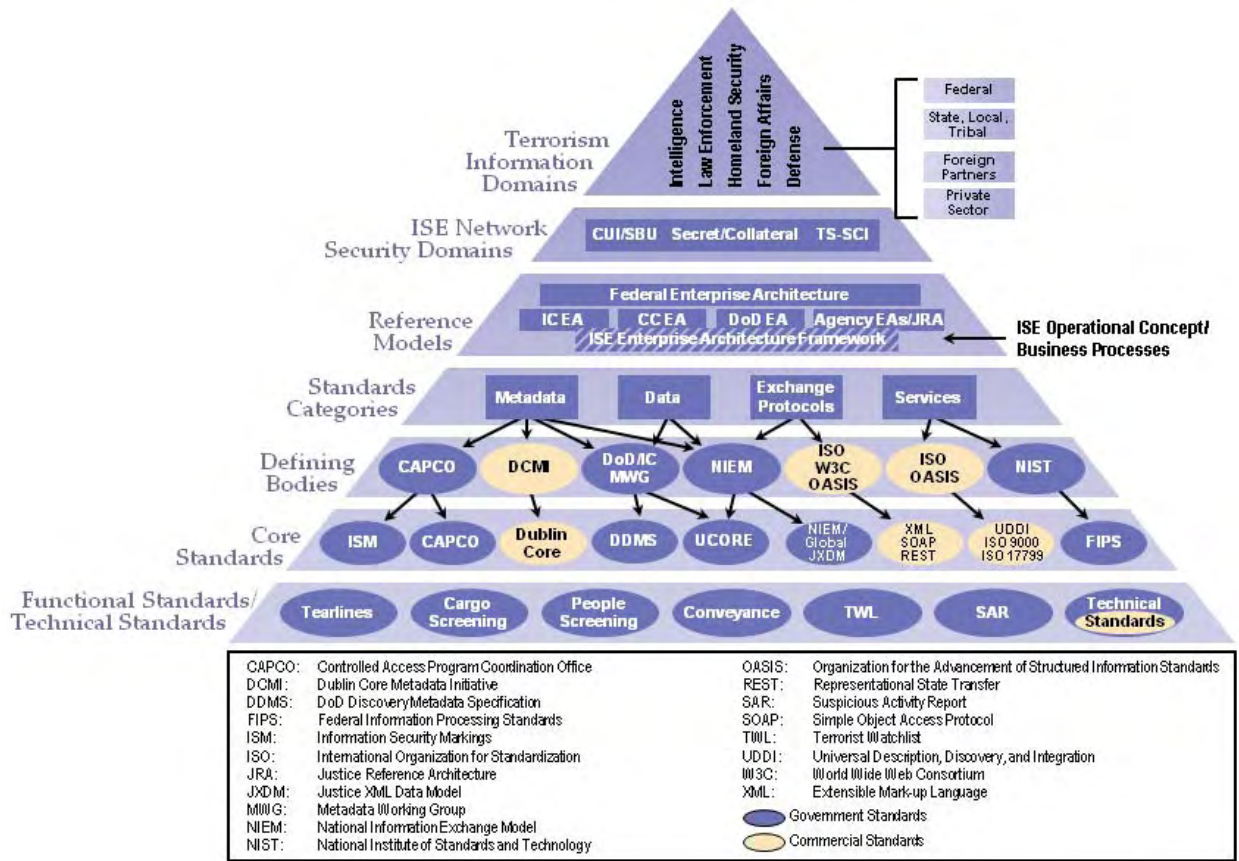


Figure 7-3. CTISS Framework

As depicted in the CTISS Framework, four broad standards types address specific aspects of information sharing products and processes:

Metadata Standards – describe those standards providing the searchable *characteristics* of terrorism information (data descriptors about actual data)

Data Standards – focus on the actual information *content* to be shared

Exchange Protocols Standards – address *the way* the information is to be shared across systems and networks

Services Standards⁶⁶ – describes the uniform *business processes, information exchanges, common services, and activities* supporting information sharing

Standards Defining Bodies represent those ISC selected public and private sector oversight and governance authorities that develop, coordinate, and issue standards for the community at large within each of the standards types that may be leveraged for CTISS. *Core standards* represent a universal set of broad, functional standards and technical standards to be leveraged from these defining bodies and tailored across the ISE community to guide agency processes and investments supporting terrorism information sharing. *Functional standards* of the CTISS will serve as the specific business process-driven and developed baseline of operational activities, processes, and mission products needed in the ISE (Suspicious Activity Reports (SARs), tearlines, cargo/people screening, terrorist watchlisting, alerts and warnings, etc.) leveraging the established core standards. *Technical standards* of the CTISS will document specific technical methodologies and practices to design and implement information sharing capabilities into ISE systems. It is at this level that near-term CTISS development and implementation activity will primarily focus.

Standards defining bodies leveraged for the CTISS program identify, develop, and release core standards used for developing business process-driven functional standards and designated technical standards. Core standards implementation recommendations from these standards bodies also provide valuable insight for establishing oversight and guidance processes into standards implementation activities used across the ISE community.

The following listing of standards defining bodies serves as representation found within the CTISS program; it does not encompass all standards bodies existing across the public and private sectors.

1. Standards Defining Bodies for Metadata
 - a. Controlled Access Program Coordination Office (CAPCO)
 - b. Dublin Core Metadata Initiative (DCMI)⁶⁷
 - c. DoD/IC Metadata Working Group
 - d. National Information Exchange Model (NIEM)

⁶⁶ At this writing, the PM-ISE intends to issue *ISE-G-106 Technical Standard Information Assurance, Version 1.0* and *ISE-G-107 Technical Standard Core Transport, Version 1.0*. When update releases to standards versions identified in ISE-G-106 and ISE-G-107 technical standards occur, the PM-ISE will release subsequent versions of the technical standards to reflect later versions and newly identified technical standards considered useful to ISE participants for managing information-related risks and perform data transmission. The *ISE-G-106 Technical Standard Information Assurance, Version 1.0* describes a suite of IA standards and recommended guidance/standards, and *ISE-G-107 Technical Standard Core Transport, Version 1.0* describes a suite of Core Transport technical standards for encapsulating data into packets suitable for transmission.

⁶⁷ The DCMI website is at <http://dublincore.org>.

2. Standards Defining Bodies for Data
 - a. NIEM
 - b. DoD/IC Metadata Working Group (MWG)
3. Standards Defining Bodies for Exchange Protocols
 - a. NIEM
 - b. International Organization for Standardization (ISO)⁶⁸
 - c. World Wide Web Consortium (W3C)
 - d. Organization for the Advancement of Structured Information Standards (OASIS)⁶⁹
4. Standards Defining Bodies for Services
 - a. ISO
 - b. OASIS
 - c. NIST

The PM-ISE publishes recommendations for information sharing standards for non-Federal government participants, through the Offices of the Secretary of Homeland Security and the Attorney General, for use by SLT governments, law enforcement agencies, and the private sector.

Consistent with Guideline 1 of the President's Memorandum of December 2005, *Guidelines and Requirements in Support of the Information Sharing Environment*, the DHS and the DOJ are responsible for making the *ISE-FS 200* and other CTISS available for use by State, local, and tribal governments and the private sector and requiring its use through grant guidance and other mechanisms, as appropriate.

7.3.1 NIEM and UCore 2.0

The NIEM program creates and manages Metadata, Data, and Exchange Protocols standards categories for several law enforcement related data domains. Universal Core (UCORE) is a product of the collaboration between the NIEM governance board at DOJ and DHS and the DOD and IC. UCORE, an inter-agency information exchange specification and implementation profile, is a starting point for data level integration and permits the development of richer domain specific exchanges across a wide variety of information sharing domains. Figure 7-4 depicts how NIEM and the DoD/IC UCORE may be leveraged to support the development of the CTISS Universal Core. The CTISS Universal Core will constitute a harmonized core set of data elements (very small in number), standards, and processes that will serve as the foundation for ISE information exchanges. Other data elements derived from ISE information sharing business process

⁶⁸ The ISO website is at <http://www.iso.org>.

⁶⁹ The OASIS website is at <http://www.oasis-open.org/home/index.php>.

will also be integrated with CTISS Core elements to define and standardize the overall information exchange.

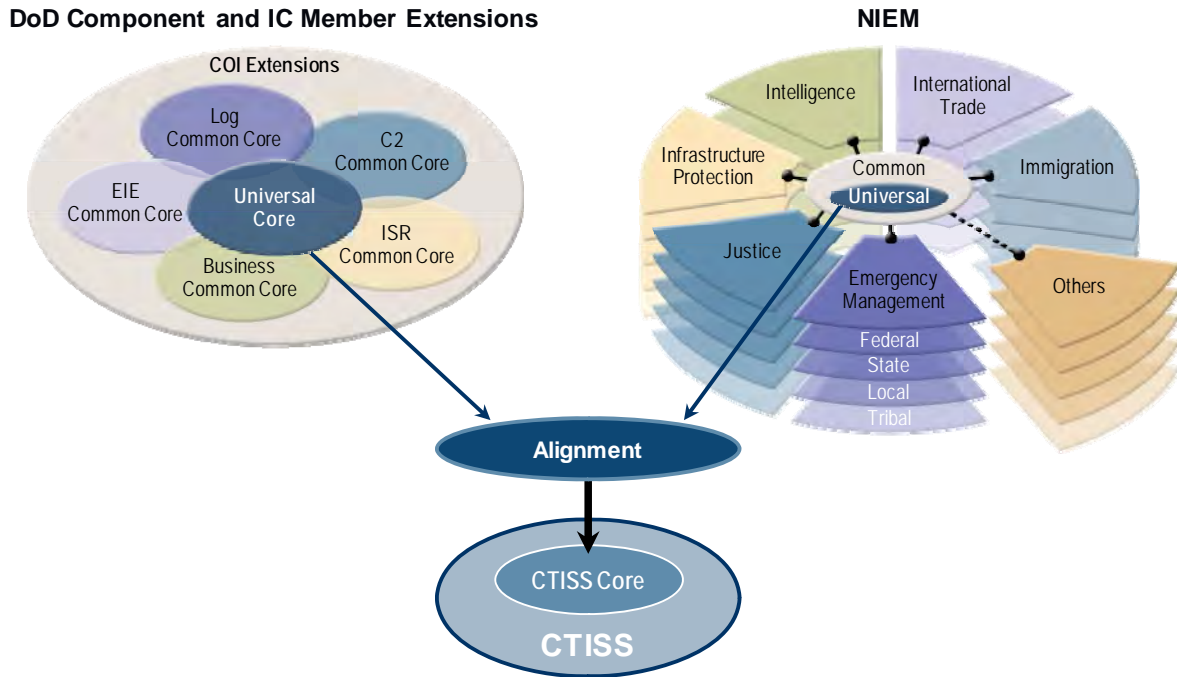


Figure 7-4. CTISS Universal Core Development

In order for an organization to effectively share information following the CTISS framework, it must have domain content to share or have a need to access CTISS data from another agency. All shared information must abide by the CTISS standards and conventions. Figure 7-5 illustrates the steps of the CTISS functional standard life cycle an ISE participant might follow when developing a standard.

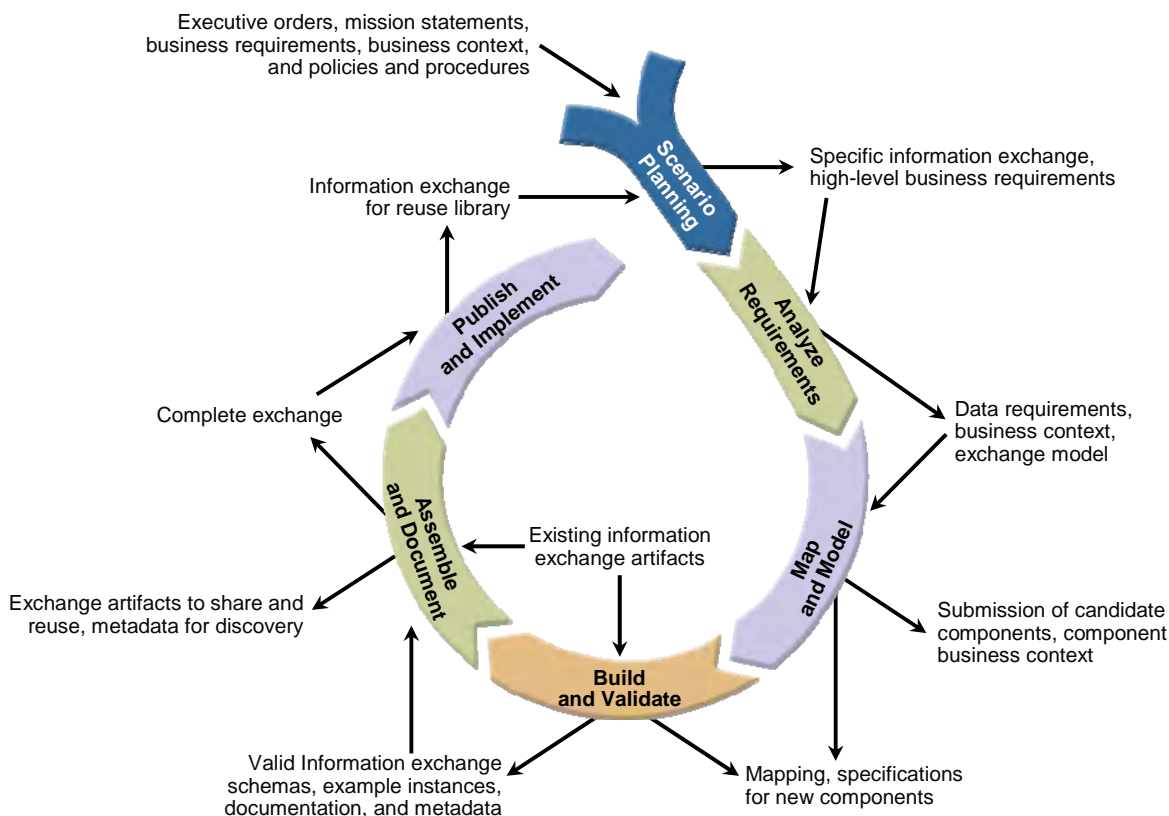


Figure 7-5. CTISS Information Exchange Life Cycle⁷⁰

Scenario Planning

Scenario planning is based, in part, on policy documents, mission statements, executive orders, ISE business processes, and other documents. Business processes are modeled in detail to determine the information currently exchanged or information that should be exchanged. For example, information about an individual to be nominated to the watchlist is identified through the Comprehensive Consolidated Terrorist Watchlist Process (an ISE business process). Such information could originate from a variety of sources.

Narratives are written to support the business models. A top-down approach may be taken using the FEA BRM to categorize business operations. The result of scenario planning includes business requirement specifications that are used to identify critical information exchanges. These requirements guide the development of an exchange through the remaining steps.

⁷⁰ Derived from the Information Exchange Package Document (IEPD) Life Cycle found in *NIEM Concept of Operations*, (NIEM Program Management Office: Washington, DC, 2007), 33.

Analyze Requirements

A high level model of the identified exchange is developed in terms of entities and relationships to identify data requirements, the organizations involved in the exchange, the trigger(s) for the exchange, and the conditions (context) for the exchange. Other products of this step may include a glossary of domain terms and a data dictionary. The products of this step are used as inputs to the next step.

Map and Model

Searches are executed to determine if there are existing exchange packages that satisfy the requirements. The COI⁷¹ may determine that an existing exchange satisfies the need or that the exchange may need to be modified. If no existing exchange satisfies the requirements, a new exchange may be developed. Similar searches are performed for the data components of the exchange. Data for the exchange are mapped against the data model, which provides a common meaning for data used among its domains, and gap analysis is performed. The results of this step are data mappings and possibly the specifications for new data components.

Build and Validate

Once the data components are mapped, the schemas (subset, exchange, extension, constraint) are developed. The COI may submit new or modified exchanges and components to the standards body based on the gap analysis. Part of this development includes generation of expanded XML instances, optional style sheets to translate the instances, and other documentation to support the exchange.

Instances based on the developed schemas must be validated to ensure they are well-formed and valid. The instances must conform to the CTISS reference schemas. The results of this step include valid schemas, examples, metadata, and documentation.

Assemble and Document

Once all the artifacts are created, the information exchange may be generated. This documentation will promote discovery and reuse.

Publish and Implement

The last stage of the information exchange life cycle is publishing and implementing. The CTISS functional standard is published within a CTISS information exchange and CTISS Federated Registry (currently available in the Common Terrorism Information sharing Standards Registry {CTISR}) that is available to other COIs for reuse. The COI may opt to publish the information exchange only in its domain. The IC Metadata

⁷¹ COI is used throughout this section to refer to a COI working on a particular data exchange model in support of the ISE program.

Standards for Publication serves as the text-based publication standard (covers both HTML and XML) within the Intelligence Community.

The CTISS process will fully support the FEA DRM. Table 7-1 summarizes the FEA DRM support provided by the CTISS information exchange development process.

Table 7-1. CTISS Information Exchange Life Cycle Support of the FEA DRM

N	Description	DRM Standardization Area		
		Data Description	Data Context	Data Sharing
1	Scenario Planning	X	X	
2	Analyze Requirements	X	X	
3	Map and Model	X	X	
4	Build and Validate			X
5	Assemble and Document	X		
6	Publish and Implement			X

7.3.2 Critical Success Factors

The **commitment of individual agencies** is critical to success. ISE participants must be firm in commitments to the use of the CTISS standard data models for all interagency data exchange. The buy-in throughout an organization can be fostered by training.

Participation in COIs is also essential in the success of ISE. A loose technical governance structure should be in place around the COIs to ensure that there is not duplicate work being conducted across COIs.

7.3.3 Observations and Issues

Because ISE implementers will follow and incorporate the CTISS, a mechanism for assuring compliance needs to be established. Tools, techniques, and training could be used to foster such compliance. Such resources should be available via a Web-based clearinghouse.

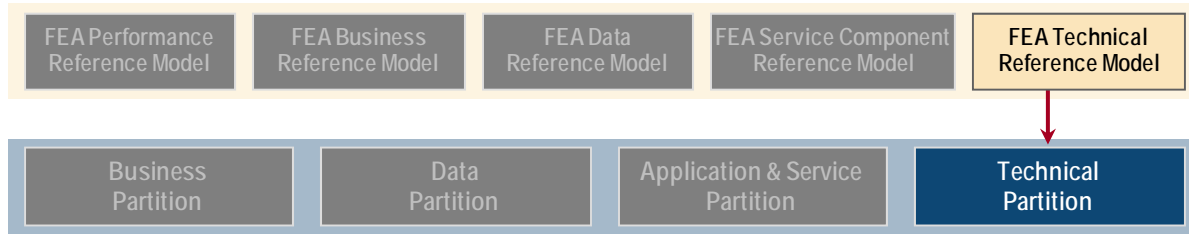
ISE participants should be encouraged to embrace voluntary consensus and Government-unique standards as appropriate, along with XML and Web services, SOAs, and intranet portal technology as well as future technologies. However, data representations should be designed around business requirements and be driven by operational needs, not by technology alone.

As more powerful and expressive mechanisms for exchanging data evolve, they should be adopted. More semantically rich representations, in particular, should be incorporated into the CTISS. This evolutionary path should be gradual. These

enhancements should be integrated to assure complete backward compatibility or require minimal manual changes.

This page intentionally blank.

Chapter 8 – Technical Partition



8.1 Introduction

This section of the *ISE EAF* identifies the appropriate components and technical standards for aligning technical architectural guidelines for implementation within the ISE. The Technical Partition also includes emerging technologies and “best practices” associated with a “TO-BE” state of a complex, interoperable, virtual ISE.

The technical standards are adopted from the *Common Terrorism Information Sharing Standards* program that defines the technical standards and guidelines for the ISE (Figure 8-1). The CTISS technical standards instantiate the technical profile required by an ISE participant and signifies what type of technology is needed to integrate an ISE participant’s IT domain within the ISE virtual domain.

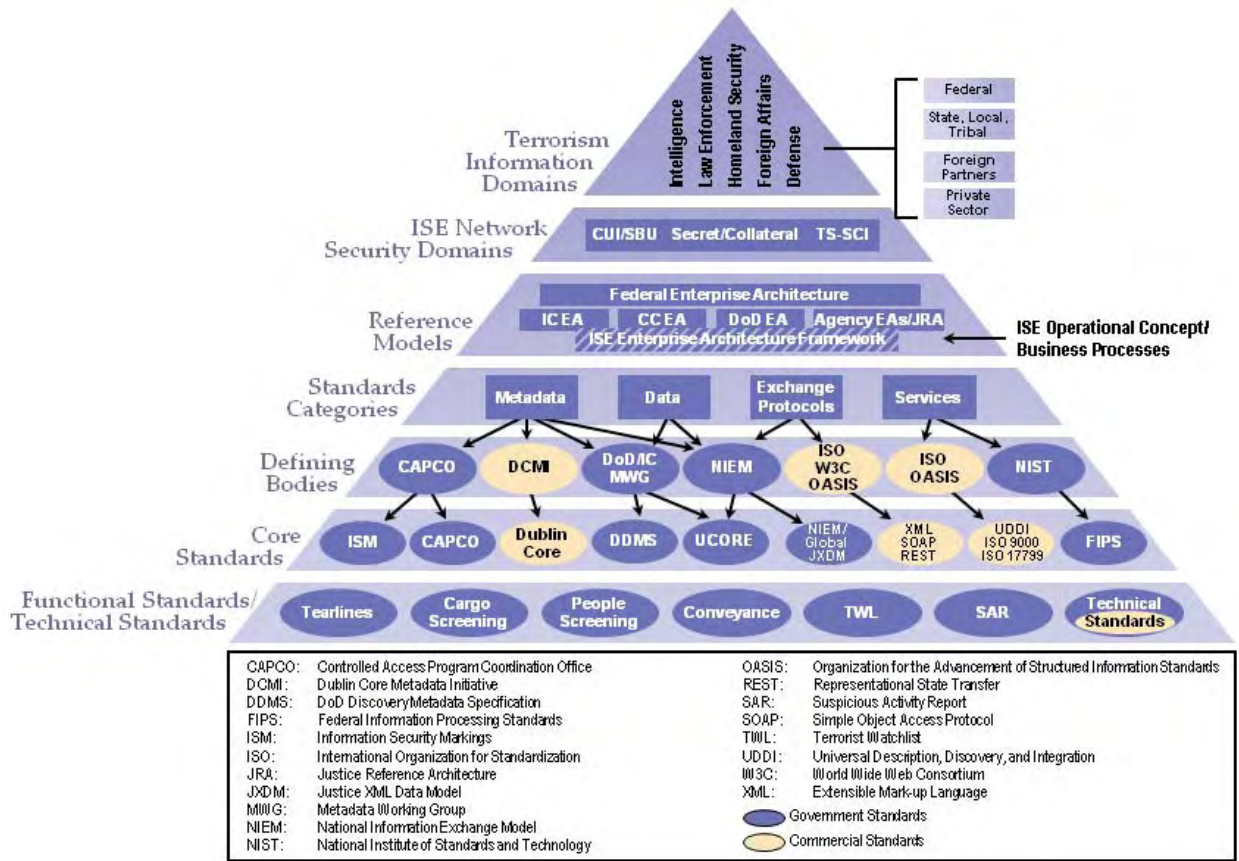


Figure 8-1. CTISS Framework

8.2 Technical Reference Model Mapping

The FEA Technical Reference Model (TRM) provides three-level taxonomy. Using this taxonomy as a basis, the *ISE EAF* Technical Partition is referenced as shown in Figure 8-2.

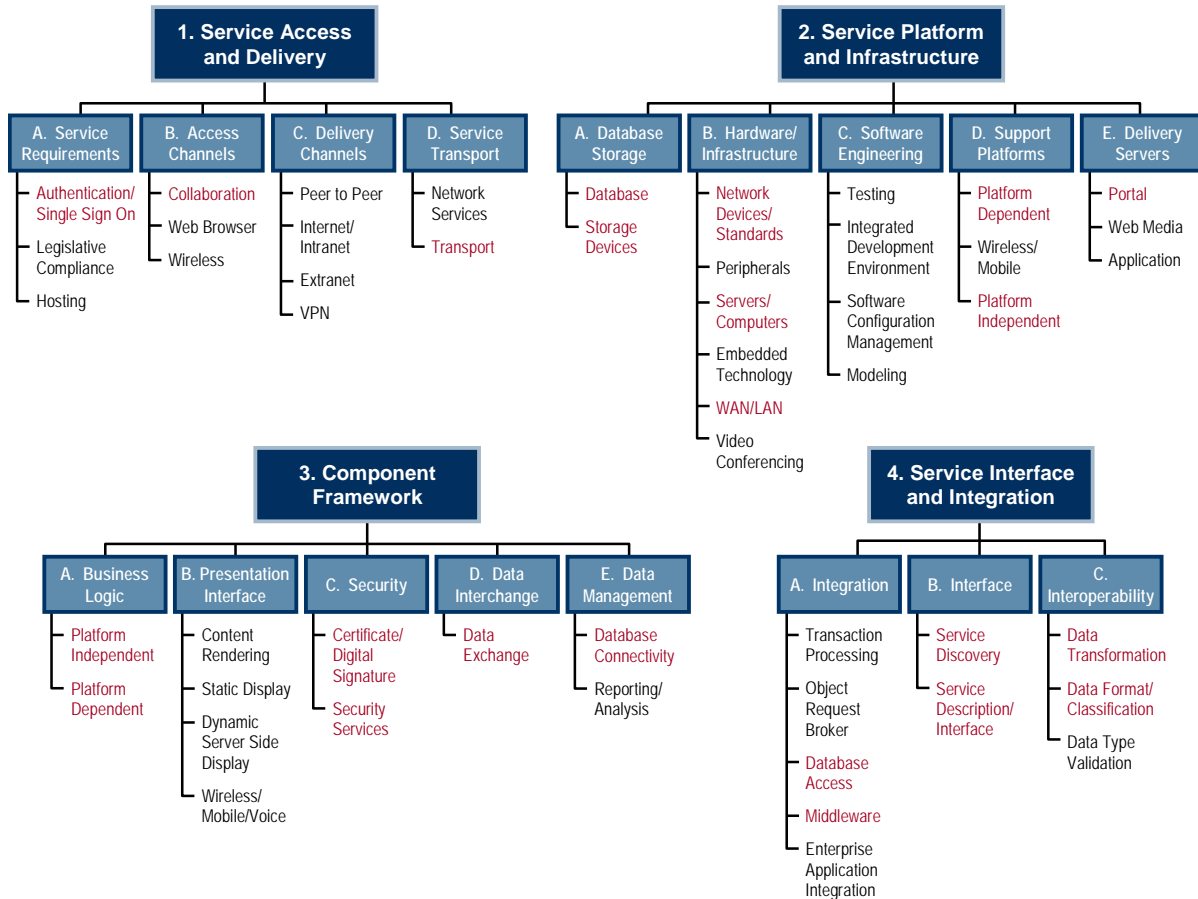


Figure 8-2. FEA Technical Reference Model

At the top level (blocks shown in blue), four Service Areas are represented:

1. Service Access and Delivery
2. Service Platform and Infrastructure
3. Component Framework
4. Service Interface and Integration

Each service area comprises several subordinate Service Categories. At the lowest level, each service category is supported by several standards/technologies. The service areas and service categories have been numbered in Figure 8-2 above.

The *ISE EAF* Technical Partition identifies technologies included in the FEA TRM that are applicable to the ISE, (indicated by red text). A number of components in the TRM are expected to be provided by ISE participants for integration with the ISE. Several examples include Web browser, wireless, mobile, and voice. The *ISE EAF* Technical Partition will also include technologies required by the ISE currently not inserted in the TRM. Table 8-1 shows the mapping of the high-priority ISE standards and technologies from the FEA TRM to the sections of the *ISE EAF* Technical Partition description.

Table 8-1. Technical Reference Model Mapping

Service Area	Service Category	Standard or Technology	Section # Herein
1	A	Authentication Single Sign-on	8.3
1	B	Collaboration	8.4
1	D	Transport	8.6
2	A	Database	8.7
2	A	Storage Devices	8.7
2	B	Network Devices/Standards	8.6
2	B	Servers/Computers	8.6
2	B	WAN/LAN	8.6
3	D	Data Exchange	8.5
3	E	Database Connectivity	8.7
4	A	Database Access	8.7
4	A	Middleware	8.3
4	B	Service Discovery	8.4
4	B	Service Description/Interface	8.4

SOA is an architectural paradigm shift and discipline that may be used to build infrastructures, enabling those with needs (consumers) and those with capabilities (providers) to interact via services across disparate domains of technology and ownership to service discovery and repurposing. Services act as the core facilitator of electronic data interchanges yet require additional mechanisms in order to function. Several new trends in the computer industry rely upon SOA as the enabling foundation. These include the automation of Business Process Management (BPM), composite applications (applications that aggregate multiple services to function), and the multitude of new architecture and design patterns generally referred to as Web 2.0.

Figure 8-3 illustrates a conceptual view of services and how a typical ISE participating organization/center would connect the internal and external environments. As shown in the figure, the ISE is divided into two spaces: the “External ISE” and the “Participant ISE Shared Spaces.” The external ISE includes the ISE Core and the ISE Shared Spaces of all other participating organizations. For SAR, AWN, and TWL, ISE Shared Spaces are defined as the places where SAR, AWN, and TWL data records would be deposited for access by ISE participants.

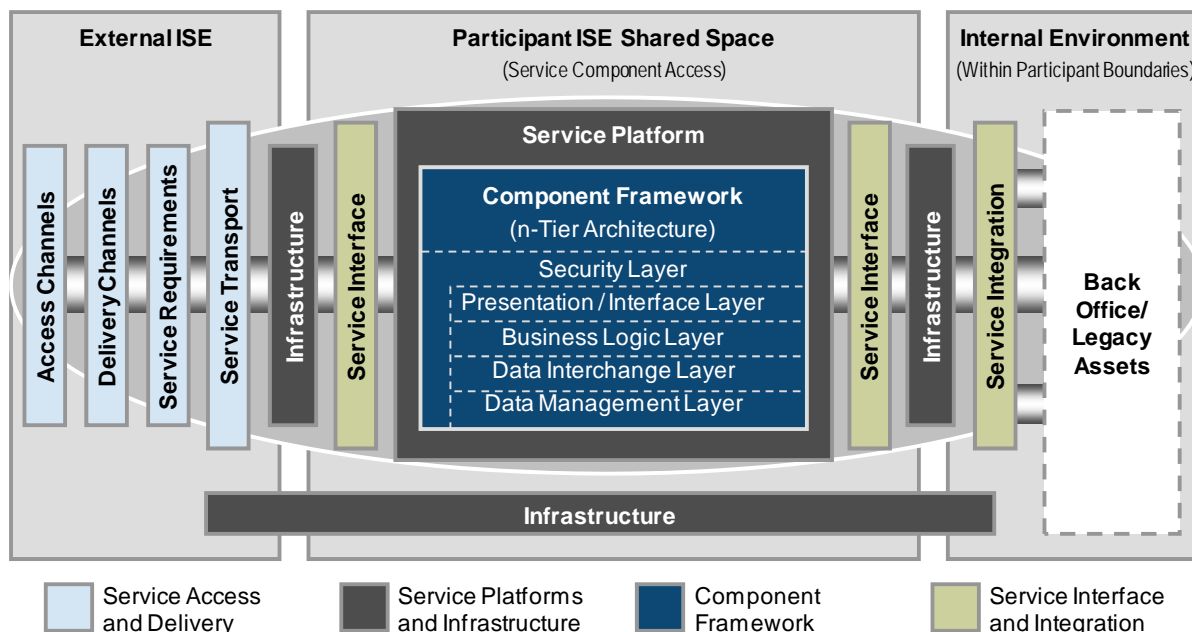


Figure 8-3. Conceptual View of Typical Participant Connection to the ISE

The technical perspective of Figure 8-3 is illustrated in Figure 8-4 wherein the Technical View captures the technology needed to support the conceptual view in two strategic aspects:

First view reflects the potential emerging technologies and standards that are considered to be the best suited to support the ISE. This is an integration of multiple independent networks and platforms into a seamlessly complex technical environment driven by the need to share nexus terrorism information within the ISE. It is composed of a wide and diverse range of technical paradigms that includes networks, communications, and various infrastructure resources.

Second view provides the guidance for implementing these technologies and how to apply and identify these technologies within the SOA landscape.

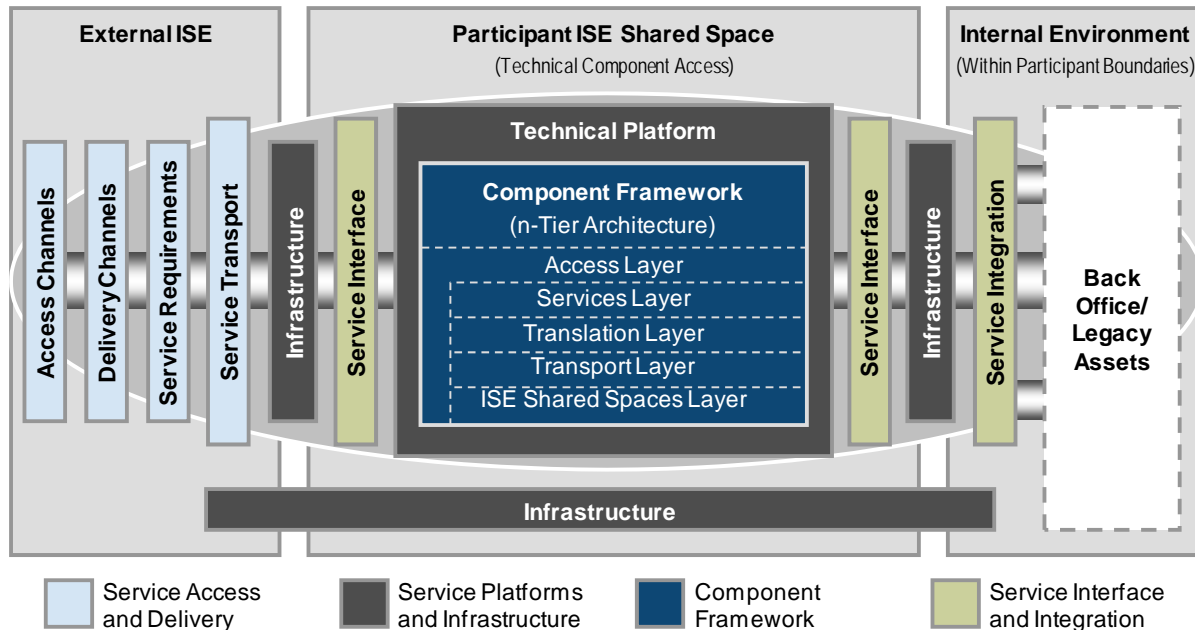


Figure 8-4. Technology View of Participant ISE Shared Space

8.3 Access Layer

This gateway could be aligned with each ISE participant's IT network, or portal. The portal has multiple accessible hyperlinks nested within access Universal Request Linkages (URL) known as "links." These links are capable of enabling a dynamic and efficient "Access" to various informational sites within the ISE once authenticated. The portal platform provides the interoperability required to cross multiple ISE participants' security domains. This technology also contains system log files that collect navigational activity during an "Access" session within the ISE. This is an auditable service that supports Information Security and Assurance and other areas of system security as specified in other sections of this document.

Identity and Access Management Framework – The Identity and Access Management (IdAM) Framework portion of "Access" is a secure and operational technical guideline. The IdAM is a framework that provides common methodology and conceptual guidelines to facilitate the governance and assurances required to manage the "Identity" authentication and the "Access Management" authorization for multiple participants within the ISE. The IdAM Framework leverages the existing and ongoing IdAM initiatives in the ISE to define overarching IdAM Framework guidance for the ISE to adopt.

The technological aspect of the IdAM guidance would include, but not be limited to, an "Access" management policy server used for "Attribute" authorization. It would be supported by business roles and Lightweight Directory Access Protocol (LDAP), a standard for global directory service technology that uses what is called a "Simple Authentication and Security Layer" (SASL) and encryption via "Secure Sockets Layer"

(SSL) technologies to support “Identity” management authentication. Both IdAM components contain log files or tables that enable the capture of authentication and authorization information used for information security and assurance purposes also in addition to access privileges.

8.4 Services Layer

This area of the ISE technology model defines the various types of technological components, appliances, “Best Practices,” and CTISS Technical Standards that would enable a SOA landscape. This landscape is a loosely coupled yet integrated architectural technical paradigm that supports the capability of shareable IT networks, infrastructure resources, and Web services across an enterprise or multiple ISE participants’ independent networks and enclaves (i.e., IC, DoD, DHS, and SLT).

The emerging technology that facilitates the sharing of IT services and resources is a key enabler that supports the ISE Core Services categories: Discovery, Mediation, Messaging, Enterprise Service Management, and Collaboration described in the ISE Core Services section of this document

The technologies that are considered to be fundamental SOA industry standards and “Best Practices” are

Web Service Manager (WSM) – Monitors and manages the inventory of Web services and their activity across the enterprise network for their reliance of efficient execution. The WSM manages the orchestration of Web services based on interdependences and services relationships. As part of the technical infrastructure, it uses and manages the Web service catalogs and registries’ infrastructure components. As part of the monitoring feature, the WSM maintains log files to record services activity, which could be a component of information assurance and network auditing.

Service Governance – Controls the accessibility and the execution of Web services based on IT service governance policies and role-based attributes that are part of the requestor profile for the messaging delivery. This capability also supports the security aspect of ISE Core Services as well as information assurance enforcement and access management.

8.5 Translation Layer

In this area of the technology model, the translation layer instantiates some of the fundamental infrastructure resources of a service oriented landscape, i.e., key resources used by Web services, data integration, and WSM to construct XML documents, interpret information messaging, and incorporate governance policy at the services level.

Service Level Agreement (SLA) Registry –an infrastructure resource used by the WSM to enforce existing business IT operational governance policy within an enterprise

informational sharing environment. It maintains the SLA's agreements between a designated "Community of Interest" concerning specific Web services or a set of services within the SOA landscape.

The SLAs control the accessibility to infrastructure services ranging from the unit level or group level within departmental to geographical locations throughout the world solely based upon "Access" agreements stated within the SLAs. Ideally, if the information requestors do not possess the required attributes that associate them as ISE participants, they may be denied "Access" to use certain services because they do not have the appropriate credentials for access as stipulated in the language of the SLAs. This identification could be considered another form of providing information assurance.

Metadata Registry –an infrastructure resource that supports key functionality within the constructs of a service oriented environment consisting of

- An XML Registry, which is a central repository component that maintains and manages ISE XML Schema document templates that are partitioned by "Name Space," a method that is used to segment the XML schemas registry by various levels of organizational constructs within the ISE.
- The XML Registry is a resource used by ISE Core services Mediation and Discovery to identify the appropriate XML standard to use as a source to capture information based on the informational requirements that are aligned with the business service instantiated to respond to the request for information. It includes and ensures that the XML schema content captured is interpreted into a common vocabulary such as NIEM and UCORE supported by the CTISS Standards Program and other ISE "Community of Interest" (COI) working groups.

8.6 Transport Layer

This area of the *ISE EAF* technical model recognizes a primary component of the IT network that represents the actual physical to virtual connectivity required to move informational content and allow communication media through the ISE virtual network connectivity across multiple independent networks, inclusive of the capability to support a heterogeneous technical paradigm similar to the ISE.

Network Management (NM) – is a technology that provides several capabilities that are essential to managing IT network operations and performance while maintaining network stability and availability. NM includes supporting the interoperability and management of IT infrastructure components and services as required in the ISE.

The NM has the capability to provide visibility to IT network operability in regard to tracking, monitoring, and managing network traffic flow throughout the enterprise network. It controls the navigation of network traffic and services across the enterprise network to maintain a consistent flow of information throughout a virtual Wide Area Network (WAN) typology as required for a cross domain informational sharing environment.

The NM is capable of monitoring and managing a network server's availability. When a network server would drop off-line, the NM would divert traffic and re-initiate the server and bring it back on-line, thereby maintaining high availability of infrastructure resources within network operability.

The NM has the capability to capture IT network operational information in log files, which is a network resource that serves multiple purposes such as reflecting network inefficiencies of performance because of improper configuration of network components or scalability. Information Assurance confirms the delivery of information and the execution of services across the network.

8.7 ISE Shared Spaces Layer

This area of the *ISE EAF* Technical Partition identifies the various Data Access (DA) technologies capable of supporting enhanced interoperability and accessibility requirements needed for a heterogeneous data network environment that may reside across multiple IT platforms.

Data Integration – In general, the data integration technology is a service oriented multi-threaded network appliance⁷² that is capable of managing and integrating the access to shareable data resources within the ISE Shared Spaces for ISE mission areas TWL, SAR, and AWN.

The data Integration appliance provides the capability to seamlessly integrate shared database resources across multiple IT platforms in a heterogeneous environment.

8.8 Technological Best Practices

This section recognizes IT considered to be “Best Practices” to instantiate an efficient, robust, and agile enterprise and Wide Area Network (WAN) technological architecture similar to the virtual environment of the ISE.

Enterprise Service Bus (ESB) – Is an integration technology that provides the capability to bridge disparate independent IT networks and platforms via a messaging broker.

IT Change and System Configuration Management (CM) – this technology is a network appliance that is considered to be an IT infrastructure operational “Best Practice” that provides the capability to integrate IT administered change and CM control services across a virtual heterogeneous network platform environment similar to the ISE.

⁷² Network Appliance (NetApp) provides an integrated solution that enables storage, delivery, and management of network data and content to achieve your business goals.

Storage Management – technologies considered to be a required IT resource management approach that provides the capability to manage space allocation and consumption for an enterprise and virtual network of multiple data storage device platforms in a data network mode similar to the ISE. Within that concept, it also provides data retention services.

Business Analytics – analytical technologies considered to be a business decision appliance that can facilitate a work flow execution of information sharing across an enterprise or multiple IT security domains as a practice to disseminate information as well as the ability to analyze the ingestion of nexus terrorism information for the appropriate data storage.

Data Replication – technologies considered to be a data resource management method that provides the capability to service high demand accessibility to frequently requested informational resources.

Performance Management – scalability is a technological approach used to meet the high performance demands required by an integrated virtual ISE network environment. Here various types of technology such as Network Load Balancer, Server Clustering, and devices and routers are included as additional technical resources and are configured or consumed within the infrastructure to meet the network demand by the ISE.

Data Migration – technologies considered to be the best approach used to meet the needs of data cleansing and transformation when loading data into a repository for an ISE Shared Space. Data migration provides the ability to clean any erroneous data during the upload migration process; it can also transform data into the appropriate format as required by the data integration specification.

8.9 CTISS Program Technical Standards

The following constitutes those technical voluntary consensus standards to be followed primarily by ISE Implementation Agents in planning, implementing, and providing Core infrastructure to the ISE. ISE participants also ensure alignment of these technical standards with existing information technology standards for interfacing their own ISE Shared Space to the ISE Core. The table below provides the core transport technical standards identified for use within the ISE Core. It lists the standards by expanded Open System Interconnect (OSI) layer, (Transport, Network, Link, and Physical), standard (Standard), implementing authoritative body (Standards Body), and a brief description (Standards Description).

Table 8-2. CTISS Program Technical Standards

OSI Layer	Standard	Standards body	Standards Description
Transport	Transmission Control Protocol (TCP)	IETF	Provides reliable, in-order delivery of a stream of bytes, providing application suitability. (Basic)
	User Datagram Protocol (UDP)	IETF	Core protocol of the Internet Protocol suite that allows networked computers to send short messages sometimes known as datagrams (using Datagram Sockets) to one another. (Basic)
Network	Internet Group Management Protocol (IGMP)	IETF	Protocol used by IPv4 systems (hosts and routers) to report IP multicast group memberships to neighboring multicast routers. Version 3, dated Oct 2002.
	Ping (PING)	IETF	Computer network tool used to test whether a host is reachable across an IP network; also used to self test network interface card of the computer. (Basic)
	Distance Vector Multicast Router Protocol (DVMRP)	IETF	Interior gateway protocol; suitable for use within an autonomous system, but not between different autonomous systems. (Basic)
	Enhanced Interior Gateway Routing Protocol (EIGRP)	IETF	Advanced distance-vector routing protocol, with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router. (Basic)
	Intrazone Routing Protocol (IARP)	IETF	Protocol that proactively tracks local network connectivity; provides support for route acquisition and route maintenance. (Basic)
	Internet Control Message Protocol (ICMP)	IETF	Protocol used for host-to-host datagram service in a system of interconnected networks. (Basic)
	Interzone Routing Protocol (IERP)	IETF	Reactive routing protocol that tries to find a route only on demand. (Basic)
	Interior Gateway Routing Protocol (IGRP)	IETF	Protocol that provides robust routing within an autonomous system. (Basic)
	Internet Protocol Version 4 (IPv4)	IETF	Data-oriented protocol to be used on packet switched internetworks; best effort protocol, does not guarantee delivery. (Basic)
	Internet Protocol Version 6 (IPv6)	IETF	Network layer for packet-switched internetworks; much larger address space, allowing greater flexibility in assigning addresses. (Basic)
	Intermediate System to Intermediate System (IS-IS)	ITU	Protocol used by network devices (routers) to determine the best way to forward datagrams or packets through a packet-based network. (Basic)

OSI Layer	Standard	Standards body	Standards Description
	Open Shortest Path First (OSPF)	IETF	Hierarchical interior gateway protocol (IGP) for routing in Internet Protocol; used to calculate the shortest path tree inside each area. Version 3, dated 1999 (supports IPv6). Version 2, dated 1998 (supports IPv4).
	Protocol Independent Multicast - Sparse Mode (PIM-SM)	IETF	Protocol for efficiently routing to multicast groups that may span wide-area (WAN and inter-domain) internets. (Basic)
	Protocol Independent Multicast - Dense Mode (PIM-DM)	IETF	Primarily designed for routing to multicast LAN applications.(Basic)
	Dynamic Host Configuration Protocol (DHCP)	IETF	Protocol used by networked devices to obtain various parameters necessary to operate in an Internet Protocol (IP) network. (Basic)
	X.25 Layer 3	ITU	Used for packet switch data communication. (Basic)
	X.75 Layer 3	ITU	Defines interconnections between multiple X.25 networks. (Basic)
Link	Asynchronous Transfer Mode (ATM)	ITU	Cell relay, packet switching network, and data link layer protocol that encodes data traffic into small fixed-sized cells. (Basic)
	Ethernet	IEEE	Family of frame-based computer networking technologies for LANs. (Basic)
	Frame Relay	ITU	Efficient data transmission technique used to send digital information quickly and cheaply in a relay of frames to one or many destinations from one or many end-points. (Basic)
	Label Distribution Protocol (LDP)	IETF	Protocol that defines a set of procedures and messages by which one LSR informs another of the label bindings it has made. (Basic)
	Link Layer Discovery Protocol (LLDP)	IEEE	Vendor-neutral Layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network, dated May 2005. (Basic)
	LLDP - Media Endpoint Discovery	TIA	Protocol used to communicate between switch ports and endpoint devices, dated 2006. (Basic)
	Multiprotocol Label Switching (MPLS)	IETF	Provides unified data-carrying service for both circuit-based clients and packet-switching clients that provide a datagram service model; can be used to carry many different kinds of traffic. (Basic)
	Point-to-Point Protocol (PPP)	IETF	Protocol for connection over synchronous and asynchronous circuits; designed to work with numerous network layer protocols. (Basic)

OSI Layer	Standard	Standards body	Standards Description
	Point-to-Point Tunneling Protocol (PPTP)	IETF	Protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating VPN across TCP/IP-based data networks. (Basic)
	Serial Line Internet Protocol (SLIP)	IETF	Protocol used for communication between two machines previously configured for communication with each other. Modifies standard Internet datagram by appending a special "SLIP END" character to it; allows datagrams to be distinguished as separate. (Basic)
	Spanning Tree Protocol (STP)	IEEE	Protocol that ensures a loop-free topology for any bridged LAN. (Basic)
	X.25 Layer 2	ITU	Used for packet switch data communication. (Basic)
	X.75 Layer 2	ITU	Defines the interconnection of two X.25 networks. (Basic)
Physical	Generalized Multiprotocol Label Switching (GMPLS)	ITU	Enhances MPLS architecture by completely separating the control and data planes of various networking layers; enables a seamless interconnection and convergence of new and legacy networks. (Basic)
	Integrated Services Digital Network (ISDN)	ITU	Allows digital transmission of voice and data over ordinary telephone copper wires; typically provides a maximum of 128 kbit/s. (Basic)
	Plesiochronous Digital Hierarchy (PDH)	ITU	Technology used in telecommunications networks to transport large quantities of data over digital transport equipment. (Basic)
	RS-232	EIA	Standard that defines communication between a DTE (Data terminal equipment) and a DCE (Data Circuit-terminating Equipment). (Basic)
	RS-422	EIA	Provides for data transmission, using balanced or differential signaling, with unidirectional/non-reversible, terminated or non-terminated transmission lines, point to point, or multi-drop. (Basic)
	RS-485	EIA	Widely used communication interface in data acquisition and control applications where multiple nodes communicate with each other. (Basic)
	Synchronous Digital Hierarchy (SDH)	ITU	Standard technology for synchronous data transmission on optical media. (Basic)
	Synchronous Optical Network (SONET)	ITU	Network technology designed to carry large volumes of traffic over relatively long distances on fiber optic cabling. (Basic)
Application	Border Gateway Protocol (BGP)	IETF	Exchanges network reachability information with other BGP systems. (Basic)

OSI Layer	Standard	Standards body	Standards Description
	Real-Time Transport Protocol (RTP)	IETF	Protocol that provides end-to-end delivery services for data with real-time characteristics. (Basic)
	Real-Time Transport Control Protocol (RTCP)	IETF	Protocol that provides control for an RTP session. Particularly, it allows devices to exchange information about the quality of the media session, including such information as jitter, packet loss, and a host of other statistics. (Basic)
	Simple Network Management Protocol (SNMP)	IETF	Network management specification that provides standard, simplified, and extensible management of LAN-based internetworking products. (Basic)
	Secure Sockets Layer (SSL)	IETF	Provides privacy and reliability between two communicating applications. (version 0.9.8i, dated Sept 2008)
	Transport Layer Security (TLS)	IETF	Provides privacy and data integrity between two communicating applications. (Basic)
	Simple Object Access Protocol (SOAP)	W3C	Protocol intended for exchanging structured information in a decentralized, distributed environment. Version 1.1, dated April 2007. (Basic)

8.10 Technical Standards under Consideration

The IA and Core Transport technical standards identified in Table 8-2, and also in *ISE-G-106* and *ISE-G-107*, respectively, address technical standards currently in use by ISE participants. As ISE participants' use of their ISE Shared Spaces increases and the exchange of data evolve, it is anticipated additional IA and Core Transport technical standards may be added to the available suite of IA and Core Transport technical standards issued in *ISE-G-106* and *ISE-G-107*.

Table 8-3 identifies technical standards that may be considered for use in ISE Shared Spaces.

Table 8-3. ISE Technical Standards being Considered

Standards Categories	Standards Subcategories		Example Standard(s)
Metadata		Controlled Vocabulary	NIEM, CAPCO, Dublin Core, DDMS, FIPS Codes, ISO/IES 2382, IC Metadata Standard for Information Security (IC ISM), ISO 11179
		Information Exchange	NIEM, GJXDM, TWPDES, OMG Standards
Data		Encoding Formats	ASCII, audio/video/data storage standards, NIEM IEPD, DoD/IC U-Core, Unicode
	Exchange Protocols	Presentation	XDR, XHTML
Session		ISCSI, RPC, SQL	
Transport			
Network			
Data Link		Ethernet	
Physical		CAT-5	
Services		IA Services	Highly Available Enterprise
	Network Defense		DCID 6/3, DoDI 5229.40
	Management and Infrastructure		PKI v1.5, X.509, XKMS
	Service Based Architecture Foundation Services	Invocation	REST
		Metadata Management	WSDL, UDDI, WS-Addressing
		Messaging	WS-Eventing, WS-Notification
		Composable Service Elements	WS-Reliability, WS-Federation, WS-Trust, WS-Security
		Mediation/Translation	XSLT, Apache Synapse
		Process Orchestration	BPEL4WS, WS-CDL
		Management	WS-Manageability, WS-Provisioning
		Presentation	JSR-168, WSRP, AJAX

This page intentionally blank.

ISE Enterprise Architecture Framework

Version 2.0

September 2008



INFORMATION SHARING ENVIRONMENT ENTERPRISE ARCHITECTURE FRAMEWORK

APPENDICES

Prepared by the
Program Manager, Information Sharing Environment

This page intentionally blank.

INFORMATION SHARING ENVIRONMENT ENTERPRISE ARCHITECTURE FRAMEWORK, VERSION 2.0, APPENDICES

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

September 2008

This page intentionally blank.

TABLE OF CONTENTS

Appendix A – ISE EAF Acronym List.....A-1
Appendix B – ISE EAF GlossaryB-1
Appendix C – ISE Business Processes..... C-1
Appendix D – ISE SAR Information Flow Description D-1
Appendix E – ISE Identification and Screening Business Process Analysis:
 Terrorist Watchlist Component – June 2008E-1
Appendix F – ISE Alerts, Warning, and Notification Business Process Analysis –
 June 2008 F-1
Appendix G – ISE Shared Spaces and Core Discussion G-1

This page intentionally blank.

Appendix A – ISE EAF Acronym List

ADL	Architecture Description Language
AIC	Architecture and Infrastructure Committee
AM	Administration Memorandum
AJAX	Asynchronous JavaScript and XML
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
AWG	Architecture Working Group
AWN	Alerts, Warning, and Notification
BATS	Bomb Arson Tracking System
BGP	Border Gateway Protocol
BP	Business Process
BPA	Business Process Analysis
BPEL4WS	Business Process Execution Language for Web Services
BPM	Business Process Model
BPMN	Business Process Modeling Notation
BRM	Business Reference Model
C.F.R	Code of Federal Regulations
CAR	Chief Architects' Roundtable
CAPCO	Controlled Access Program Coordination Office
CBP	Customs and Border Protection
CC	Continuity Communications
CDD	Capability Development Document
CDL	Choreography Description Language
CES	Core Enterprise Service
CIO	Chief Information Officer
CLASS	Consular Lookout and Support System
CM	Configuration Management
CNSS	Committee on National Security Systems
COI	Community of Interest
CONS	Connection Oriented Network Service
COOP	Continuity of Operations Planning
CPD	Capability Production Document
CPIC	Capital Planning and Investment Control

CRL	Certificate Revocation List
CRM	Consolidated Reference Model
CSG	Counterterrorism Support Group
CT	Counterterrorism
CTISS	Common Terrorism Information Sharing Standard
CUI	Controlled Unclassified Information
CVS	Certificate Validation Service
CWIN	Critical infrastructure Warning Information Network
DA	Data Access
DCID	Director Central Intelligence Directive
DCMI	Dublin Core Metadata Initiative
DDMS	DoD Discovery Metadata Specification
DHS	Department of Homeland Security
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNI	Director of National Intelligence
DOC	Department of Commerce
DoD	Department of Defense
DODI	Department of Defense Instruction
DOE	Department of Energy
DOI	Department of Interior
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DOTreas.	Department of Treasury
DRM	Data Reference Model
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
EAI	Enterprise Application Integration
ebXML	Electronic Business using XML
EDS	Electronic Directory Services
EE	Evaluation Environment
EGOV	Electronic Government
EI	Enterprise Integration

EMA	Encounter Management Application
EO	Executive Order
EPA	Environment Protection Agency
ESB	Enterprise Service Bus
ESM	Enterprise Services Management
FAQ	Frequently Asked Questions
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FIG	Field Intelligence Group
FISMA	Federal Information Security Management Act
FIPS	Federal Information Processing Standards
FS	Functional Standard
FTF-C	Federal Transition Framework Catalog
GAO	Government Accountability Office
GIG	Global Information Grid
GJXDM	Global Justice Exchange Data Model
HAIBE	High Assurance Internet Protocol Encryption
HHS	Department of Health and Human Services
HLS	Homeland Security
HSDN	Homeland Secure Data Network
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAFIS	Integrated Automated Fingerprint Identification System
IC	Intelligence Community
ICD	Interface Control Document
ICE	Immigration and Customs Enforcement
ID	Identification/Identifier
IdAM	Identity and Access Management
IDE	Integrated Development Environment

IDENT	Automated Biometric Identification System
IDS	Intrusion Detection System
IDW	Investigative Data Warehouse
IEP	Information Exchange Package
IEPD	Information Exchange Package Document/Documentation
IICT	Interagency Intelligence Committee on Terrorism
ILC	Implementation Life Cycle
IMP	ISE Management Portal
IOC	Initial Operating Capability
IP	Internet Protocol
IPS	Intrusion Prevention System
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
IS	Information Sharing
ISC	Information Sharing Council
ISDN	Integrated Services Digital Network
ISE	Information Sharing Environment
ISEA	Information Sharing Environment Architecture
ISE-G	Information Sharing Environment Guidance
ISM	Information Security Markings
ISO	International Organization for Standardization
ISO/IES	International Organization for Standardization /Information Exchange Standards
ISP	Internet Service Provider
ISSA	Information Sharing Segment Architecture
IT	Information Technology
ITACG	Interagency Threat Assessment Coordinating Group
JPEG	Joint Photographic Experts Group
JSR	Java Specification Request
JTF	Joint Task Force
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
JXDM	Justice XML Data Model
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LE	Law Enforcement
LoB	Line of Business

MDA	Maritime Domain Awareness
MWG	MetaData Working Group
NCS	National Communication System
NCCC	National Command and Coordination Capability
NCES	Net-Centric Enterprise Services
NCID	Net-Centric Implementation Document
NCTC	National Counterterrorism Center
NDR	Naming and Design Rules
NEF	National Essential Functions
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIPC	National Infrastructure Protection Center
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NM	Network Management
NOC	Network Operations Center
NSA	National Security Agency
NSC	National Security Council
NSIS	National Strategy for Information Sharing
NSPD	National Security Presidential Directive
OASIS	Organization for the Advancement of Structured Information Standards
OMB	Office of Management and Budget
ORB	Object Request Broker
OSI	Open System Interconnect
OWL	Web Ontology Language
PART	Program Assessment Rating Tool
PDD	Presidential Decision Directive
PDS	Policy Decision Service
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
PM	Program Manager
PAIS	Profile and Architecture Implementation Strategy
PGFSOA	Program Guidance Framework for Service Oriented Architecture
PM-ISE	Program Manager - Information Sharing Environment

PMO	Program Management Office
POAM	Plan of Action and Milestones
PoAS	Policy Administration Service
PPP	Point-to-Point Protocol
PrAS	Principal Attribute Service
PRM	Performance Reference Model
PRS	Policy Retrieval Service
QA	Quality Assurance
QoS	Quality of Service
REST	Representation State Transfer
RM	Reference Model
RMF	Risk Management Framework
S	Secret (Security Classification)
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAR	Suspicious Activity Reporting
SASL	Simple Authentication and Security Layer
SBU	Sensitive but Unclassified (Security Classification)
SCI	Special Compartmented Information (Security Classification)
SCM	Software Configuration Management
SIMAS	Security Incident Management and Analysis System
SIOC	Security Intelligence and Operation Center
SIPRNet	Secret Internet Protocol Router Network
SIR	Suspicious Incident Report
SLA	Service Level Agreement
SLIP	Serial Line Internet Protocol
SLT	State, Local, and Tribal
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOAF	Service-Oriented Architecture Foundation
SOAP	Simple Object Access Protocol
SONET	Synchronous Optical Network
SOP	Standard Operating Procedures
SRM	Service Reference Model

SSL	Secure Socket Layer
SVTC	Secure Video Teleconference Capability
TCP	Transmission Control Protocol
TIDE	Terrorist Identity Datamart Environment
TLS	Transport Layer Security
TRM	Technical Reference Model
TS	Top Secret (Security Classification)
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TTL	time-to-live
TWL	Terrorist Watchlist
TWPDES	Terrorist Watchlist Person Data Exchange Standard
UCORE	Universal Core
UDDI	Universal Description, Discovery, and Integration
UDP	User Datagram Protocol
UML	Unified Modeling Language
UNIX	Uni-plexed Information and Computing System
URI	Uniform Resource Identifier
URL	Universal Request Linkage
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network
WG	Working Group
WS	Web Services
WSDL	Web Services Description Language
WS-I	Web Services Interoperability
WSM	Web Service Manager
WSRP	Web Services for Remote Portals
XACML	Extensible Access Control Markup Language
XKMS	XML Key Management Specification
XML	Extensible Markup Language

XPath	XML Path Language
XSD	XML Schema Definition
XSLT	Extensible Style Sheet Language Transformation
XSTF	XML Structure Task Force

Appendix B – ISE EAF 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 Transport—That infrastructure (including cabling, network components, and protocols) that enables the movement of data within a domain and between agencies participating in the ISE.

Agency—Has the meaning set forth for the term “executive agency” in section 105 of title 5, United States Code (i.e., an Executive department, a Government corporation, and an independent establishment), together with the Department of Homeland Security, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office. [E.O. 13388 Section (6)(a) and 5 U.S.C. 105]

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

Application Architecture—The high-level design which defines the major components of a software application, the information that flows between those components, and the transformations that those components apply to that information.

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.

Audit Trail Capture and Analysis—Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

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 Analytical Services—supports “the extraction, aggregation, and presentation of information to facilitate decision analysis.”

[http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v20_Final_June_2006.pdf]

Business Architecture—An inventory of agency business processes, aligned to the FEA Business Reference Model (BRM), linked to layers of the agency EA and used to inform investment decision making.

[http://www.whitehouse.gov/omb/egov/documents/OMB_EA_Assessment_Framework_2_FINAL.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_v20_Final_June_2006.pdf]

Common Services—In a service-oriented architecture, Web services are divided into two broad categories: Line of Business Services and Common Services. Common services are those services employed by a large subset of users. These services are provided centrally by an enterprise authority to assure interoperability and maximize reuse.

Community of Interest (COI)—COI are defined in the National Information Exchange Model (NIEM) CONOPS, October 2004, as a collaborative group of users who require a shared vocabulary to exchange information in pursuit of common goals, interests, and business objectives.

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)—Plan 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 that require controls that protect it from public release, both to safeguard the civil liberties and legal rights of U.S. citizens, and to deny information advantage to those who threaten the security of the nation.

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.

[http://www.nces.dod.mil/aboutNCES/glossary_content.aspx]

Cross-Agency Initiative—An effort supported with resources (including staff, products, information, and/or funding) from multiple Federal agencies for the mutual benefit of all.

Cross-Domain Security—An integrated, comprehensive, and consistent approach to addressing the shared risk associated with the connection of networks of different classification levels. [<http://ia.gordon.army.mil/iaso/Army/AR25-2/main.htm>]

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 and tagged with metadata to enable access to all users except when limited by security, policy, or regulations.

Data Context—Any information that provides additional meaning to data. Data Context typically specifies a designation or description of the application environment or discipline in which data is applied or from which it originates. It provides perspective, significance, and connotation to data, and is vital to the discovery, use, and comprehension of data.

[http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Description—A rich description of data, thereby supporting its discovery and sharing. [http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data 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. [<http://en.wikipedia.org/wiki/Interoperability#Software>]

Data-in-Transit—Data is typically referred to as being in one of three states at any time: (1) at rest, (2) processing, or (3) in transit. Data-in-Transit refers to the state when data is being passed from one physical location to another via the ISE Transport. Data is in transit when it is passing over physical cables, being transmitted over wireless networks and satellite links, and passing through routers and other network components.

Data Reference Model—One of the five reference models of the Federal Enterprise Architecture (FEA). The DRM is a framework whose primary purpose is to enable information sharing and reuse across the Federal Government via the standard description and discovery of common data and the promotion of uniform data management practices.

[http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Sharing—Describes the sharing and exchange of data, where sharing may consist of ad-hoc requests (such as a one-time query of a particular data asset), scheduled queries, and/or exchanges characterized by fixed, reoccurring transactions between parties. It involves exchanges within and between agencies and COIs to support mission-critical capabilities. Finally, it eliminates duplication and/or replication of data, thereby increasing data quality and integrity.

[http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Trustability—those functional capabilities of the ISE that enable a user to place a value on specific data provided in the ISE. In particular, Data Trustability depends on the principle that data shall be tagged with metadata describing its pedigree, source, timeliness, confidence, or other attributes associated with trust.

Data Understandability—The functional capabilities of the ISE that enable a user to properly interpret specific data and use that data in an appropriate manner. In particular Data Understandability depends on the principle that data shall be tagged with metadata describing its pedigree, source, timeliness, and perhaps description. Even more important, however, is that data be described in standard ways using common terminology as established by negotiated and accepted taxonomies.

Data Visibility—The functional capabilities of the ISE that reveal the existence of specific data to a user of the ISE. In particular, Data Visibility depends on the principles that all data shall be posted to shared spaces and tagged with metadata to enable discovery of data by users.

Detailed ISE SAR IEPD: Technical artifacts (data model, data schema, and reference vocabulary) in the ISE-SAR Functional Standard providing descriptions and relationships of all SAR data that may be exchanged, including data tagged elements (using metadata markup technology) requiring protection under privacy laws and regulations (designated as privacy fields or privacy information). In the Detailed ISE SAR IEPD all 189 data fields can be made available by data owner to external users.

Digital Signature—Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. Synonymous with electronic signature.
[\[http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf\]](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf)

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.

Domain Routing—The functionality that allows data to cross domain borders. For example, data may be routed from a Secret domain to a Sensitive But Unclassified domain through a trusted guard that enables specified policies for the declassification of information. In the near term, a routing protocol domain boundary will be established at these administrative domain boundaries.
[\[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/d12.htm\]](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/d12.htm)

Enabling Technology—Any technological capability used to support ISE policies or business processes.

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

Enterprise Architecture—A strategic information asset base, which defines the mission, the information necessary to perform the mission and the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. [Endorsed definition from the Federal CIO Council]

Enterprise Search—The act of searching content to discover data, information, and knowledge wherever it exists.

Extensible Markup Language (XML)—XML is a simple, very flexible text format derived from Standard Generalized Markup Language (SGML). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing 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, services, data, and technology).

Federations—Federations are legally autonomous/sovereign Enterprises that agree to Federation (Self-Regulation) rules whereby they establish and maintain trust amongst themselves.

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 local governments designed to coordinate the gathering, analysis, and dissemination of law enforcement, public-safety, and terrorism information.

Global Information Grid (GIG)—Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel. [http://www.nces.dod.mil/aboutNCES/glossary_content.aspx]

Homeland Security Information—Any information possessed by a Federal, state, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act. [Section 892(f)(1) of the Homeland Security Act (6 U.S.C. 482(f)(1))]

Identity Management—The combination of technical systems, rules, and procedures that define the ownership, utilization and safeguarding of personal identity information.

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)] E.O. 13388, which superseded E.O. 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)]

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]

Intelligence Community Enterprise Architecture (ICEA)—Establishes the interoperability framework between the organizational/mission enterprise architecture necessary to support the business of intelligence.

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; however, prevent intrusion from occurring.

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 that participates in the ISE.

ISE Transport—That infrastructure (including cabling, network components, and protocols) that enables the movement of data between agencies participating in the ISE (synonymous with Agency Transport).

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.

Line Business—Internal operations of the federal government and its services, independent of the agencies that perform them.

http://www.whitehouse.gov/OMB/egov/documents/DRM_2_0_Final.pdf

Local Government—Means (A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity. [Homeland Security Act of 2002, 6 U.S.C. 101]

National Information Exchange Model (NIEM)—An interagency initiative to provide the foundation and building blocks for national-level interoperable information sharing and data exchange. <http://www.niem.gov/aboutniem.php>

Net-centricity—Robust networks without central weakness versus centralized chains that can be cut or broken. Interoperable communications versus “stove-piped” communications infrastructure. Dynamic-situational security versus fixed-domain specific-security. Pull assured information versus push information out. Only handle

information once versus duplicate entries.

[\[http://www.nces.dod.mil/aboutNCEs/glossary_content.aspx\]](http://www.nces.dod.mil/aboutNCEs/glossary_content.aspx)

Non-repudiation—Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. [\[http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf\]](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf)

Outcome Measures—Outcomes describe the intended result of carrying out a program or activity. They define an event or condition that is external to the program or activity and that is of direct importance to the intended beneficiaries and/or the public.
[OMB A 11]

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

Program Manager—Means the program manager designated under subsection 1016(f) of the IRTPA, who is responsible for information sharing across the Federal Government and shall, in consultation with the Information Sharing Council, plan for and oversee the implementation of, and manage, the ISE. [Extracted from IRTPA 1016(a) (3) and 1016(f)]

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

Role/Privilege Management—Set of functions that protect networks and systems from unauthorized access by persons, acts, or influences and includes many sub-functions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges.

Security Domain—the term "Security Domains" refers to three security levels—Special Compartmented Information (SCI), Secret/Collateral, and Controlled Unclassified Information (CUI)/Sensitive but Unclassified (SBU)—across which the ISE must operate.

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 Adaptation—Solves the problem of converting between the rules used by one service into that required by another while maintaining the integrity of the message being sent through the SOA.

[\[http://www.nces.dod.mil/coreServices/mediation_content.aspx\]](http://www.nces.dod.mil/coreServices/mediation_content.aspx)

Service Level Agreement (SLA)—SLA defines mutual understandings and expectations of the Web 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.

[\[http://www.nces.dod.mil/aboutNCEs/glossary_content.aspx\]](http://www.nces.dod.mil/aboutNCEs/glossary_content.aspx)

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.

Shared Data—The terrorism data collected and maintained by agencies in the course of executing their mission.

Simple Object Access Protocol (SOAP)—SOAP Version 1.2 is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. The “Messaging Framework” component defines, using XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols.

[\[http://www.w3.org/TR/soap12-part1/\]](http://www.w3.org/TR/soap12-part1/)

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]

Summary ISE SAR Information: Summary ISE SAR Information is derived from the technical artifacts from the "Detailed ISE SAR IEPD", but the viewable information has the privacy fields stripped from any results.

Suspicious Activities Report (SAR)—Suspicious activity is defined as; “behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal espionage, or other illicit intention. A SAR consolidates information recorded by observers of suspicious activity providing the identification of patterns, trends, or nationally suspicious activities beyond what would be recognized within a single jurisdiction, state, or territory.

Technical Architecture—This component characterizes hardware, operating systems, programming, and network solutions used across the ISE.

Technical Reference Model—A component-driven, technical framework used to categorize the standards, specifications, and technologies that support and enable the delivery of service components and capabilities. The TRM provides a foundation to categorize the standards, specifications, and technologies to support the construction, delivery, and exchange of business and application components that may be used and leveraged in a Component-Based or Service-Oriented Architecture. It also unifies existing agency TRMs and Electronic Government (EGOV) guidance by providing a foundation to advance the re-use of technology and component services from a government-wide perspective.

[\[http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf\]](http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf)

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, or United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals. [IRTPA 1016(a) (4)]

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

Universal Description, Discovery and Integration (UDDI)—The UDDI protocol is one of the major building blocks required for successful Web services. UDDI creates a standard interoperable platform that enables companies and applications to quickly, easily, and dynamically find and use Web services over the Internet. UDDI also allows operational registries to be maintained for different purposes in different contexts.

[\[http://www.uddi.org/about.html\]](http://www.uddi.org/about.html)

User Applications—Software applications used by one or more ISE user communities wishing to leverage the capabilities of the ISE. User Applications is in contrast to Enterprise Applications, which are used by a large subset of ISE users and provided centrally, or Management Applications, which are used by a small set of administrators to maintain and operate the ISE.

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 thanks to the use of 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 Description 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>]

Web Services Interoperability (WS-I)—WS-I creates, promotes and supports generic protocols for the interoperable exchange of messages between Web services. In this context, “generic protocols” are protocols that are independent of any action indicated by a message, other than those actions necessary for its secure, reliable and efficient delivery, and “interoperable” means suitable for multiple operating systems and multiple programming languages. [<http://www.ws-i.org/about/Default.aspx>]

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 C – 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	Reports observed behavior that maybe indicative of intelligence gathering or pre-operational planning related to terrorism, criminal espionage, and other illicit information.
Identification and Screening	Supports the counterterrorism (CT) community efforts to identify and screen personnel and material. This 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 effort 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 LE 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 dissemination 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 Alert and Warnings 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 link-ability 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	Ensure that the sharing environment accords 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 SBU and classified terrorism information.) Removes impediments to ISE clearances and visit handling, leverages C&A 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 ISE.
ISE Governance and Management	Ensure that ISE governance process functions effectively and efficiently. This category includes processes that support ISE budgeting, auditing, and quality assurance.

This page intentionally blank.

Appendix D – ISE SAR Information Flow Description

Step	Activity	Process	Notes
1	Observation	The process begins when a person or persons observe unusual behavior. Such activities could include, but are not limited to, surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, possible testing of security or security response, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemical/agents or toxic materials, or other unusual behavior or sector-specific incidents. ¹	The observer may be a private citizen, a government official, or a law enforcement officer.
2	Initial Response and Investigation	<p>An official of a Federal, State, or local agency with jurisdiction responds to the reported observation.² This official gathers additional facts through personal observations, interviews, and other investigative activities. In the context of priority information requirements, as provided by State and major urban area fusion centers, the officer/agent may use a number of fact based systems to continue the investigation. These fact based systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of fact based systems and the information they may provide include:</p> <ul style="list-style-type: none"> • Department of Motor Vehicles provides drivers license and vehicle registration information; • National Crime Information Center provides wants and warrants information, criminal history information and access to the Terrorist Screening Center and the terrorist watch list, and Violent Gang/Terrorism Organization File (VGTOF); and, • Other Federal, State, and local systems can provide criminal checks within the immediate and surrounding jurisdictions. <p>When the initial investigation is complete, the official documents the event. The report becomes the initial record for the law enforcement or Federal agency's records management system (RMS).</p> <p>The records may be hard and/or soft copy and does not yet constitute an ISE-SAR.</p>	The event may be documented using a variety of reporting mechanisms and processes, including but not limited to, reports of investigation, event histories, field interviews (FI), citations, incident reports, and arrest reports.

1 Suspicious activity reporting (SAR) is an official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism.

2 If a suspicious activity has a direct connection to terrorist activity the flow moves along an operational path. Depending upon urgency, the information could move immediately into law enforcement operations and lead to action against the identified terrorist activity. In this case, the suspicious activity would travel from the initial law enforcement contact directly to the law enforcement agency with enforcement responsibility.

Step	Activity	Process	Notes
3	Local/Regional Processing	<p>The agency processes and stores the information in the RMS following agency policies and procedures. The flow will vary depending on whether the reporting organization is a State or local agency or a field element of a Federal agency.</p> <p>State and local: Based on specific criteria or the nature of the activity observed, the State or local law enforcement components forward the information to the State or major urban area fusion center for further analysis.</p> <p>Federal: Federal field components collecting suspicious activity would forward their reports to the appropriate resident, district, or division office. This information—still only fact information—would be reported to field intelligence groups or headquarters elements through processes that vary from agency to agency.</p> <p>In addition to providing the fact information to its headquarters, the Federal field component would provide an information copy to the State or major urban area fusion center in its geographic region. This information contributes to the assessment of all suspicious activity in the State or major urban area fusion center's area of responsibility.</p>	<p>The State or major urban area fusion center should have access to all suspicious activity reporting in its geographic region whether collected by SLT or Federal field components.</p>
4	Creation of an ISE-SAR	<p>The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria may have a nexus to terrorism.</p> <p>Once this determination is made, the information becomes an "ISE-SAR" and is formatted in accordance with ISE-FS-200 (ISE-SAR Functional Standard). The ISE-SAR would then be shared with appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.</p> <p>For State, local, and tribal law enforcement, the ISE-SAR information, may be fact information or criminal intelligence and is handled in accordance with 28 CFR Part 23. It may be shared with State or Federal law enforcement personnel with the privacy field included.</p>	<p>Some of this information may be intelligence, which identifies trends and other terrorist related information and is derived from Federal agencies such as NCTC, DHS, and the FBI.</p>
5	ISE-SAR Sharing and Dissemination	<p>In a State or major urban area fusion center, the ISE-SAR is shared with the appropriate FBI field components and the DHS representative and placed in the State or major urban area fusion center's ISE Shared Spaces or otherwise made available to members of the ISE.</p> <p>The FBI field component enters the ISE-SAR information into the FBI system and sends the information to FBI Headquarters.</p>	

Step	Activity	Process	Notes
6	Federal Headquarters (HQ) Processing	<p>At the Federal headquarters level, ISE-SAR information is combined with information from other State or major urban area fusion centers and Federal field components and incorporated into an agency-specific national threat assessment that is shared with ISE members.</p> <p>The DHS representative enters the ISE-SAR information into the DHS system and sends the information to DHS, Office of Intelligence Analysis.</p> <p>The ISE-SAR information may be provided to NCTC in the form of an agency-specific strategic threat assessment (e.g., strategic intelligence product).</p>	<p>When a State or local originated ISE-SAR is in the Federal system, the rules of sharing are no longer governed by 28 CFR Part 23, but rather by appropriate Federal privacy laws and guidelines.</p>
7	NCTC Analysis	<p>When product(s) containing the ISE-SAR information are made available to NCTC, they are processed, collated, and analyzed with terrorism information from across the five communities—intelligence, defense, law enforcement, homeland security, and foreign affairs—and open sources.</p> <p>NCTC has the primary responsibility within the Federal government for analysis of terrorism information. NCTC produces federally coordinated analytic products that are shared through NCTC Online, the NCTC secure web site.</p> <p>The Interagency Threat Assessment and Coordinating Group (ITACG), housed at NCTC, facilitates the production of coordinated terrorism-related products that are focused on issues and needs of State, local, and tribal entities and when appropriate private sector entities. ITACG is the mechanism that facilitates the sharing of counterterrorism information with SLT.</p>	
8	NCTC Alerts, Warnings, Notifications	<p>NCTC products³, informed by the ITACG as appropriate, are shared with all appropriate Federal departments and agencies and with SLT through the State or major urban area fusion centers. The sharing with SLT and private sector occurs through the Federal departments or agencies that have been assigned the responsibility and have connectivity with the State or major urban area fusion centers. Some State or major urban area fusion centers, with secure connectivity and an NCTC Online account, can access NCTC products directly. State or major urban area fusion centers will use NCTC and ITACG informed products to help develop geographic-specific risk assessments (GSRA) to facilitate regional counterterrorism efforts. The GSRA are shared with SLT organizations and the private sector as appropriate. The recipient of the GSRA may use the GSRA to develop information gathering priorities or requirements.</p> <p>NCTC products should be responsive to informational needs of State, local, and tribal entities.</p>	<p>NCTC products form the foundation of informational needs and guide collection of additional information.</p>

³ NCTC product include: Alerts, warnings, and notifications—identifying time sensitive or strategic threats; Situational awareness reports; and Strategic and foundational assessments of terrorist risks and threats to the United States and related intelligence information.

Step	Activity	Process	Notes
9	Focused Collection	The information has come full circle and the process begins again, informed by an NCTC or other Federal organization's product and the identified information needs of State, local and tribal entities and Federal field components.	

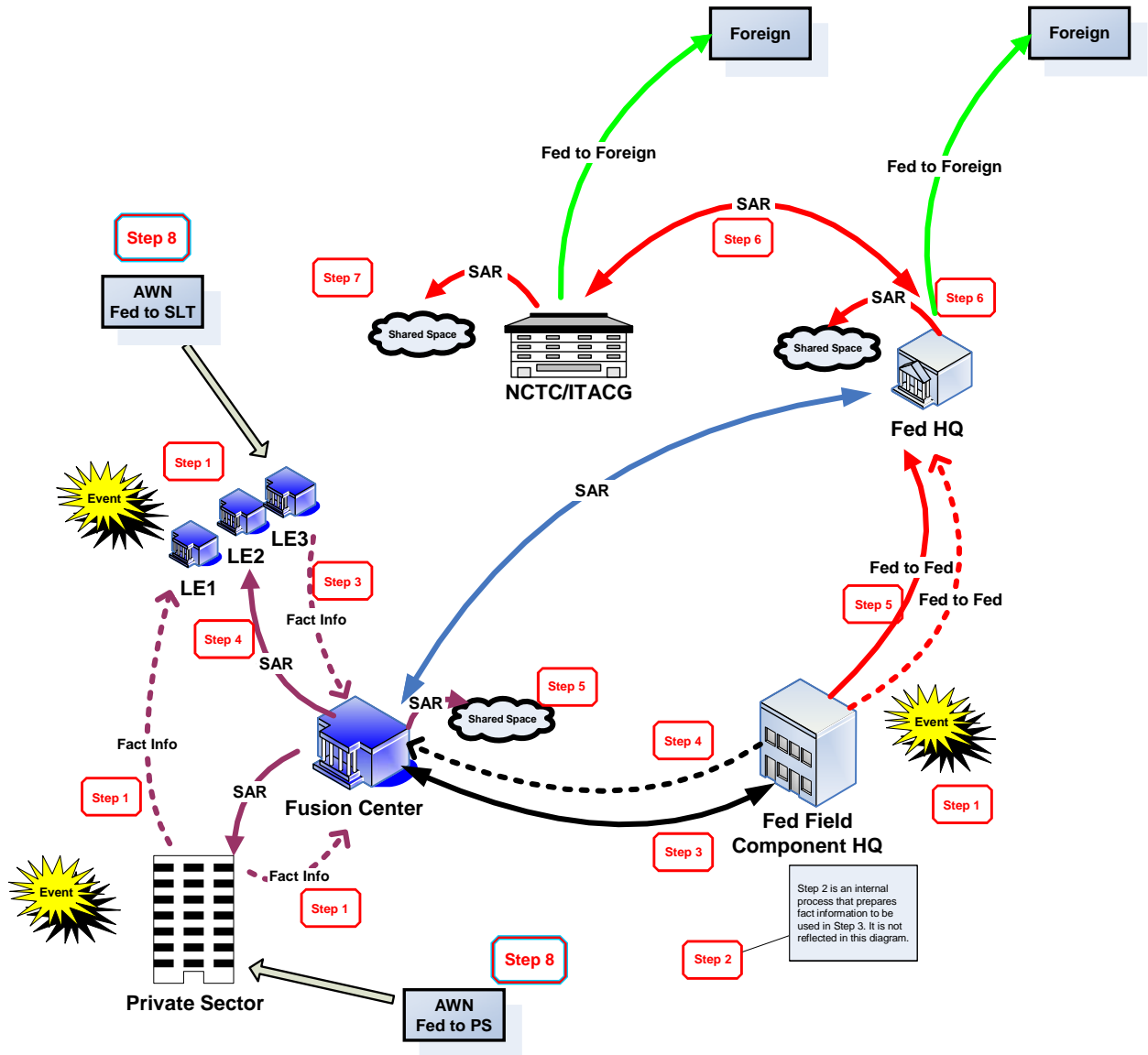


Figure 1: SAR Information Flow Diagram

Appendix E – ISE Identification and Screening Business Process Analysis: Terrorist Watchlist Component – June 2008

I. Purpose

The purpose of this Business Process Analysis (BPA) is to assess the current Consolidated Terrorist Watchlist (terrorist watchlist) environment and to identify any significant watchlist screening and sharing policy, business process and technology gaps as they relate to the Information Sharing Environment (ISE). This BPA represents a joint effort between the Terrorist Screening Center (TSC) and the Program Manager for the Information Sharing Environment (PM-ISE) who worked over the last several months to analyze the Watchlisting environment. The intended audiences for this ISE Watchlist BPA are all Federal participants in the ISE Watchlist process.

II. Scope of Document

This BPA describes the comprehensive, end-to-end watchlist business process. The comprehensive watchlist process encompasses the receiving/sharing of reported information, the nomination, export, screening, encounter, redress, and update functions. The remainder of this BPA includes:

1. Section III, which provides definitions related to watchlists
2. Section IV, which provides the background on the establishment of the Terrorist Screening Center (TSC) and the consolidated terrorist watchlist
3. Section V, which provides the scope of the PM-ISE terrorist watchlist effort
4. Section VI, which provides the methodology used to assess the environment
5. Section VII, which presents the TSC and its progress to date
6. Section VIII, which presents the comprehensive, end-to-end terrorist business process
7. Section IX, which provides the conclusion of this analysis.

III. Definitions

The purpose of this section is to provide the common definitions as they relate to the terrorist watchlist process. To ensure a common understanding, please see below for definitions associated with terrorist Watchlisting:

Biographic Information – information about a person or identity that can be used for identification but does not tie back to a biological measurement. For example, a person's name, date of birth, address, etc. As a general rule of thumb, this is information that the individual does know about themselves but can generally be easily changed.

Biometric Information – refers to the measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition; examples include fingerprint, face, and iris recognition.⁴

Consolidated Terrorist Watchlist (a.k.a. Terrorist Screening Database (TSDB)) – maintained by the Terrorist Screening Center as the consolidated database of the names and other identifying information for all known or suspected terrorists (KSTs).

Derogatory information – classified information that supports an individual's nomination as a KST to the TSDB.

'Known' terrorists – an individual known to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism.⁵

'Suspected' terrorists – an individual suspected to have been involved in activities constituting terrorism or in activities in preparation for or related to terrorism.⁶

IV. Background

One of the most important tools in the fight against terrorism is the U.S. Government's consolidated terrorist watchlist (terrorist watchlist). The terrorist watchlist is the key source for all known and appropriately suspected terrorist. The terrorist watchlist is used by many U.S. Federal departments and agencies, State, local, and tribal (SLT) entities, foreign, and private sector partners in support of their operational mission. Information sharing is critical to the success of the U.S. Government's terrorist-related screening programs. An accurate terrorist watchlist, shared across the ISE community, aids in controlling and protecting our nation's borders. Secured borders strengthen our nation in its global war on terrorism.

The terrorist watchlist is guided by Presidential Directives, Executive Order, and the Intelligence Reform and Terrorism Prevention Act (IRTPA).

- a. The Homeland Security Presidential Directive (HSPD)-6, Integration and Use of Screening Information (September 16, 2003), established the TSC, as a multi-agency effort to be administered by the Federal Bureau of Investigation (FBI), where several watchlists are being consolidated into a single TSDB for use during security-related screening processes. The TSDB is also known as the "terrorist watchlist."
- b. The Memorandum of Understanding (MOU) that accompanied HSPD-6 established the creation of the Terrorist Screening Center (TSC) to integrate the

⁴ National Security Presidential Directive/NSPD-59, Homeland Security Presidential Directive/HSPD-24: Biometrics for Identification and Screening to Enhance National Security, June 5, 2008.

⁵ Terrorist Screening Center Memorandum, Protocol Memorializing the U.S. Governments' Watchlisting Procedures, July 26, 2007.

⁶ Ibid.

existing U.S. government terrorist watchlists and provide 24-hour, 7-day a week responses for agencies that use the watchlist process to screen individuals. TSC officially began operating in December of 2003.

- c. Section 1016(h) of the IRTPA requires the performance management report to include the extent to which all terrorism watchlists are available for combined searching in real-time through the ISE and whether consistent standards exist for adding, removing, and correcting information in the watchlists.
- d. On August 27, 2004, the President signed Executive Order (EO) 13354 National Counterterrorism Center (NCTC), which directed agencies that possess or acquire terrorism and counterterrorism information, except purely domestic counterterrorism information, to promptly give access to such information to the NCTC.
- e. HSPD-11, Comprehensive Terrorist-Related Screening Procedures (August, 27, 2007), builds upon HSPD-6 and required the Secretary of Homeland Security—in coordination with the heads of appropriate federal departments and agencies—to outline a strategy to enhance the effectiveness of terrorist-related screening activities and develop a prioritized investment and implementation plan for detecting and interdicting suspected terrorists and terrorist activities.

V. Scope of PM-ISE Effort

The scope of the PM-ISE terrorist watchlist effort is to ensure ISE participants, in each of the five ISE Communities (Intelligence, Law Enforcement, Defense, Homeland Security, and Foreign Affairs), provide and receive terrorist watchlist information in support of their mission to protect the American people and institutions and to defeat terrorists and their support networks at home and abroad. This paper encompasses the full terrorist watchlist process. (See Section VIII for description of the terrorist watchlist process.)

The PM-ISE matrix team was charged with assessing the current terrorist watchlist environment; documenting business processes and information flows; and identifying any significant watchlist screening and sharing policy, business process and technology gaps. Additionally, the team was tasked to determine if an ISE functional standard is necessary for terrorist watchlist data. The PM-ISE matrix team recognizes existing terrorist watchlist standards (Terrorist Watchlist Person Data Exchange Standard, (TWPDES)) that support the interoperability among the Federal Department and Agencies (D/As); however, there are particular ISE nuances and sensitivities for interfacing with all ISE stakeholders, which may require additional standards.

VI. Methodology

The PM-ISE established a matrix team to conduct the analysis of the current terrorist watchlist operating environment. The team worked closely with the TSC throughout this effort. The internal PM-ISE matrix team is comprised of representation from across the

PM-ISE to include the Business Process Division, the Policy and Planning Division, the Technology Division, the Office of the General Counsel, and the Outreach and Communications team. In assessing the terrorist watchlist environment, the team reviewed and analyzed legal and policy drivers regarding terrorist watchlists; TSC standard operating procedures; TSC protocol regarding terrorist nominations; and other relevant documentation, including various Government Accountability Office (GAO) reports, the Department of Justice and the Office of the Director of National Intelligence Inspector General (IG) reports. Further, the team interviewed TSC and NCTC process owners whose missions most frequently and directly involve interactions with the terrorist watchlist.

VII. Terrorist Screening Center

HSPD-6, signed on September 16, 2003, required the creation of the TSC to integrate the existing U.S. government terrorist watchlists in order to facilitate information sharing to protect the nation and the international community and provide 24-hour, 7-day a week responses for agencies that use the watchlisting process to screen individuals. Prior to the establishment of the TSC, the Federal Government relied on many separate watchlists maintained by different federal agencies for screening individuals.

Based on document reviews and TSC interviews, the following are significant TSC accomplishments in continuously improving the terrorist watchlist:

- Established a proactive mechanism, the Terrorist Encounter Review Process (TERP), to review watchlist data related to frequently encountered individuals and make corrections or enhancements to the watchlist, as appropriate
- Expanded its efforts to ensure the quality of watchlist data by increasing the number of staff assigned to data quality management and improving quality assurance processes;
- Performed selected scrubs of watchlist data, including, a special quality assurance review of the No Fly List, and an on-going record-by-record review of the entire TSDB;
- Established a process and a separate office to address complaints filed by persons seeking relief from adverse effects of related terrorist watchlist screening;
- Established an interagency working group to review and implement improvement opportunities for watchlist process; and
- Coordinated with State and major urban area fusion centers and Joint Terrorism Task Forces to help them better understand the role of the TSC and use the TSDB more effectively
- Participating in Federal-wide government efforts underway to establish mutually compatible methods for sharing biometric information

VIII. Comprehensive Consolidated Terrorist Watchlist Business Process

The TSC's consolidated terrorist watchlist (a.k.a. the Terrorist Screening Database or TSDB) is the U.S. Government's master repository for all known or appropriately suspected international and domestic terrorist records used for watchlist-related screening. NCTC's database serves as the single source for the TSDB, except for purely domestic terrorism information which is provided directly to the TSDB from the FBI via a formalized procedure.

The TSC records contain sensitive but unclassified information on terrorist identities—such as name and date of birth—that can be shared with screening agencies, whereas the classified derogatory information that supports the watchlist records is maintained in other law enforcement and intelligence agency databases.

The terrorist watchlist BPA encompasses the receiving/sharing of reported information, the nomination, export, screening, encounter, redress, and updates to the TSDB. Figure 1 illustrates the end-to-end Consolidated Terrorist Watchlist process followed by a description of each step.

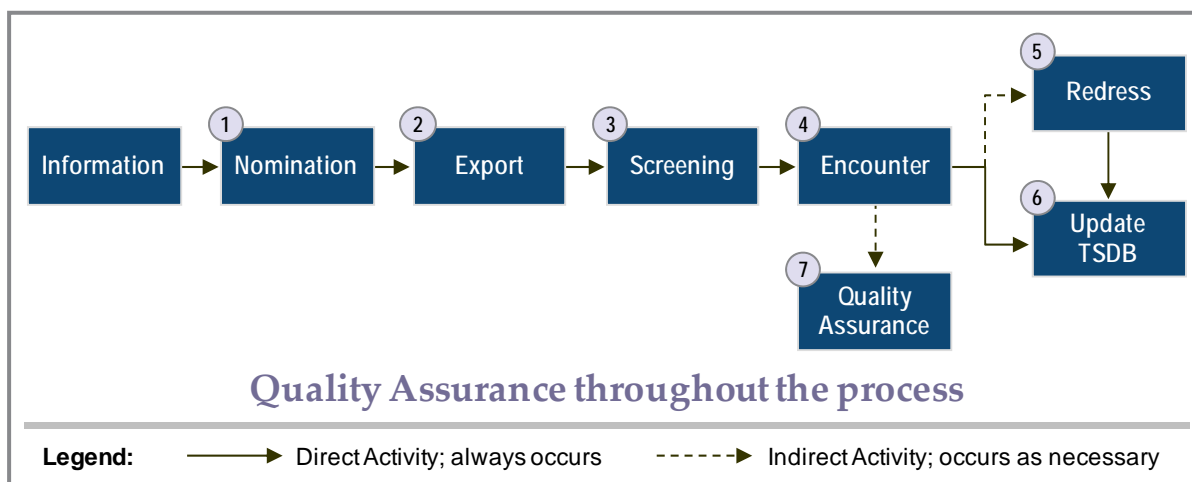


Figure 1: Comprehensive Consolidated Terrorist Watchlist Process

Information

The process begins when reported information is received and/or shared that prompts the need for a nomination to the consolidated terrorist watchlist. Information that would trigger the need for an individual to be nominated to the watch list could originate from a variety of sources. A criminal investigation could identify an individual or individuals engaged in terrorism or supporting terrorism activities. Confidential sources or electronic surveillance are other sources of information that could trigger an individual's nomination to the watchlist. Clandestine operations could uncover information that would lead to a nomination. Engaging in suspicious activity or other criminal activities

such as money laundering could lead to investigative activities which may lead to a nomination.

Step 1—Nomination

Please see pages E-10 – E-15 for the corresponding detailed nomination and export information flow.

A nomination may be in the form of: 1) an addition of a “Known or appropriately Suspected Terrorist” (KST) to the terrorist watchlist; 2) a modification of existing information of a KST on the terrorist watchlist; or 3) a deletion of existing information on the KST.

Nominations fall into two distinct categories: international and purely domestic. The NCTC provides all international KST nominations to the TSC; whereas the FBI provides all purely domestic KST nominations to the TSC. The TSC conducts a review of all nominations and makes a determination to accept or reject nominations.

International KST Nominations. The NCTC receives nominations from nominating agencies which includes all ISE participant communities (Intelligence, Defense, Homeland Security, Law Enforcement, and select Foreign Partners). Nominating agencies must ensure that the information is properly marked with any applicable restrictions, including caveats on its use, dissemination, retention, or destruction. The NCTC reviews all international nominations and makes a determination to either accept or reject based on various criteria.⁷ If the NCTC does not accept the nomination, NCTC will notify the nominating agency that the nomination was rejected. If the NCTC accepts the nomination, NCTC will accept the nomination into its database. Currently, the NCTC database contains both identifying information and derogatory information. The NCTC provides a sensitive but unclassified export of the international KST nominations to the TSC using the TWPDES. The NCTC export to the TSDB only contains identifying information.

Purely Domestic KST Nominations. The FBI headquarters receives purely domestic nominations from the law enforcement community. These nominations are subject to review and further analysis by the FBI. The FBI forwards those purely domestic KST nominations directly to the TSC.

TSC Review Process. The TSC reviews all nominations (international and domestic) and makes a determination for inclusion in the TSDB based on watchlisting criteria and standards. The TSC will notify the NCTC and the FBI of any nominations not accepted and the reason for why a nomination is not accepted to support quality improvement processes. The TSC follows a detailed standard operating procedure for uploading NCTC’s information into the TSDB.

⁷ Specific criteria is classified and therefore not detailed in this report.

Currently, Federal departments and agencies submit their international nominations based on internal agency procedures. At this writing, the NCTC is in the process of standardizing the mechanisms by which Federal departments and agencies submit international nominations to NCTC by employing a standard electronic nomination form. This standardization will enable NCTC to obtain information (biographic and biometric) in a structured, standard format for easy ingest into its database. NCTC plans to work with stakeholders to develop templates and mechanisms to ensure successful implementation of the standardized nomination form.

Additionally, the watchlist community is in the process of extending their existing TWPDES implementation to include biometric data elements to reduce false positive matches and improve quality of data within the consolidated Terrorist Watchlist database.

Step 2—Export

Please see pages E-10 – E-15 for the corresponding detailed nomination and export information flow.

Currently, the TSC exports applicable records from the watchlist containing biographic data, such as name and date of birth, to Federal Government databases used by agencies that conduct terrorism screening. The screening community spans across Federal, State, and local governments, the private sector, and U.S. Government partnerships with those organizations among the international community that have terrorist-related screening functions. TSC provides this information directly to Federal, selected foreign government, and others through various methods (e.g., email, database export).

Step 3—Screening

Please see pages E-16 – E-19 for the corresponding detailed screening and encounter information flow.

The screening community accepts and uses the TSDB export. The screening community conducts terrorist-related queries that support homeland security inside the U.S., at the borders, and abroad. For example, Department of State will query its databases before issuing visas or passports; Departments of Treasury, Justice, and Homeland Security will query their respective databases to control entry into and exit from the U.S. (control land, air, and sea ports of entry); and the Departments of Justice, Defense, and Homeland Security will query their respective databases to manage stays within the U.S.

Step 4—Encounter

Please see pages E-16 – E-19 for the corresponding detailed screening and encounter information flow.

The screening community conducts terrorist-related queries that support homeland security inside the U.S., at the borders, and abroad. Individuals initiate the encounter process when they seek a particular service or encounter law enforcement or homeland security personnel. For example, when an individual makes an airline reservation, arrives at a U.S. port of entry, applies for a U.S. visa/passport, or is stopped by state or local law enforcement within the U.S., the frontline screening agency or airline conducts a name-based search of the individual against applicable terrorist watchlist records.

Based on the information queried and the results of the query, a number of actions may be taken. Actions may include granting or denying a visa/passport request, or entry into the U.S.; or release or arrest of individual.

Step 5—Redress

Please see pages E-20 – E-23 for the corresponding detailed redress information flow.

Individuals who have a negative screening experience may file a redress complaint with the screening agency involved in the encounter. In 2005, the TSC established a formal watchlist redress process that allows agencies that use the TSDB data during a terrorism screening process to refer individuals' complaints to the TSC when it appears the complaints are related to the TSDB. The goal of the redress process is to provide for timely and fair review of individuals' complaints and to identify and correct any data errors, including errors in the Terrorist Watchlist.⁸ Complainants file redress inquiries with the frontline screening agencies involved in the encounters. The TSC does not work directly with the complainants.

Additionally, in April 2008, the TSC initiated a new program to automatically review the Terrorist Watchlist records of frequently encountered individuals even if no formal redress requests are filed. The Terrorist Encounter Review Process (TERP) will provide a guaranteed review of such records to ensure they are accurate, complete, and current.⁹

Step 6—Update

Based on the screening results, encounter, redress inquiry, or general quality assurance, there may be a need to update the TSDB. This is done in collaboration with NCTC, FBI, TSC, and screening agencies. Internal to TSC, the call center operations specialist obtaining updated information initiates a quality assurance record.

⁸ Terrorist Screening Center website: <http://www.fbi.gov/terrorinfo/counterrorism/redress.htm>; researched May 20, 2008.

⁹ Terrorist Screening Center Website: <http://www.fbi.gov/terrorinfo/counterrorism/tsc041008.pdf>; researched June 5, 2008.

Step 7—Quality Assurance

Encounters provide an additional opportunity to conduct quality assurance against the TSDB. The TSC uses a software application called the Encounter Management Application (EMA) to manage information related to “hits” or possible matches against the Terrorist Watchlist. The EMA contains the details of all incoming encounters. This information may be used in support of larger quality assurance efforts to provide accurate and timely watchlist information to customers.

IX. Conclusions

The Federal government currently has processes that enable the successful creation and maintenance of the Consolidated Terrorist Watchlist. The watchlist process provides the watchlisting and screening communities the opportunity to nominate and to screen against the TSDB based on mission needs. The TSDB provides a direct export to the majority of the watchlisting community via database uploads, various applications, and email. Additionally, the watchlist process conforms to the Presidential Guidelines.¹⁰

With support and input from the watchlisting community, the TSC drafted a protocol to document the U.S. Governments’ watchlisting procedures “Protocol”¹¹. This protocol formalizes the various watchlisting policies and procedures of the U.S. Government; and provides supplemental Watchlisting guidance to the federal departments and agencies that comprise the Watchlisting community.¹²

¹⁰ *Presidential Guideline 1: Develop Common Standards to Maximize the Acquisition, Access, Retention, Productions, Use, Management, and sharing of terrorism information; Presidential Guideline 2: Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, local, and tribal governments, law enforcement agencies, and the private sector; Presidential Guideline 3: Standardize Procedures for Sensitive But Unclassified (SBU) Information; Presidential Guideline 4: Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners; Presidential Guideline 5: Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the ISE.*

¹¹ Terrorist Screening Center Memorandum, Protocol Memorializing the U.S. Governments’ Watchlisting Procedures, July 26, 2007.

¹² Memorandum Recipients: National Security Council; Homeland Security Council; Director of National Intelligence; Department of State; Department of Justice; Department of Homeland security; Department of Treasury; Department of Defense; Department of Energy; Central Intelligence Agency; Federal Bureau of Investigation; National Counterterrorism Center; National Security Agency; Defense Intelligence Agency.

Nomination and Export Information Flow

Step	Activity	Process	Notes
1	Reported Information From All Sources, Including Private Sector	The process begins when information is reported that prompts the need for a nomination to the Consolidated Terrorist Watchlist (terrorist watchlist). A nomination may be in the form of: 1) an addition of a "Known or appropriately Suspected Terrorist" (KST) to the terrorist watchlist; 2) a modification of existing information of a KST on the terrorist watchlist; or 3) a deletion of existing information on the KST.	An individual may be nominated by a foreign partner (through a U.S. Federal organization), a Federal organization, law enforcement, or through the redress process. Additionally, this initial step is meant to capture information reported from all ISE sources (Defense, LE, Homeland Security, Foreign, and Private Sector communities).
2	Nomination	International: ¹³ A Foreign partner may nominate a KST for inclusion on the terrorist watchlist through existing partnership(s) with US Federal government organization(s). Federal organizations may also nominate international KSTs. All international KST nominations, including those nominated by the FBI, must be submitted through NCTC for review and adjudication. Once nominations are accepted, NCTC will include KSTs in their classified database. TIDE is classified system. Domestic: ¹⁴ The FBI may nominate a domestic KST through investigative information. State and local law enforcement entities may also nominate KSTs by way of their Federal law enforcement partners (i.e., DOJ, Treasury). All domestic law enforcement nominations are submitted to the TSC through the FBI HQ (i.e., law enforcement information is forwarded to FBI HQs).	A nomination may be due to intelligence (international terrorist) information, FBI investigative (domestic terrorist or international) information, or part of the Redress process (please note the Redress process is addressed in the Redress Information Flow), through a Federal organization to add or remove an individual's name from the terrorist watchlist. All international nominations of KSTs must be reported through the NCTC. International KSTs from FBI or other US government law enforcement organizations must be submitted to the NCTC. This is represented by the "Federal HQs International Nomination" in the information flow. Nominations among the various agencies are based on their internal procedures.

¹³ The following Federal organizations provide international terrorism information to NCTC: Department of Justice, Central Intelligence Agency, Defense Intelligence Agency, Department of Treasury, Department of State, and the Department of Homeland Security.

¹⁴ All domestic terrorism information for inclusion to the Watchlist must be submitted through the Department of Justice, FBI.

Step	Activity	Process	Notes
3	Submit Nomination	<p>International: Federal HQs submit nominations to NCTC.</p> <p>Domestic: FBI HQs receives nominations through various mechanisms, conducts further analysis, and forwards the nomination to TSC as appropriate.</p> <p>Local law enforcement (LE) has the capability to pass information directly to Joint Terrorism Task Forces (JTTFs).¹⁵ The JTTF, which is part of the Federal system would look at the information and possibly conduct further inquiry into the event/information. The JTTF would pass the information to Federal law enforcement where it would be subjected to further analysis, and if appropriate then forwarded to FBI HQs for analysis and coordination before being submitted to the TSC</p> <p>A local law enforcement agency may pass the information to a fusion center. The FBI has a number of JTTFs and Field Intelligence Groups (FIGs)¹⁶ co-located in fusion centers. The information would be subject to the same checks as if it was reported directly to a JTTF, then sent up the chain of command eventually finding its way to TSC, if appropriate.</p> <p>A State fusion center has the ability to pass information directly to the JTTF if it feels the information has a terrorism nexus, as a local police department may not be able to make the determination.</p> <p>Additionally, the JTTF, through investigative activity, which can be independent of state, local and tribal law enforcement, can decide that a person or event meets the criteria for inclusion on the watchlist and pass the information to TSC.</p>	<p>Currently, agencies submit their nominations based on internal policies and procedures.</p> <p>NCTC is standardizing the mechanisms and format (to include biometrics) by which Federal agencies submit nominations to NCTC by employing a standard, electronic nomination form.</p>

¹⁵ Joint Terrorism Task Forces are teams of state and local law enforcement officials, FBI agents, and other federal agents and personnel whose mission is to investigate and prevent acts of terrorism. There is a Joint Terrorism Task Force for each of the FBI's 56 main field offices, and additional task forces are located in smaller FBI offices.

¹⁶ Field Intelligence Groups are teams of FBI intelligence analysts and special agents whose mission is to analyze and process raw intelligence gathered in the course of investigative activity to provide tactical and strategic intelligence products in support of the FBI field division.

Step	Activity	Process	Notes
4	Review Nomination (NCTC)	<p>International:¹⁷ NCTC reviews the nomination and makes a determination whether to accept the nomination. If NCTC accepts the nomination, then the nomination is incorporated into the NCTC's database and exported via Terrorist Watchlist Person Data Exchange Standards (TWPDES) in a Sensitive But Unclassified format to TSC for inclusion in the TSDB.¹⁸</p> <p>If a nomination is not accepted, NCTC will return the nomination to the nominating agency.</p>	Review includes an analysis of information supporting the watchlist nomination, as well as an examination of the quality, accuracy, and sufficiency of the identify information.
5	Review Nomination (TSC)	TSC reviews each nomination for completeness, accuracy, and timeliness of information prior to accepting the nomination into the terrorist watchlist. ¹⁹ If a nomination is not accepted, TSC will return the nomination to NCTC (international nominations) or FBI (domestic nominations).	A variety of checks are conducted on the nominations prior to accepting nomination into the TSDB. General criterion for including a record in the TSDB is that the nominating agency must have provided evidence of a nexus to terrorism.
6	Accept Nomination into Terrorist Watchlist	After review and adjudication by TSC staff and if the nominee meets the criteria for inclusion, TSC accepts the name and adds it to the consolidated terrorist watchlist.	Entries here do not include classified/intelligence information. Only unclassified identity and biographical information is added to the TSDB for use by screening agencies. Soon, biometric information will also be included based on mutually compatible Federal solutions.

¹⁷ NCTC exports international terrorism information to the TSC on a daily basis.

¹⁸ NCTC provides international terrorism information to the Intelligence Community.

¹⁹ TSC receives, reviews, and makes determinations on nominations (both international and domestic) six days a week.

Step	Activity	Process	Notes
7	Provide Terrorist Identity Information to Screening Communities	<p>TSC exports applicable records from the watchlist—containing identifying data or biographic data, such as name and date of birth—to federal government databases used by agencies that conduct terrorism screening—the screening community.²⁰ TSC provides this information directly to Federal, selected Foreign governments, and others through various methods (e.g., email, database upload).</p> <p>The applicable records that TSC exports to each of these databases vary based on the screening agency’s mission responsibilities and the technical capability of the agency’s computer systems.</p>	<p>Provide²¹ to: DHS and appropriate components such as Transportation Security Administration (TSA), Department of State, Law Enforcement, and Selected Foreign Partners.</p> <p>The TSC shares the terrorist identity and biographic information contained in the TSDB by sending it “downstream” (i.e., exporting) to other government screening systems where frontline screening agents can use the information to identify individuals against TSDB records.</p> <p>Federal-wide government efforts are underway to establish mutually compatible methods for biometric information.</p>

²⁰ The screening community extends across Federal, State, and local governments, the private sector, and to U.S. Government partnerships with those organizations among the international community that have terrorist-related screening functions.

²¹ Information is shared with the following databases: DHS’ Treasury Enforcement Communications System (TECS)/IBIS; TSA’s No Fly and Selectee List, National Crime information Center’s (NCIC) Violent Gang and Terrorist Organizational File (VGTOF); Department of State’s Consular Lookout and Support System (CLASS VISA/Passport); foreign partners, and others.

Step	Activity	Process	Notes
8	Accept and Use Terrorist Watchlist	<p>The screening community conducts terrorist-related queries that support homeland security inside the U.S., at the borders, and abroad. For example, Department of State will query its database before issuing visas or passports; Departments of Treasury, Justice, and Homeland Security will query their respective databases to control entry into the US (control land, air, and sea ports of entry); Departments of Justice, Defense, and Homeland Security will query their respective databases to manage stays within the US; and Departments of Treasury, Justice, and Homeland Security will query their respective databases to control exits from the US (control land, air, and sea ports of departure).</p> <p>Secure Flight Program will eliminate the need to export No Fly/Selectee List to the Private Sector; instead this function will reside with the Federal government. Implementation is expected within the next two years.</p>	<p>Based on the information queried and the results of the query, a number of actions may be taken. Actions may include granting or denying a visa or passport, release or arrest, report or contact of an agency with information of encounter, etc.</p> <p>The screening community provides screening results back to the NCTC and the FBI through the TSC's 24-hour call center in support of terrorist-related investigations and encounters, both positive and inconclusive.</p> <p>Details around encounter management are addressed in the Encounter Management Information Flow.</p>
	Update Terrorist Watchlist (Ongoing)	<p>New information on an individual is developed that requires a change in the individual's status or identity. The individual name is submitted into the nomination process, identified in Steps 1 and 2, as an addition, modification, or deletion.</p>	<p>TSC has increased its quality assurance efforts and implemented a data quality improvement plan that details the TSC's intent to conduct a record-by-record review of the TSDB. TSC examines historical TSDB records for accuracy and completeness through targeted reviews of specific subsets of the watchlist records. For example, TSC conducted a special quality assurance review of TSA's No Fly List, which reduced the number of records on the list and increased the accuracy and integrity of this data. Plans are in place to conduct additional special quality assurance reviews</p>

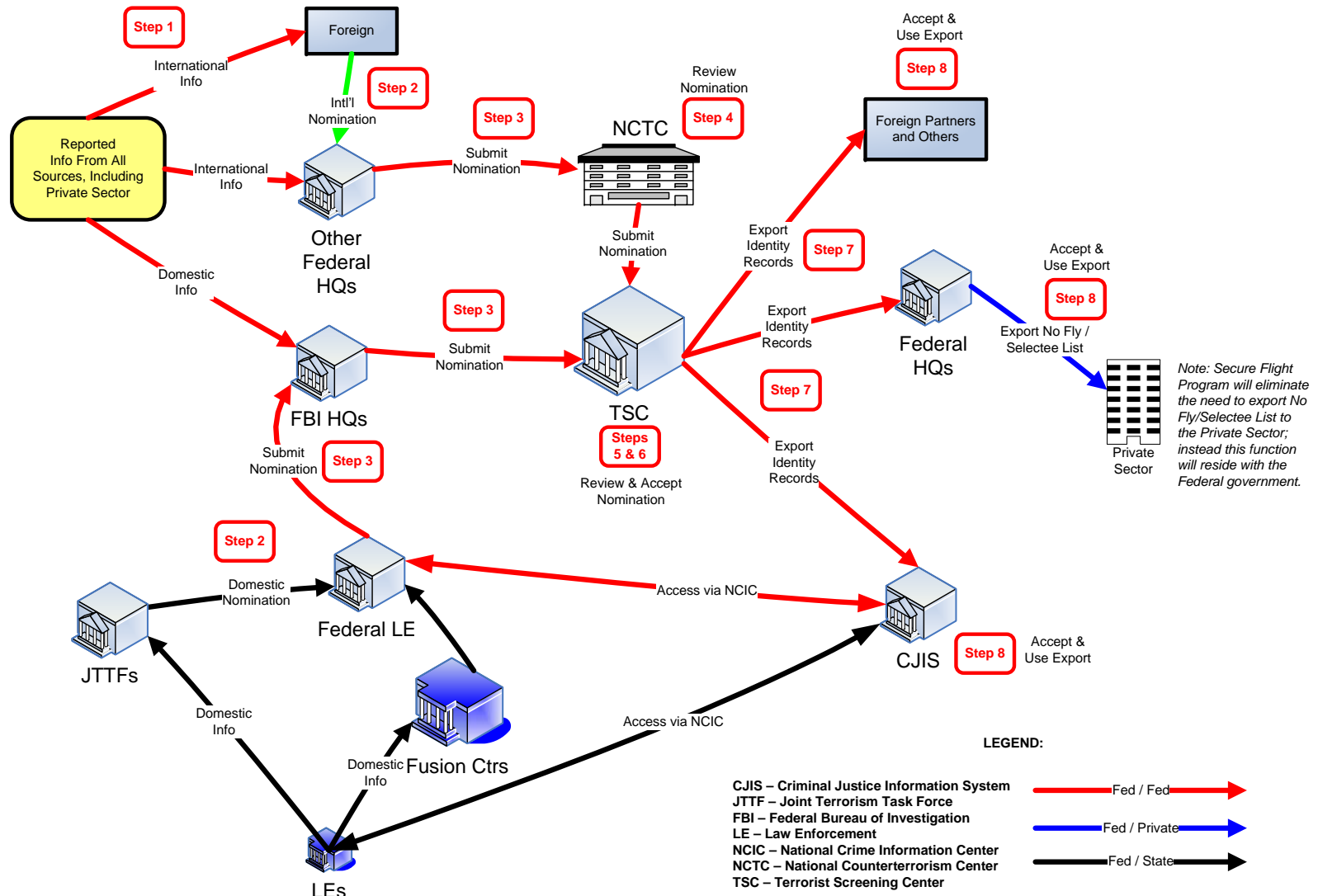


Figure 2: Consolidated Terrorist Watchlist Nomination and Export Information Flow Diagram

Screening and Encounter Information Flow

Step	Activity	Process	Notes
1	Initiate Screening Process	<p>The Terrorist Screening Center's (TSC) consolidated terrorist watchlist is the United States (U.S.) government's master repository for all known or appropriately suspected international and domestic terrorist records used for watchlist-related screening.</p> <p>The screening community conducts terrorist-related queries that support homeland security inside the U.S., at the borders, and abroad. Individuals initiate the screening process when they seek a particular service or encounter law enforcement or homeland security personnel. For example, when an individual makes an airline reservation, arrives at a U.S. port of entry, applies for a U.S. visa/passport, or is stopped by state or local police within the United States, the frontline screening agency or airline conducts a name-based search of the individual against applicable terrorist watchlist list records.</p>	<p>Records for inclusion on the consolidated terrorist watchlist are nominated to TSC from the following two sources:</p> <p>International terrorist information is provided to TSC by the NCTC.</p> <p>Purely domestic terrorist information is provided to the TSC by the FBI.</p> <p>The TSC records contain sensitive but unclassified information on terrorist identities—such as name and date of birth—that can be shared with screening agencies, whereas the classified derogatory information that supports the watchlist records is maintained in other law enforcement and intelligence agency databases.</p>
2	Search Airline or Agency Database (Screening Agency)	<p>Screening Agencies conduct queries against the terrorist watchlist. For example, the Department of State will query its database before issuing visa/passport; Departments of Treasury, Justice, and Homeland Security will query their respective databases to control entry into the US (control land, air, and sea ports of entry); Departments of Justice and Defense will query their respective databases to manage stays within the U.S.; and Departments of Treasury, Justice, and Homeland Security will query their respective databases to control exits from the U.S. (control land, air, and sea ports of departure).</p>	<p>In general, when the computerized name-matching system of an airline or screening agency generates a "hit" (a potential name match) against watchlist records, the airline or agency is to review each potential match.</p> <p>All border entries are the responsibility of Customs and Border Patrol (CBP)/National Targeting Center (NTC) within DHS. On the departure side, TSA has control of domestic flights through the no-fly/selectee lists and CBP/NTC provides TSC passenger manifests of all outbound international flights for identity resolution and notification(s)</p>

Step	Activity	Process	Notes
3	Search Results (Screening Agency)	Any obvious mismatches (negative matches) are to be resolved by the airline or screening agency, if possible and the individual is notified. However, clearly positive or exact matches and matches that are inconclusive (uncertain or difficult-to-verify) are to be referred to the TSC's call center. State and local law enforcement officials are instructed to refer exact matches and inconclusive matches directly to TSC.	The screening community provides screening results back to the NCTC and the FBI through the TSC's 24-hour call center in support of terrorist-related investigations and positive or inconclusive encounters. The TSC uses a software application called the Encounter Management Application (EMA) to manage information related to "hits" or possible matches against the terrorist watchlist. The EMA contains the details of all incoming encounters.
4	Review (TSC)	TSC checks its databases and other sources—including classified databases maintained by NCTC and the FBI—and confirms whether the individual is a positive, negative, or inconclusive match to the watchlist records.	
5	Search Results (TSC)	TSC refers all positive and some inconclusive matches to the FBI's Counterterrorism Division, Terrorist Screening Operations Unit (TSOU) for an operational response. Collaboration among the frontline screening agency, NCTC or other intelligence community members, and the FBI or other investigative agencies may be necessary to resolve an encounter. Operational collaboration is typically done by TSOU. TSC is engaged in various Outreach efforts with State and major urban area fusion centers and Joint Terrorism Task Forces to help them better understand the role of the TSC and use the TSDB more effectively	NCTC and the FBI are involved because they maintain the underlying derogatory information that supports terrorist watchlist records, which is needed to help determine the appropriate counterterrorism response.

Step	Activity	Process	Notes
6	Need Additional Information	Law enforcement encounters provide an opportunity or need to obtain additional information about the person encountered. In this case, the TSOU may request a member of an FBI Joint Terrorism Task Force, ²² screening agency, or other law enforcement agencies—such as U.S. Immigration and Customs Enforcement—to respond and collect information.	
7	Encounter Resolution	The screening agency is responsible for processing and communicating the TSC coordinated screening / encounter decision to the individual.	Based on the information queried and the results of the query, a number of actions may be taken. Actions may include granting or denying visa/passport request, or entry into the U.S.; release or arrest of individual.
	Update Terrorist Watchlist (Ongoing)	Based on the encounter and screening results, there may be a need to update the TSDB. This is done in collaboration with NCTC, FBI, TSC, and screening agencies. Internally, the call center operations specialist at TSC obtaining updated information initiates a form quality assurance (QA) record.	Additionally, encounter activities and resolution are captured in the EMA

²² Joint Terrorism Task Forces are teams of state and local law enforcement officials, FBI agents, and other Federal agents and personnel whose mission is to investigate and prevent acts of terrorism. There is a Joint Terrorism Task Force in each of the FBI's 56 main field offices, and additional task forces are located in smaller FBI offices.

Redress Information Flow

Step	Activity	Process	Additional Information
1	File Redress Inquiries	<p>Individuals who have a negative screening experience may file a redress complaint with the screening agency involved in the encounter.</p> <p>The goal of the Consolidated Terrorist Watchlist (terrorist watchlist) redress process is to provide for timely and fair review of individuals' complaints, and to identify and correct any data errors, including errors in the terrorist watchlist itself.</p> <p>Complainants file redress inquiries with the frontline screening agencies involved in the encounters. For example, if an individual is prohibited from boarding a domestic commercial airline flight, the person would contact the Transportation Security Administration (TSA) to file a redress complaint.</p> <p>Additionally, in April 2008, the TSC initiated a new program to automatically review the Terrorist Watchlist records of frequently encountered individuals even if no formal redress requests are filed. The Terrorist Encounter Review Process (TERP) will provide a guaranteed review of such records to ensure they are accurate, complete, and current.</p>	<p>Since most screening is conducted by Department of Homeland Security (DHS) and the Department of State (DoS), on February 20, 2007, DHS and the DoS implemented the Traveler Redress Inquiry Program (TRIP). This program established a centralized portal for persons to file complaints regarding difficulties experienced at screening points during travel, such as airports, train stations, and border crossings.</p> <p>Complainants file redress inquiries with the frontline screening agencies involved in the encounters, such as through TRIP for DHS and the DoS.</p> <p>Individuals, who have complaints with agencies not involved in TRIP, send complaints directly to those agencies.</p>
2	Review Complaint (Screening Agency)	<p>The screening agency reviews the complaint and determines if the inquiry relates to a possible terrorist watchlist match. This internal review must consider if the complaint: 1) is related to TSC data, and 2) complies with TSC's requirements for accepting redress matters.</p> <p>If the screening agency determines that the complaint is not related to the terrorist watchlist, it will resolve the matter internally and respond to the complainant.</p> <p>If the screening agency determines that a complaint pertains to a possible watchlist match, it will forward the complaint to the TSC.</p>	<p>For example, an airline may deny a person from boarding an airplane because of drunkenness or disorderly behavior. Complaints related to these types of matters and others unrelated to the terrorist watchlist should not be referred to the TSC.</p> <p>Screening agencies refer redress matters to TSC's Redress Officer. Redress matters must be accompanied by the TSC Redress Referral Checklist and an identity document to verify the subject's identity.</p>

Step	Activity	Process	Additional Information
3	Review Complaint (TSC)	<p>The TSC Redress Office (RO) determines if the complaint is related to a terrorist watchlist identity. TSC Redress Office is responsible for reviewing redress inquiries, corresponding with partner agencies for clarification or additional information, and makes the final determination as to an individual's watchlist status.</p> <p>If the complaint is not related to terrorist watchlist, the TSC returns the complaint to the screening agency for resolution.</p> <p>If the complaint is related to the terrorist watchlist, the TSC conducts a review of watchlist records, various databases, and coordinates with partner agencies and determines relationship to terrorist watchlist.</p> <p>Based on the results of the database checks and analysis of the results, the TSC will make a determination to assign one of the following redress disposition categories to the redress matter: Not related, Positive match, or Misidentification.</p> <p>For redress matters that are not related to the terrorist watchlist, the TSC returns this matter to the appropriate screening agency for resolution.</p> <p>For redress matters that are a positive match to terrorist watchlist, the TSC conducts a complete review of the watchlist records and supporting information to ensure information on the individual meets the criteria for watchlisting and is accurate, complete, and current. This review will also include contacting the nominating agency to obtain any new or clarifying information on the individual not available to the TSC.</p> <p>Redress matters that are determined to be Misidentification are processed by TSC similar to positive match matters. The TSC reviews the terrorist watchlist record involved in the misidentification and supporting information to ensure the record is accurate, complete, and current. The TSC coordinates and consults with the nominating agency to get any updated information and make the final determination as to the individual's watchlist status.</p>	<p>TSC works with each screening agency to establish an appropriately secure means by which to receive redress matters, which typically contain sensitive personal data and may be Privacy Act protected. Preferred transmission options are encrypted email or email sent within a secured government network.</p> <p>"Not related" is used when a determination is made when the complaint does not match a terrorist watchlist identity and was not the subject of an encounter involving a potential match.</p> <p>A positive match is a complainant who matches an identity on the terrorist watchlist and was the subject of at least one watchlist-related encounter.</p> <p>A misidentification is an individual who is the subject of a terrorist-related screening but whose identity is deemed a negative match to the terrorist watchlist.</p> <p>Typically, the TSC undertakes a redress review only when an individual submits a formal redress complaint.</p>

Step	Activity	Process	Additional Information
4	Revise Watchlist Record(s) as Necessary (TSC)	Based on the determination of the redress disposition category and resolution, the TSC will correct/update information in the terrorist watchlist, as appropriate.	
5	Determine Disposition(TSC)	Based on redress disposition category assigned to the redress matter, the TSC resolves the complaint and notifies the screening agency of its decision.	The TSC does not provide derogatory information to the screening agency. The TSC simply provides the agency with the individual's watchlist status.
6	Communicate Disposition Determination	Based on the TSC disposition determination, the screening agency is responsible for communicating the TSC decision to the individual. Screening agencies use letters that are pre-approved by the watchlist community that neither confirm nor deny an individual's status on the TSDB. By agreement of the community, any letters that are not pre-approved must be vetted through the TSC to ensure the proposed letter does not have an adverse effect on the terrorist watchlist community.	TSC does not directly respond to redress matters from individuals, instead, works with the screening agency and the nominating agency to develop an appropriate written response, or use a template response that has been approved in advance.

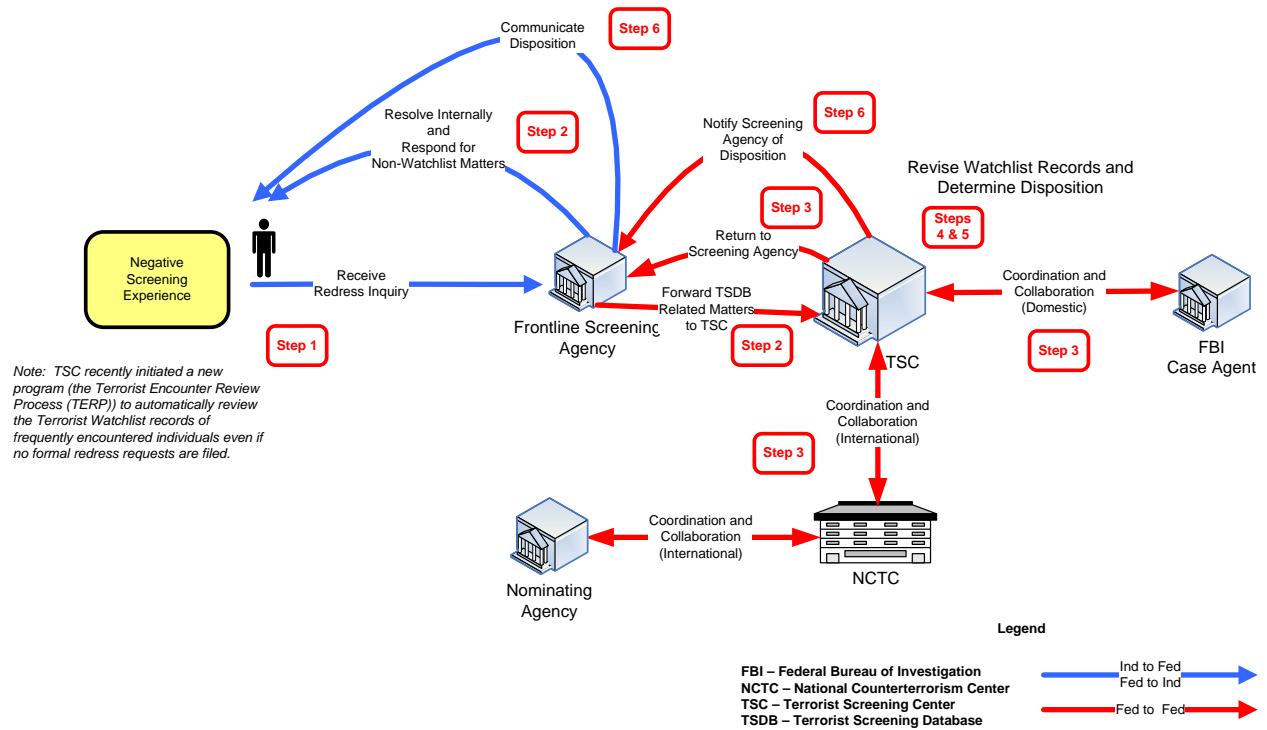


Figure 4: Consolidated Terrorist Watchlist Redress Information Flow Diagram

This page intentionally blank.

Appendix F – ISE Alerts, Warning, and Notification Business Process Analysis – June 2008

I. Purpose

The purpose of this Business Process Analysis (BPA) is to define and document the mostly common and commonly understood Federal alerts, warnings, and notifications (AWN) process for the Information Sharing Environment (ISE). This BPA describes how the Federal Government is addressing *National Strategy for Information Sharing (NSIS)* objectives for inter-agency production and dissemination of “federally coordinated” AWN products.²³ The intended audiences for this ISE AWN BPA are all Federal participants in the ISE AWN process.

II. Scope of Document

This BPA documents the high level ISE AWN business process for analyzing information, coordinating, producing and disseminating “federally coordinated” ISE AWN products and the roles of the four major Federal ISE AWN coordination, production and dissemination partners. A working definition of an ISE AWN for the purposes of this BPA is as follows: ‘ISE AWNs are terrorism-related AWNs produced as a result of interagency coordination and disseminated to ISE participants. ISE AWNs also include urgent AWNs developed with only internal agency coordination, but disseminated to ISE participants.’²⁴ The Federal ISE AWN process describes how agencies across the Federal government collaborate in support of the ISE AWN mission.

This BPA includes:

1. The legislative and policy background guiding Federal ISE AWN;
2. Definitions for alerts, advisories, and assessments, as defined by the Interagency Intelligence Committee on Terrorism (IICT) and discussion of the need for further work to define ISE AWNs;
3. The commonly understood ISE process for producing and disseminating federally coordinated ISE AWNs. It clarifies where the process activities are implemented differently for threats with a foreign nexus versus purely domestic threats;²⁵ this process is scalable to also address threats whose urgency necessarily precludes inter-agency coordination, but allows for internal agency coordination.

²³ *National Strategy for Information Sharing*. The White House (October 2007) pp. A1-7 and A1-8. Addressing the NSIS AWN objectives will strengthen the Nation’s counterterrorism mission.

²⁴ Based upon input from key Federal AWN producers, “urgent” signified timeframes that precluded interagency coordination.

²⁵ In this BPA, foreign terrorism nexus and foreign terrorism threat mean the same as transnational terrorism nexus or threat. These terms refer to threats against the U.S. homeland linked to terrorist activities overseas.

4. Description of the roles and responsibilities of the National Counterterrorism Center (NCTC), the NCTC's Interagency Threat Assessment and Coordination Group (ITACG) and the IICT, for the coordination and production of federally coordinated terrorism-related ISE AWNs;
5. Description of high level Department of Homeland Security (DHS) and Federal Bureau of Investigations (FBI) ISE AWN coordination and production roles as the two primary producers of ISE AWNs for threats with a purely domestic nexus; and of their dissemination roles as the primary disseminators of ISE AWNs to State, local, tribal (SLT) governments and the private sector;
6. The high level ISE AWN information flow (pages F-20 – F-31) for the analysis, coordination, production, dissemination, and follow-up activities within the ISE AWN process.

Figure 1 illustrates the scope of this document and shows where, within that scope; the coordination, production and dissemination activities occur.

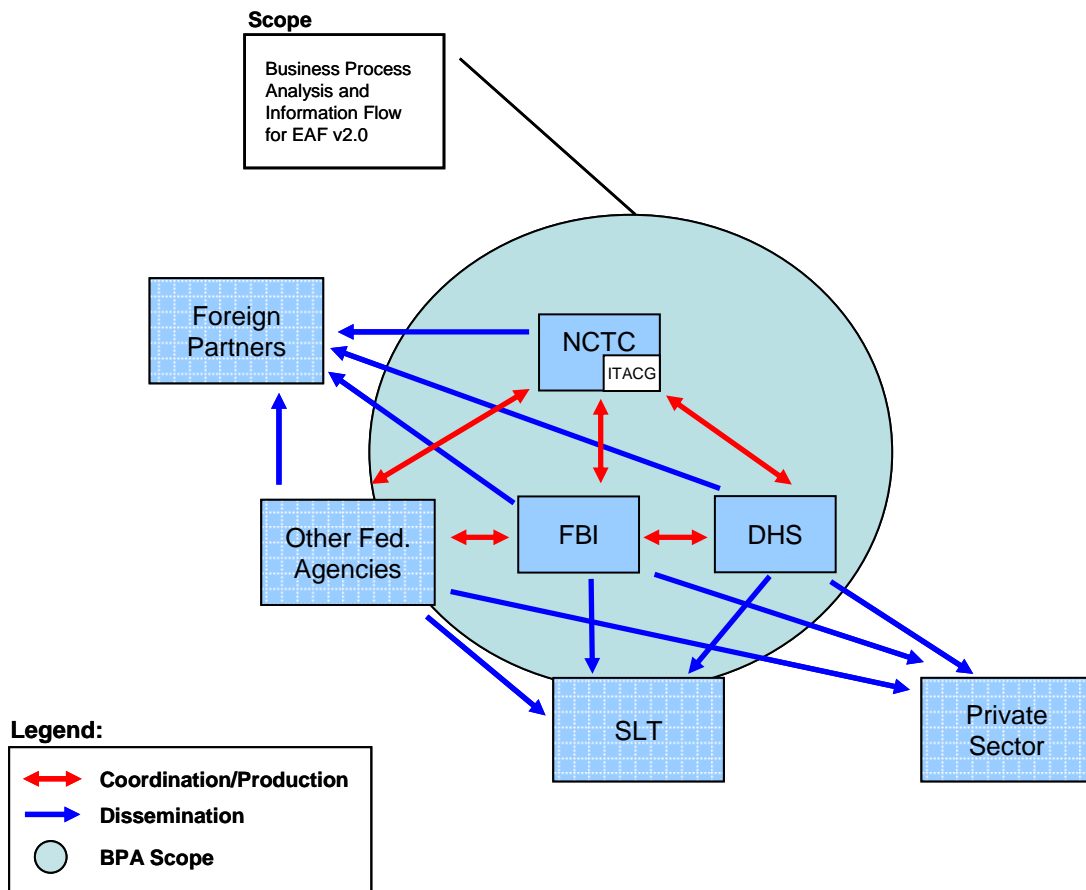


Figure 1: Scope of ISE AWN Business Process Analysis

III. Definitions

The Program Manager for the Information Sharing Environment (PM-ISE) preliminary findings on AWN definitions indicate the need for common AWN definitions for the ISE. The different titles and content of Federal agencies' AWN products leave their recipients without clarity as to what is an alert, a warning or a notification; or which AWN products contain urgent versus more general threat information. Recipients must comb through the contents of sometimes conflicting and sometimes duplicate AWN products to determine the nature, meaning and significance of the information contained in them. This puts an added burden on resource challenged organizations. Even the efforts of resource robust organizations to clarify federally disseminated AWN information may still result in discrepancies and vagueness. Consequently, organizations struggle with prioritizing their responses to the AWN information they receive, due to a lack of commonly understood AWN definitions. This struggle is compounded in crisis situations when prompt and effective responses are necessary. Organizations also struggle to provide clear feedback on Federal AWN information and often talk at cross purposes. Thus, a lack of common AWN definitions for the ISE hurts the AWN mission.

Despite the lack of ISE AWN definitions and the subsequent challenges, the Federal Government does have a commonly understood process for coordinating and producing federally coordinated ISE AWN products. The PM-ISE describes this process in Section V of this appendix; this process does accommodate the definitions Federal agencies have of ISE AWNs. This process aims to produce as outputs common federally coordinated ISE AWN products, drawing upon the different types of ISE AWN information and perspectives among the Federal agencies that participate in the process. The outputs of this process do include certain ISE AWN products whose titles and descriptions are commonly understood and accepted by Federal agencies as federally coordinated ISE AWN products regarding threats with a foreign nexus.

Federal agency representatives have begun efforts to define AWN for the ISE; these efforts helped set expectations for what an ISE AWN should encompass. Further work remains to finalize a standard set of ISE AWN definitions, which would help the Federal Government to improve the consistency of types of information included in agency ISE AWN products and assist recipients to better understand the nature and urgency of those products.²⁶ The PM-ISE recommends that Federal AWN producers determine what the common definitions should be for threats with a foreign and with an exclusively domestic nexus. These common definitions should build upon existing definitions. ISE AWN definitions should be broad enough to account for the various AWN terms and definitions currently in use both among and within agencies yet specific enough to precisely define an ISE AWN.

²⁶ The Information Sharing Council (ISC) Alerts Warnings Working Group established an initial set of ISE AWN definitions.

IV. Legislative and Policy Review

The ISE AWN process is driven by a myriad of statutory and non-statutory requirements that guide the roles and responsibilities of Federal agencies in the production, coordination and dissemination of terrorism-related AWN products for the ISE. This section provides a high-level overview of these authorities.

A. The Homeland Security Act of 2002

The Homeland Security Act of 2002 (the Homeland Security Act), as amended, gives the Department of Homeland Security (DHS) the authority to administer the Homeland Security Advisory System and to issue warnings. Specifically, the Secretary of DHS has the authority to establish and administer the Homeland Security Advisory System as a comprehensive and effective means to provide advisories or warnings regarding the threat or risk that acts of terrorism will be committed on the homeland to Federal and SLT government authorities and to the people of the U.S. According to the Homeland Security Act, in administering this advisory system, the Secretary of DHS shall:

1. Establish criteria and methodology for the issuance and revocation of advisories or warnings.
2. Provide specific information and advice regarding appropriate protective measures and countermeasures that may be taken in response to the threat or risk.
3. Wherever possible, limit the scope to a specific region, locality, or economic sector believed to be under threat or at risk.
4. Not use color designations as the exclusive means of specifying homeland security threat conditions that are the subject of the advisory or warning.

B. 28 C.F.R. Section 0.85

Authorized by *28 C.F.R. Section 0.85*, the Attorney General has long exercised authority to share information with SLT and private sector partners. This authority is based, in part, on his broad statutory authority to detect, investigate and prosecute crimes and primary investigative responsibility for all Federal crimes of terrorism, which often involves the analysis and sharing of information with SLT officials and the private sector. The Attorney General has designated the FBI the lead investigative agency for intelligence and counterterrorism (CT).

FBI's role as a lead agency for investigating terrorism matters is supported by various Presidential Decision Directives (PDD). For example:

PDD-39 sets forth the U.S. counterterrorism policy and outlines the FBI's jurisdictional responsibilities in relation to terrorism: "unless otherwise specified by the Attorney General, the FBI shall have lead responsibility for operational response

to terrorist incidents that take place within U.S. territory or that occur in international waters and do not involve the flag vessel of a foreign country. Within this role, the FBI functions as the on-scene manager for the U.S. Government." Moreover, "the FBI shall have lead responsibility for investigating terrorist acts planned or carried out by foreign or domestic terrorist groups in the U.S. or which are directed at U.S. citizens or institutions abroad."

PDD-62 grants the Department of Justice, acting through the FBI, lead agency or operational response authority to an incident.

PDD-63 directs that the National Infrastructure Protection Center (NIPC) serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity and that its mission "will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response." Under the directive, the Department of Justice/FBI has been given the responsibility for the Emergency Law Enforcement Services Sector. Helping assure the security of law enforcement agencies across the United States greatly increases preparedness to deal with terrorist incidents.

C. Executive Order 13354: National Counterterrorism Center

Issued on August 27, 2004, *Executive Order (E.O.) 13354: National Counterterrorism Center*, authorizes the NCTC to "disseminate transnational terrorism information, including current terrorism threat analysis, to the President, the Vice President in the performance of Executive functions, the Secretaries of State, Defense, and Homeland Security, the Attorney General, the Director of Central Intelligence Agency, and other officials of the executive branch when approved by the Central Intelligence Agency (Sec 5 (c))." In addition, "NCTC must support DHS, the Department of Justice (DOJ), and other appropriate agencies, in fulfillment of their responsibility, to disseminate terrorism information to State and local government officials, and other entities, and coordinate dissemination of terrorism information to foreign governments (Sec 5(d))."

D. The Intelligence Reform and Terrorism Prevention Act of 2004

Section 102(A)

Section 102(A) of *Intelligence Reform and Terrorism Prevention Act of 2004, as amended (IRTPA)* authorizes the DNI with the responsibility to provide national intelligence (to include terrorism-related intelligence) to the President, the heads of departments and agencies of the Executive Branch, the Chairman of the Joint Chiefs of Staff, the Senate and House of Representatives and other such persons as the Director of National Intelligence (DNI) determines to be appropriate.

Section 1021

Section 1021 of IRTPA, designates the NCTC “as the primary organization for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism.”²⁷ NCTC must also “assign roles and responsibilities as part of its strategic operational planning duties to lead departments and agencies for counterterrorism activities, but shall not direct the execution of any resulting operations.”²⁸ Furthermore, the NCTC shall: “ensure that agencies have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis;” “ensure that such agencies have access to and receive intelligence needed to accomplish their assigned activities;” and “serve as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support.”²⁹

IRTPA also delegates specific responsibilities to the NCTC regarding domestic CT intelligence. Section 1021 designates that the “Center [NCTC] may, consistent with applicable law, the direction of the President, and the guidelines referred to in section 102A(b), receive intelligence pertaining exclusively to domestic counterterrorism from any Federal, State, or local government or other source necessary to fulfill its responsibilities and retain and disseminate such intelligence.”³⁰ “Any agency authorized to conduct counterterrorism activities may request information from the Center to assist it in its responsibilities, consistent with applicable law and the guidelines referred to in section 102A(b).”³¹

Section 1011

Section 1011 of IRTPA provides that the DNI’s authority to determine requirements and priorities for, and manage and direct the dissemination of national intelligence by intelligence community (IC) elements, does not apply to the direct dissemination of information to SLT government and private sector officials under Sections 201 and 892 of the Homeland Security Act.

E. The Implementing Recommendations of the 9/11 Commission Act of 2007

On August 3, 2007, the *Implementing Recommendations of the 9/11 Commission Act of 2007* (the 9/11 Act) established the ITACG at NCTC to improve the sharing of information within the scope of the ISE, established under Section 1016 of IRTPA, with

²⁷ IRTPA, as amended, Section 1021(d) (1).

²⁸ IRTPA, as amended, Section 1021(d) (3).

²⁹ IRTPA, as amended, Section 1021(d) (4)-(6).

³⁰ IRTPA, as amended, Section 1021(e) (1).

³¹ IRTPA, as amended, Section 1021(e) (2).

SLT and private sector officials.³² The DNI, through the PM-ISE, in coordination with the Secretary of DHS, shall coordinate and oversee the creation of the ITACG. The ITACG is responsible for developing federally coordinated terrorism information products, including AWNs and updates of time-sensitive information related to terrorism threats for SLT organizations and the private sector.

F. The National Strategy for Information Sharing

Issued by the President in October 2007, the NSIS outlines specific activities for the Federal Government, in coordination with SLT authorities, to establish processes to manage the issuance of AWNs to State and major urban area fusion centers regarding time sensitive threats and other information requiring some type of State and/or local reaction or response.³³ In addition, the NSIS identifies activities for how State and major urban area fusion centers are encouraged to ensure that alert, warnings or notifications are disseminated, as appropriate, to SLT authorities, the private sector and the general public.³⁴

G. The Fusion Center Guidelines

Issued in August 2006, the Fusion Center Guidelines direct DOJ, DHS, the Office of the Director of National Intelligence and the Department of Defense to draw upon existing and ongoing efforts at the Federal level to establish a coordinated set of policies, protocols, and procedures to (among other things) ensure that no gaps exist in production capabilities as they relate to the production of AWN regarding time sensitive threats. Additionally, the Federal Government is directed to maintain the capability to produce and coordinate multi-channel dissemination of Federal-level inter-agency coordinated AWNs of time sensitive terrorism-related information.

V. High-level ISE AWN Process

This section describes a high level Federal ISE AWN process commonly understood among Federal agencies with ISE AWN responsibilities. This process contains activities that Federal agencies perform in support of the ISE AWN mission. The ISE AWN process activities include: (1) analysis of information by Federal agencies; (2) coordination among key ISE AWN producers and production of federally coordinated ISE AWN products; (3) dissemination of those products to Federal, SLT, private sector partners and foreign partners; and (4) follow-up activities.³⁵ The PM-ISE developed this

³² IRTPA, as amended, Section 210D.

³³ NSIS, p A1-7.

³⁴ NSIS, p A1-8.

³⁵ Coordination among Federal AWN producers, development of federally coordinated AWN products, dissemination of those products to SLT and private sector partners, and follow-up from SLT to the Federal Government, are key requirements of the NSIS. See NSIS, pp. A1-7 and A1-8.

Federal ISE AWN process based upon its discussions with NCTC, ITACG, FBI, DHS, and other Federal AWN producers and recipients.³⁶

The Federal ISE AWN process applies to threats with either a foreign or a domestic terrorism nexus.³⁷ However, the degree to which agencies are involved, and their respective roles (i.e., analysis, coordination, production, and dissemination); may change for threats with a foreign versus domestic nexus. (See pages F-20 – F-31 and Figures 3 and 4 for the ISE AWN Information Flow and Narrative.)

For threats with a foreign nexus, NCTC, ITACG, DHS, FBI and other IC agencies are key participants in the analysis, coordination, production and dissemination of ISE AWNs. The NCTC is designated as the primary organization for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to foreign-related terrorism and CT.³⁸ Following the analysis and integration of intelligence by members of the IC, or receipt of warning intelligence developed elsewhere, the IICT, administered by NCTC, coordinates and produces foreign-related ISE AWNs. Organized within the NCTC, the ITACG supports the efforts of the NCTC to produce federally coordinated terrorism-related information products intended for dissemination to SLT officials and private sector partners through existing channels established by Federal departments and agencies. ITACG is responsible for facilitating the development of federally coordinated terrorism AWNs and updates of time sensitive information related to terrorism threats produced for SLT governments and the private sector. NCTC disseminates these AWNs to national policy makers (to include the President, his Cabinet, and the National Security Council) and Federal agencies. FBI and DHS disseminate foreign-related ISE AWN products to SLT and private sector partners.

For exclusively domestic threats, DHS, FBI and other Federal agencies, except intelligence community (IC) agencies and IC elements within DHS and FBI; coordinate, produce and disseminate ISE AWNs. The ITACG provides input on and assists in developing ISE AWNs suitable for SLT organizations and the private sector. As with threats with a foreign nexus, DHS and FBI are the main channels for disseminating Federal AWN products with a domestic nexus to SLT and private sector partners. (Refer to Section VI for more detailed descriptions of agency roles.)

The Federal ISE AWN process can be grouped into four phases: Analysis, Coordination and Production; Dissemination; and Follow-up (Figure 2). Steps for each phase of the process are detailed below. While the phases of this process represent functions that agencies, to greater and lesser degrees, currently carry out, the PM-ISE refers to this process in Figure 2 as a “Should-Be” process, because it outlines activities Federal

³⁶ The other Federal producers of ISE AWNs from whom we gathered input for this BPA include: Defense Intelligence Agency (DIA), Department of Commerce (DOC), Department of Energy (DOE), Department of Health and Human Services (HHS), Department of the Interior (DOI), Department of Transportation (DOT), Department of the Treasury, and the United States Department of Agriculture (USDA).

³⁷ Federal agencies could also apply this process to non-terrorism information.

³⁸ IRTPA, as amended, Section 1021(d) (1).

agencies should perform in accordance with laws, policies and NSIS objectives. The process begins when a Federal agency becomes aware of a terrorism-related threat through intelligence-gathering or law enforcement operations. Information on threats to the homeland can come from State and local officials, fusion centers, or other Federal agencies. A Federal agency obtaining terrorism threat information will analyze it and share it with other Federal agencies. The output of this analysis is input to the Coordination and Production phase. The output of the Coordination and Production phase of the ISE AWN process is an approved ISE AWN product. The Dissemination phase provides a disseminated ISE AWN as an output. The Follow-up phase begins with Step 6, Monitor Threat Information, and ends with Step 10 De-escalate AWN or Step 12, Retract AWN.

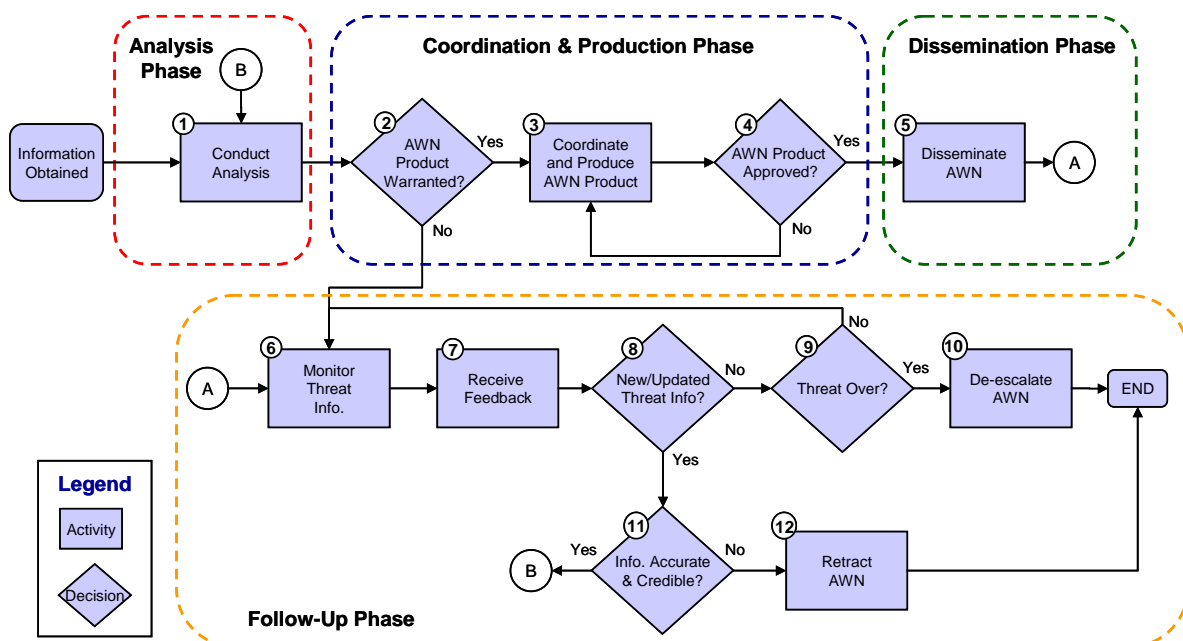


Figure 2: High Level Federal ISE AWN “Should-Be” Process

A. Analysis

Agencies analyze threat information prior to sharing it. Sharing of analyzed threat information is a prelude to coordination and production activities. Agency analysis of threat information is described below in Step 1.

Step 1—Conduct Analysis

The agency that initially receives threat information analyzes it to assess the reliability and credibility of its source. Agency officials check existing intelligence to determine whether domestic threat information has a foreign terrorism nexus. If the agency with the initial threat information does not have the analytic capability to assess the reliability and credibility of the source, that agency shares the information with an appropriate agency with such capability (e.g., FBI or DHS or IC agencies) allowing them to lead the

effort in assessing the threat and then disseminate any required ISE AWN through their channels.

Federal agencies use several means to routinely share threat information. These means include: shared access to intelligence information systems across agencies; published Intelligence Information Reports (IIRs) and other forms of raw intelligence reporting, Intelligence Bulletins, Situational Awareness Reports (SitReps), the Central Intelligence Agency's (CIA) Telegraphic Dissemination (TD); the daily Threat Matrix, or participation in the three times per day, NCTC-hosted, secure video teleconference (SVTC) meetings. Agencies also receive threat information from the National Washington Area Alert System (NWAAS); and the National Operations and Intelligence Watch Officers Network (NOIWON).

B. Coordination and Production

Steps 2-4 of the Federal ISE AWN process pertain to coordination among Federal agencies for the production of federally coordinated ISE AWN products. Coordination and production includes the approval of ISE AWN products by key Federal ISE AWN process participants.

Step 2—AWN Product Warranted? (Sensitive content withheld: overall classification of the document is Unclassified)

Step 3—Coordinate and Produce AWN Product

If an ISE AWN is warranted, Federal agencies coordinate the production of ISE AWNs, to the extent that time and operational priorities allow. ISE AWNs are coordinated federally to ensure that recipients receive the most clear, consistent, and credible information feasible. ISE threats with a foreign nexus and/or target are coordinated using the IICT process. The thrice daily SVTC calls are the mechanisms for participants to share information on ISE AWN threat analysis, which can contribute to ISE AWN production. In addition, the ITACG reviews IICT products to ensure that SLT and private sector needs are met, by seeking to ensure that specific, relevant threats are shared at the lowest feasible security classification level, including unclassified For Official Use Only (FOUO), and that the content of the threat information is useful and relevant for SLT and private sector partners.

For ISE threats with a purely domestic nature, FBI leads ISE AWN coordination and production in concert with DHS, ITACG and other Federal agencies, as relevant. Many other Federal, non-IC agencies have specific missions that include sharing of information that may be terrorism-related, for instance Health and Human Services (HHS). DHS and FBI are integral parts of these agencies' information coordination and sharing efforts, providing a level of Federal coordination for domestic threats.

Step 4—AWN Product Approved?

For foreign terrorism threat products, the IICT Executive Secretariat assigns a drafter and coordinates with the other key IC agencies via IC E-mail to approve the product. For domestic terrorism threat products, DHS and FBI rely on their respective processes to approve products. Agencies take this step for threats whose urgency level allows time for inter-agency coordination. Otherwise, agencies unilaterally develop AWN products relying only on internal agency approvals before dissemination. A “Yes” at this decision means the product is approved and Step 5, Disseminate, occurs next. A “No” means further coordination (Step 3) is required to get approval for product dissemination.

C. Dissemination

The Dissemination phase consists of Step 5 of the process. It involves Federal agencies disseminating ISE AWN products. DHS and FBI are the primary Federal channels for disseminating ISE AWN products, of foreign terrorism nexus and domestic terrorism nexus, to SLT governments, the private sector and foreign partners.

Step 5—Disseminate AWN

The dissemination activity occurs, following ISE AWN product approval, through multiple organizational channels. All IICT products are disseminated across the Federal government at the appropriate security levels via IC agencies. Agencies forward ISE AWN products, at the appropriate security levels, to their identified constituent recipients. DHS and the FBI are the primary means for ISE AWN distribution, including foreign threats, to the SLT governments, fusion centers, private sector partners and critical infrastructure/key resource (CI/KR) operators.

DHS and FBI also have the Federal mandate to distribute threats with a purely domestic nexus down to SLT officials. A number of other Federal agencies also have specific AWN responsibilities as part of their broader missions. (Some examples of these other Federal agencies are the Center for Disease Control, part of HHS, and the Federal Aviation Administration). These agencies disseminate AWN products to their constituencies, including public health constituencies, SLT, and specific private sector constituencies.

D. Follow up

Steps 6-12 discuss follow-up activities after ISE AWN products have been disseminated.

Step 6—Monitor Threat Information

If an ISE AWN threat product is not deemed warranted (see Step 2 AWN Product Warranted? decision), individual agencies monitor information to determine if there are changes to the threat situation. Similarly, if an ISE AWN product is distributed (Step 5, Disseminate AWN); the recipient organizations evaluate updated information for changes to, and for clarification of, the threat. This information is monitored, and shared, throughout ISE participant agencies, as applicable.

Step 7—Receive Feedback

SLT and private sector partners, fusion centers and our foreign allies provide the U.S. Government with feedback on the status of actions taken in response to ISE AWN. Federal agencies use that feedback to gain further knowledge about the current threat and to develop future AWN products.

Step 8—New/Updated Threat Information?

This decision point regarding whether there is New/Updated Threat Information is a continuous activity taken during the on-going monitoring (Step 6) of the threat. It is connected to further decision points regarding whether the threat is over (Step 9) or whether the new threat information indicates that the information in the AWN product was accurate and credible (Step 11).

Step 9—Threat Over?

If the threat is not yet over, the monitoring activity (Step 6) continues. If the threat is over, the De-escalate AWN activity (Step 10) follows.

Step 10—De-escalate AWN

If a threat is over, the ISE AWN is de-escalated by the disseminating agency as soon as is feasible, allowing the potentially impacted parties, such as law enforcement, to stand down for this threat. This can be done through either the establishment of a standard expiration date for each specific category of AWN, the implicit or explicit establishment of an expiration date for specific information within the AWN product, or through a follow up to the original AWN message.

Step 11—Information Accurate and Credible?

When new or updated threat information is received (Step 8), the determination of whether the original information was accurate and credible is made by IICT members for a foreign nexus threat or by the FBI or the original disseminating agency for an exclusively domestic threat. If the original information was not accurate or credible (“No”), the Retract AWN activity (Step 11) follows. If the new information confirms

and/or adds to the original threat information (“Yes”), Conduct Analysis (Step 1) is begun again, followed by a new determination whether an additional ISE AWN product is warranted.

Step 12—Retract AWN

ISE AWNs are retracted by IICT members for a foreign nexus or by the FBI or the original disseminating agency for a domestic threat, if further threat information reveals that the information in the original ISE AWN was not accurate or credible. An AWN retraction allows the potentially impacted parties, such as law enforcement, to stand down their alert for that specific threat and to re-prioritize their focus.

END

The process ends following either the de-escalation (step 10) or the retraction (step 12) of the ISE AWN.

VI. Major Federal ISE AWN Roles

Several Federal agencies have major roles within the ISE AWN process. In keeping with Guideline 2 and the NSIS; this section focuses on NCTC, DHS, FBI and ITACG roles as major Federal AWN participants in analysis, coordination and production, Federal dissemination and follow up of Federal ISE AWN.

A. NCTC Roles in the Federal ISE AWN Process

The NCTC role in the ISE AWN process includes analysis of terrorism information and the distribution of that analysis, oversight of the federal production of foreign intelligence on terrorism, coordination and production of ISE AWN with a foreign nexus across the government, the dissemination of the resulting foreign intelligence to national policy makers (to include the President, his Cabinet, and the National Security Council); and on-going monitoring of terrorism threat information.

A.1. Analysis

According to E.O. 13354, the NCTC is to “disseminate transnational Terrorism information, including current terrorism threat analysis” to national policy makers and to serve in the oversight role for terrorism information analysis.³⁹ The NCTC analytic processes provide analytic support to the decision-making and development of ISE AWNs with terrorism information analysis. NCTC monitors the various threat streams and analyzes threat information it receives. NCTC documents threat information in the daily Threat Matrix and provides situational awareness information in the twice daily situational awareness reports. Helping to assure the completeness of this monitoring

³⁹ (U)E.O. 13354: National Counterterrorism Center, (Section 5(C)).

process the FBI Counter Terrorism Watch, the CIA Counter Terrorism Center Watch and the Joint Intelligence Task Force CT defense intelligence unit are integrated into the NCTC watch operations center.

A.2. Coordination of ISE AWN Production

The NCTC is responsible for coordinating the production of federally coordinated ISE AWNs of a foreign terrorism nexus for the Federal Government. The NCTC uses the processes established by the IICT as the primary mechanism for doing this coordination and production. The IICT process is initiated upon receipt of information indicating a credible threat to U.S. interests, personnel, or facilities. The agency recognizing the need requests the IICT Executive Secretariat, which is located within the NCTC Directorate of Intelligence, to seek a decision on whether to proceed with an Alert or Advisory.⁴⁰ If agreed to, the IICT Executive Secretariat then assigns a primary drafting agency to initiate production of the ISE AWN. The resulting draft is then coordinated according to IICT procedures. All IICT products are coordinated among key IICT participants. Other agencies coordinate when appropriate, e.g., Treasury for questions of terrorist financing and DOE and NRC for a threat to a nuclear power plant. Once ready for release, the product is sent by multiple communications media to include IC E-mail. Record communications (e.g. cables/messages) and hardcopies of the AWN product are produced for executive distribution to the President's Daily Briefing (PDB) staff for distribution to the briefer of the Senior Principals (President, Vice President, Secretary of State, Secretary of Defense, etc.). The production of Threat Assessments is also governed under the IICT process. However, a consensus among the key IICT members is not necessary to develop an Assessment, although Assessments are coordinated among IICT participants.

A.3. Dissemination

NCTC has the primary Federal responsibility for disseminating terrorist threat information to national policy makers and to all Federal agencies. Included in this responsibility is the dissemination of ISE AWNs for threats with a foreign nexus. Through increasingly prevalent access to the NCTC On-line (NOL) portal, some SLT and regional fusion centers users are receiving ISE AWNs directly from NCTC. However, this provision is a secondary role, with the FBI and DHS serving as the primary disseminators of ISE AWN to fusion centers.

A.4. Follow-up

The NCTC performs follow-up activities by monitoring the various threat streams on an on-going basis. NCTC analyzes any new or updated threat information. NCTC will reflect any updated threat information in the daily Threat Matrix and twice daily situational awareness reports. This monitoring and analysis is used across the IC to

⁴⁰ (U) *Guidelines for Intelligence Community Terrorist Threat Warning System*, June 26, 2007.

make decisions regarding the need for additional AWN, for de-escalation or retraction, and for counterterrorism action.

B. ITACG Roles in the Federal ISE AWN Process

The purpose of the ITACG is to facilitate the sharing of information between Federal, SLT, and private sector partners. ITACG informs and helps shape IC threat, situational awareness, and finished intelligence reporting; identifies relevant information of interest to SLT and private sector partners; and reviews the information to ensure it serves the interests of SLT and private sector partners, and provides input to publications to reflect counterterrorism needs and SLT and private sector interests.⁴¹

B.1. Analysis

The ITACG's role in analysis as part of the ISE AWN process is limited. The ITACG reviews analysis primarily produced by other agencies to advise those agencies on information that is relevant to SLT and private sector partners for inclusion in an ISE AWN.

B.2. Coordination of ISE AWN Production

The ITACG plays an important role in the coordination and production process as it advises DHS, the FBI, NCTC and other IC agencies on how they can make their threat information and products more relevant and accessible to SLT partners and the private sector.

The ITACG obtains threat information for review from a variety of IC and Law Enforcement CT information systems and databases across all security domains [Unclassified, Secret and Top Secret/Sensitive Compartmented Information (SCI)]. The ITACG also attends daily SVTC meetings as an observer; FBI Counterterrorism Watch turnover meetings; NJTTF meetings; and other IC-related briefings in order to obtain additional threat-related information.⁴²

Next, the ITACG identifies information that would be of interest to SLTs, and to other Stakeholders.

For post-dissemination review, ITACG reviews finished ISE AWN.

The ITACG checks whether ISE AWN eligible for downgrade are already present on systems within lower security domains and available to SLT and private sector partners. ITACG then works with the product originator to determine whether products marked Secret should be re-written at the FOUO level. The ITACG also checks whether products posted on Law Enforcement Online (LEO) and Homeland Security Information

⁴¹ ITACG SOP DRAFT (FOUO), p. 1.

⁴² ITACG SOP DRAFT (FOUO), p. 7.

Network (HSIN) are also posted on other systems accessible to SLT and private sector partners to help ensure maximum distribution.

B.3. Dissemination

The ITACG does not disseminate ISE AWNs.

B.4. Follow-up

The ITACG participates in Follow-up to the extent of following intelligence relating to ongoing monitoring of the various threat streams and making recommendations regarding the need for additional ISE AWN products or for retraction or de-escalation notices.

C. DHS Roles in the Federal ISE AWN Process

DHS' role in the Federal ISE AWN process is to analyze information from the IC and DHS Components; coordinate both the production of threats to the homeland with a foreign nexus and those threats with a domestic nexus; and to provide dissemination of ISE AWN to SLT and private sector authorities, and when appropriate, to the public.

C.1. Analysis

Within DHS there are approximately seven major line organizations, as well as a number of specialty elements, capable of producing information related to threats to the homeland. This provides a broad base of input to producing ISE AWNs, should the circumstance arise. DHS analysis provides the entry of the information into the ISE AWN process.

C.2. Coordination and Production

Coordination amongst Stakeholder are developed here to determine whether existing terrorism threat intelligence has relevance to new threat information received. If so, appropriate follow on steps are taken. If threat information is of a purely domestic nature, DHS coordinates with the FBI and the FBI Counterterrorism Watch (CT Watch). As part of this coordination process, DHS works with the FBI to develop a "dual seal" product for dissemination to their respective stakeholders. DHS disseminates the AWN information in the form of a Situational Awareness Note (SAN) or a Chief Intelligence Officer (CINT) Note. The ITACG reviews DHS ISE AWN products and provides suggestions regarding information useful to SLT governments and the private sector. NCTC, time permitting, is included in the sharing of this type of threat information but does not influence the coordination or production process for purely domestic threats to the Homeland.

C.3. Dissemination

Upon coordination and approval of an ISE AWN, DHS disseminates information to four primary stakeholder types: Federal agencies, State and major urban area fusion centers, the private sector, and SLT officials. The ISE AWN reaches a wide variety of personnel including Homeland Security Advisors, fusion centers and their partners, and SLT officials, typically law enforcement.

Primary conduits for ISE AWN products from DHS to SLT government entities are the State and major urban area fusion centers.⁴³ Fusion centers and Homeland Security Advisors directly receive the ISE AWN through e-mail and decide on further dissemination that includes local law enforcement and key government personnel. DHS ISE AWN reaches the private sector either directly from DHS or via fusion centers. In both cases the ISE AWN is intended for critical infrastructure and key personnel. Depending on the threat, additional private sector entities could receive the ISE AWN.

C.4. Follow-up

DHS' role in follow-up includes monitoring and analyzing threat-related intelligence, making decisions regarding the need for additional ISE AWN or for retraction or de-escalation notices as a result of new threat information, and establishing processes for SLT to provide feedback on actions taken as a response to ISE AWN. DHS' role is to use the feedback provided to inform decisions and content regarding future threat warning activities and ISE AWN products.

D. FBI Roles in the Federal ISE AWN Process

The FBI is an Intelligence and Law Enforcement entity primarily responsible for investigating and disrupting terrorist, cyber and foreign intelligence threats to the U.S. It is also the primary collector of terrorism-related intelligence inside the U.S. Hence, the role of the FBI in the Federal ISE AWN process is to provide initial threat information analysis, coordination and production, dissemination, and follow-up activities.

D.1. Analysis

The alert, advisory, and warning process begins when the FBI acquires information about terrorist planning, operations, or techniques.⁴⁴ The first determination is whether or not this terrorist activity has a foreign nexus. If this activity does have foreign nexus then the FBI invokes the processes of the IICT.⁴⁵ If the information is not clear (i.e. the activity implied by the information is questionable in its origin) the information will typically be entered into the threat matrix and during one of the daily secure video

⁴³ DHS and FBI also disseminate directly to over 40,000 SLT partners via their existing email distribution lists.

⁴⁴ The terms Alert, Advisory and Warning given here are as used by the FBI, and while they have similar meanings they are not precisely the same terms.

⁴⁵ For a more complete description of the IICT Process see the discussion in section VI, A, above.

teleconferences it will be discussed by the participants. If other information is related to this questionable data and it now brings some clarity to the original information such that the IC feels it has the basis for an alert/advisory then the IICT process for determining whether an ISE AWN should be produced and disseminated is followed.

On the other hand, if the determination is that the information that the FBI has obtained is for a purely domestic threat, it invokes processes developed jointly with DHS. The nature and urgency of the information determines the required product – alert, advisory or warning – and the coordination and dissemination method.

D.2. Coordination and Production

If the FBI determines that the information is not extremely urgent, the FBI CT Division will begin the coordination process by sending the information to DHS, Office of Intelligence and Analysis (OIA), Intelligence Watch and Warning Division (IWW). The IWW will coordinate the information within DHS. DHS and FBI representatives may coordinate with ITACG, if time allows. Once this coordination is completed DHS and FBI will disseminate the alert and advisory message with both agency seals on the document.⁴⁶ The FBI also provides the information to the NCTC. The FBI Strategic Information and Operations Center (SIOC) disseminates the joint seal alert and advisory message to FBI field offices, Joint Terrorism Task Forces (JTTF), Field Intelligence Groups (FIG), fusion centers, State Homeland Security Advisors, and State and local police agencies. The JTTF or the local field component would coordinate the sharing of the alert and advisory message with private sector entities. When the threat is deemed to be extremely urgent, interagency coordination may be minimal or may not occur in advance of ISE AWN dissemination.

D.3. Dissemination

The FBI's dissemination process depends upon to whom they are sending information. The FBI communicates with its field components and state and local law enforcement via LEO, FBINet, telephone, E-mail, blackberry and pagers. The FBI also uses the National Law Enforcement Telecommunications System (NLETS) and FBINet to communicate ISE AWN information to local law enforcement. The FBI communicates with fusion centers through LEO and their JTTF or FIG personnel who are assigned to the fusion center. Additionally, State Homeland Security Advisors have access to LEO. The FBI passes information to the private sector through DHS, fusion centers, a telephone call, or a visit.

The FBI uses warning messages when there is a sense of urgency associated with the information. Warning messages are usually disseminated to a smaller group via

⁴⁶ DHS calls these joint products CINT Notes; FBI calls them SIOC Law Enforcement Alert Messages (SLAMs). Regardless of the name difference, the content of these joint DHS-FBI products is similar.

telephone or blackberry. Depending on the urgency, coordination with NCTC and others may be completed after the FBI sends a warning message.

D.4. Follow-up

Like DHS, the FBI's role in follow-up includes monitoring and analyzing threat-related intelligence, making decisions regarding the need for additional ISE AWN or for retraction or de-escalation notices as a result of new threat information, and establishing processes for SLT to provide feedback on actions taken in response to an ISE AWN. The FBI's role is to use the feedback information provided to inform decisions and content regarding future threat warning activities and ISE AWN products.

However, despite their role, the FBI has no formal process for de-escalation of ISE AWN. The FBI tracks their alert and advisory messages, which are SIOC Law Enforcement Alert Messages, by date and subject or title but does not have the information technology support needed to track by threat stream in order to facilitate sending de-escalation messages. Updating the alert and advisory messages is ad hoc with changes communicated directly to organizations and entities involved and those interacting with the FBI. The FBI uses NLETS, LEO, and other internal communications systems or the internet to pass the information updates.

VII. Conclusions

The Federal Government currently has processes that enable Federal-wide coordination on the production of ISE AWN for terrorist threat information of both foreign and domestic origin. The Federal ISE AWN process provides all ISE participants with a process for coordinating threat information, producing coordinated ISE AWNs, and disseminating and receiving ISE AWNs, according to their need. ISE AWNs can be disseminated and received by a wide variety of means, including telephone, pager, e-mail, retrieval from an electronic portal, and facsimile. When implemented as it should be, this process is both effective and robust enough to meet stakeholder requirements.

ISE Federal AWN Information Flows and Narratives

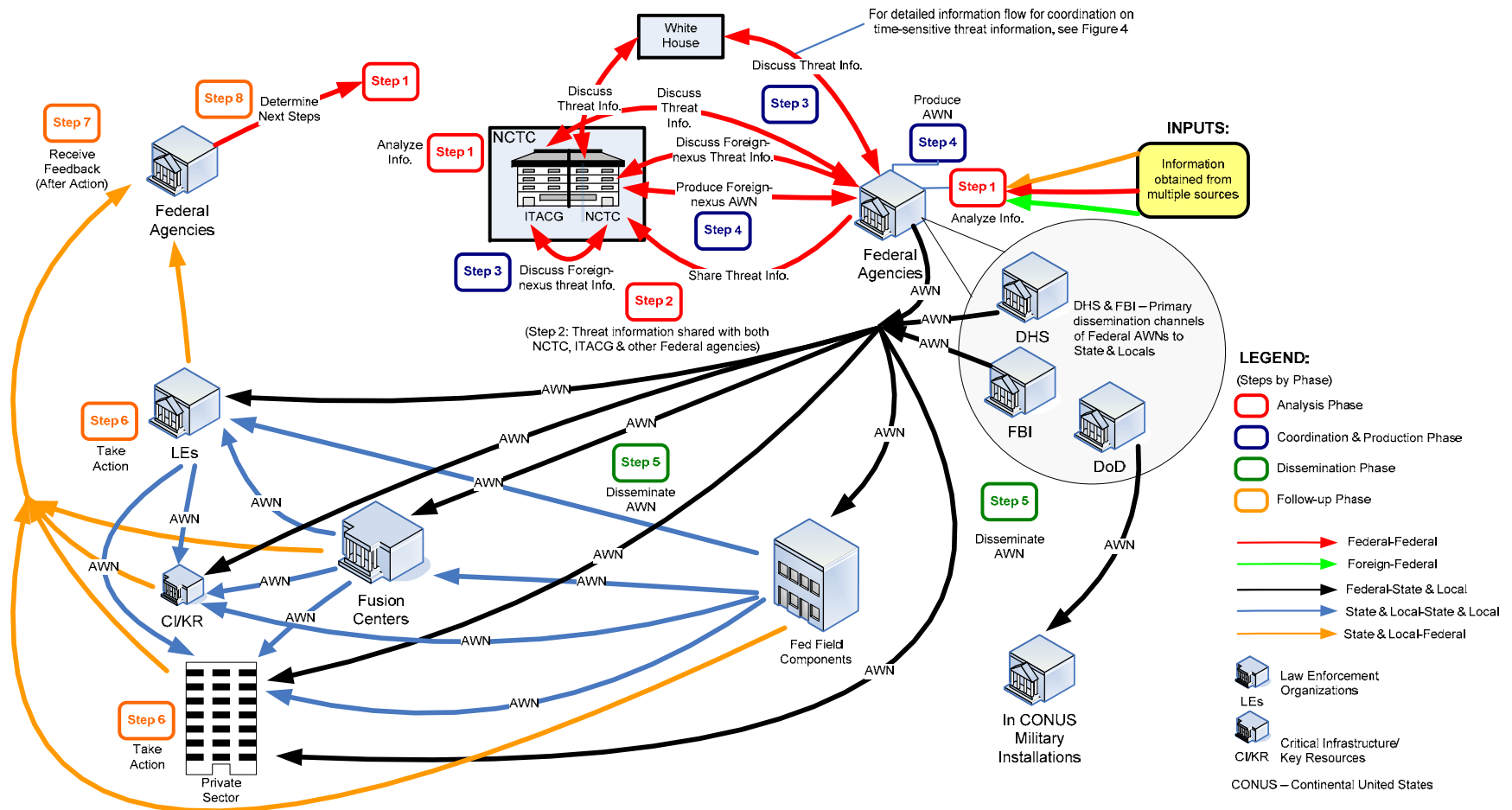


Figure 3: ISE High Level Federal AWN “Should-Be” Information Flow

ISE High Level Federal AWN Information Flow Narrative

Step	Activity	Process	Notes
(U) ANALYSIS PHASE			
1	Analyze Information	Federal agencies receive terrorism information from multiple sources: SLT, private sector, operators of critical infrastructure/key resources and other Federal agencies. Federal agencies evaluate the terrorist threat and other types of information they receive. They check the reliability of the source and/or analyze the reported information in concert with other intelligence and reporting. After internal analysis, Federal agencies share their terrorism threat information with NCTC. The Federal agency that first obtained the threat information will share it and discuss it with other Federal agencies, as appropriate, in addition to NCTC.	
2	Share Threat Information	Federal Agencies share Controlled Unclassified Information using classified and unclassified email, phone, fax, etc. Classified email is via IC-Email on the Joint Worldwide Intelligence Communications System (JWICS) or on the SIPRNET. Federal agency users may use enterprise unclassified email, such as UGov, hosted by the CIA's Agency Internet (AIN). Authorized Federal users may also share threat information using Intelink at all three security domains. Federal Agencies also share threat information with the White House. Prior to discussion of threat information with other Federal agencies, NCTC analyzes the threat information they receive from Federal agencies, using additional information NCTC draws from the Terrorist Identity Environment (TIDE) database. NCTC integrates threat information from other Federal agencies with TIDE information and its own terrorism-related intelligence.	Federal agencies from all five ISE communities may initially receive threat information from various sources or uncover threat information in the course of daily operations. Federal agencies share terrorism threat information of both a foreign nexus and an exclusively domestic nexus with NCTC.
(U) COORDINATION AND PRODUCTION PHASE			
3	Discuss Threat Information	Threats with Foreign terrorism nexus: NCTC puts together a classified "Threat Matrix" and Sit Rep (situational	NCTC invites Federal Agencies (beyond the IC and DHS and FBI) to participate in

Step	Activity	Process	Notes
		<p>awareness report – worldwide) and communicates this to various IC agencies, ITACG, DHS, FBI and other agencies, as applicable, through the daily Secure Video Teleconference (SVTC) meetings.</p> <p>Federal coordination partners for foreign nexus threats—NCTC, IC agencies, DHS, FBI, and other Federal agencies, as applicable—use the daily SVTC meetings as the mechanisms to discuss threat information and as precursor discussion to the decision regarding producing an ISE AWN and which type of AWN is required. Discussion via SVTC meetings is the main mechanism for federal-wide coordination on threat information with a foreign nexus. (ITACG is a listen-only participant.)</p> <p>ITACG representatives discuss inclusion of additional information of value, as needed, to SLT and private sector partners with DHS and FBI representatives via email, phone and fax, both prior to and after SVTC meetings. DHS, FBI, and NCTC representatives present ITACG perspectives at SVTC meetings upon the ITACG's request. ITACG does not produce AWN products but provides input to agencies that do, especially DHS and FBI.</p> <p>Threats with an exclusively Domestic terrorism nexus:</p> <p>Federal agencies send threat information that is exclusively domestic in nature to DHS and FBI in addition to NCTC. DHS and FBI confirm that threat information is exclusively domestic in nature by checking intelligence products posted on NCTC On-line (NOL), usually the classified portal. DHS and FBI may also discuss with NCTC representatives whether domestic threat information has a foreign terrorism nexus.</p> <p>DHS discusses threat information with representatives from other non-IC Federal agencies at its National Operations Center (NOC), using unclassified and IC-E-mail, phone, fax, and in-person discussions. FBI is included among those agencies at the DHS NOC. NOC and DHS Intelligence & Analysis officials will</p>	<p>SVTC meetings, depending on the nature of the threat information.</p> <p>Based on the contents of the Threat Matrix, NCTC would recommend to the participants of the SVTC which type of AWN product, if any, is required.</p> <p><i>(NOTE: NCTC does not focus on threat information that is exclusively domestic; thus on the Information Flow Diagram, the word "Foreign-nexus" has been inserted in the descriptions of Step 3 Discuss Threat Information and Step 4, Produce AWN arrows to denote that NCTC discusses and coordinates on Foreign threat information only.) "Steps 3 & 4" have been placed next to Federal agencies to denote that Federal agencies, except NCTC and other IC agencies, discuss exclusively domestic threat information and produce exclusively domestic ISE AWN products. DHS and FBI are usually leads in producing exclusively domestic ISE AWNs.</i></p> <p>Based on the urgency or the nature of the threat NCTC can issue a warning if there is not enough time to coordinate. Other agencies may do the same, provided the urgency precludes discussion in the production of federally coordinated threat products.</p>

Step	Activity	Process	Notes
		<p>also coordinate. Likewise, DHS and FBI Intelligence elements coordinate, especially in producing joint DHS-FBI products (DHS CINT Notes and FBI SLAMs).</p> <p>ITACG representatives pull finished DHS and FBI threat intelligence products from various classified and unclassified electronic sources and provide information of value to SLT and private sector. Unclassified electronic sources include:</p> <ul style="list-style-type: none"> • NOL (portal) • Homeland Security Information Network (HSIN) (portal) • Law Enforcement Online (LEO) (portal) • NIPRNET (Network) • AIN and Open Source systems and networks 	
4	Produce AWN	<p>Threats with Foreign terrorism nexus:</p> <p>When NCTC and key IC agencies participating in the IICT decide to develop an ISE AWN, the IICT Secretariat assigns drafting responsibilities to a Federal agency with the appropriate expertise. The IICT Secretariat leads the development of draft threat products, in concert with other agencies, via IC-E-mail. NCTC also coordinates their final approval via IC-E-mail.</p> <p>DHS and FBI produce individual ISE AWNs and joint ISE AWNs. Joint DHS-FBI ISE AWNs are DHS CINT Notes and FBI SLAMs. DHS works with other non-IC Federal agencies in developing exclusively domestic ISE AWN products.</p> <p>Threats with an exclusively Domestic terrorism nexus:</p> <p>ITACG representatives also pull drafts of DHS and FBI AWN products and provide input to DHS and FBI via unclassified and IC-E-mail. ITACG representatives pull finished AWN products from various classified and unclassified electronic resources across intelligence, law enforcement, homeland security and defense communities. Unclassified resources are mentioned above.</p>	

Step	Activity	Process	Notes
		ITACG assists the development of domestic ISE AWN by providing information of relevance to SLT and private sector partners.	
(U) DISSEMINATION PHASE			
5	Disseminate AWN	<p>DHS and FBI disseminate federally coordinated threat products of both foreign and domestic threats to SLT law enforcement organizations, fusion centers and the private sector primarily through:</p> <ul style="list-style-type: none"> • DHS HSIN • FBI LEO • NOL • Other Federal agencies' Portals/databases • Unclassified E-mail <p>Classified threat products are posted to DHS and FBI web pages on SIPRNET and JWICS and on NOL-S. NCTC, DHS and FBI as well as other Federal agencies also disseminate threat products to foreign partners via email. Joint DHS-FBI products—CINT Notes (DHS) and SLAMs (FBI)—are communicated via Blackberry, email, pager; and posted to NOL, HSIN and LEO.</p> <p>NCTC, DHS, FBI and other Federal agencies disseminate threat products to authorized Federal agencies.</p>	
(U) FOLLOW-UP PHASE			
6	Take Action	SLT law enforcement officials, private sector officials and Federal field agents will take the appropriate actions, as needed, in response to receiving AWN information and products from the Federal Government.	
7	Receive Feedback (After Action)	Federal agencies who disseminate Federal threat products should obtain feedback from their recipients. These include SLT Law Enforcement organizations, the private sector, critical infrastructure and key resources operators, and Federal field components. Feedback mechanisms include unclassified and classified email, phone, fax and meetings. Authorized users at	The reporting agency should monitor the response of the recipients and the situation in order to update the AWN.

Step	Activity	Process	Notes
		SLT levels of unclassified portals such as NOL, HISN, LEO and other agency portals may use feedback mechanisms contained within them such as notifications, chat and posting updated information.	
8	Determine Next Steps	Federal agencies that disseminated their threat products to SLT Law Enforcement organizations, the private sector, critical infrastructure and key resources operators, and Federal field components, should review feedback and determine the nature and credibility of the information. This will assist in determining next steps, particularly de-escalating a threat or retracting a threat message, based on new, more accurate information. If new information is more credible and accurate, Federal agencies will determine whether new information is credible and accurate through analysis, which brings the information flow back to Step 1. Federal agencies will go through the process again, using the same mechanisms (phone, fax, email, meetings, portals, etc.) to conclude whether to de-escalate threats or retract threat messages. They will in turn disseminate any retracted messages and information on de-escalating threats.	

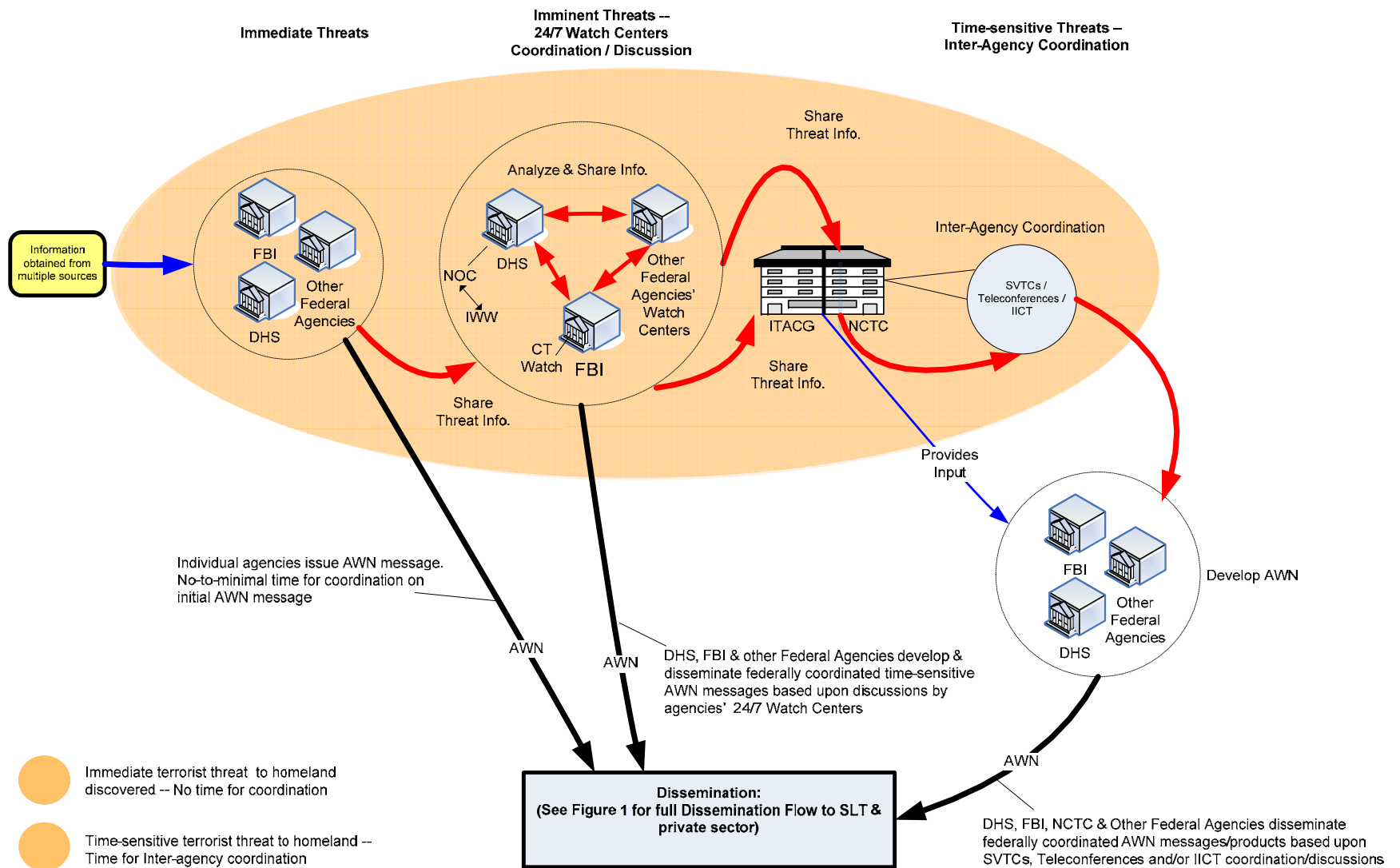


Figure 4: ISE AWN High Level Information Flow for Inter-agency Coordination on Time Sensitive Threats

ISE High-Level AWN Information Flow Narrative for Inter-Agency Coordination on Time Sensitive Threats⁴⁷

Process
IMMEDIATE THREATS
<p>Immediate Terrorist Threats indicate threats where there is no time for inter-agency coordination/discussion prior to the issuance of an initial alert, warning, or notification (AWN). Therefore, there will be minimal analysis of the information; rather the agency or agencies obtaining the information will focus on source verification and disseminating that information out to their State, Local, Tribal (SLT) and private sector partners. A secure video teleconference (SVTC) or teleconference may also be convened, as appropriate, as time permits. The Federal Bureau of Investigation (FBI) notifies their respective Field Office and Joint Terrorism Task Force (JTTF) to immediately begin their operations, investigation, and outreach to the appropriate SLT and private sector partners. As Federal Agencies disseminate the threat information they also provide it to operational and intelligence elements among agencies' 24 hour, 7 days a week (24/7) Watch Centers for action they deem appropriate. Supervisory personnel within the Watch Centers may develop and disseminate a subsequent AWN if they deem it necessary. Concurrently, the Watch Centers share the threat information with the National Counterterrorism Center (NCTC), which in turn provides that information at the next SVTC.⁴⁸</p>
IMMINENT THREATS – 24/7 WATCH CENTER COORDINATION / DISCUSSION
<p>Time sensitive threats with inter-agency coordination among Federal Watch Centers pertain to time-sensitive threats for which there is time for coordination/discussion among different agencies' 24/7 Watch Centers prior to disseminating an initial AWN. Federal Watch Centers evaluate the terrorist threat information by checking the reliability of the source and/or analyzing the reported information in concert with other threat reporting and intelligence. Coordination among agency Watch Centers will involve analysis of the threat information in conjunction with the sharing and discussion with other Watch Center personnel either in person, by email, by facsimile (fax), by teleconference or SVTC. The DHS National Operations Center (NOC) and the FBI Security Intelligence and Operations Center (SIOC) are lead Watch Centers. DHS has representatives from other agencies collocated at the DHS NOC. As intelligence, operational and Watch Center personnel develop an initial AWN as a result of their coordination, they share the threat information with NCTC. NCTC ensures active collaboration through the Interagency Intelligence Committee on Terrorism (IICT) and daily SVTC's.</p>

⁴⁷ This ISE AWN information flow and narrative for inter-agency coordination on time-sensitive threats represents input from PM-ISE staff and key Federal AWN stakeholders: NCTC Community Integration Group; DHS Office of Intelligence Watch and Warning located within the DHS National Operations Center; and the FBI, Counterterrorism Watch Office.

⁴⁸ Secure video teleconferences (SVTC) references can be found in "Statement for the Record House Permanent Select Committee on Intelligence and House Armed Services Committee, July 25, 2007: Implications of the NIE The Terrorism Threat to the US Homeland" by Edward Gistaro, National Intelligence Officer/Transnational Threats, Office of the Director of National Intelligence & Michael Leiter, Principal Deputy Director National Counterterrorism Center, and in the NCTC.gov Press Room, "Statement for the Record before the House Armed Services Committee" by The Honorable John Scott Redd, Director, National Counterterrorism Center Vice Admiral, United States Navy (Ret.), April 4, 2006.

Process
TIME SENSITIVE THREATS – INTER-AGENCY COORDINATION
<p>Time sensitive threats with inter-agency coordination pertain to time-sensitive threats for which there is time for inter-agency coordination via at least a SVTC meeting, teleconference, IICT coordination, or series of e-mail exchanges. Agencies participating in the daily SVTC and/or teleconferences include representatives from key IC components and other agencies with information and intelligence relevant to the threat under discussion. Additional Federal Agencies are invited to participate in the SVTC by the National Security Council's (NSC) Counterterrorism Support Group (CSG), depending upon the nature of the threat, along with White House Principals. The SVTC discussions will result in federally coordinated information about threats to the homeland. This federally coordinated information will be reflected in AWN messages/products that agencies develop and then disseminate to Field Offices and/or SLT and private sector partners.</p>

Data Elements

The following is a sample of data elements found in an existing AWN standard established by the Organization for the Advancement of Structured Information Standards (OASIS) titled Common Alerting Protocol (CAP) version 1.1.⁴⁹

AWN Structure

Alert

The <alert> segment provides basic information about the current message: its purpose, its source and its status, as well as unique identifier for the current message and links to any other, related messages. An <alert> segment may be used alone for message acknowledgements, cancellations or other system functions, but most <alert> segments will include at least one <info> segment.

Information

The <info> segment describes an anticipated or actual event in terms of its urgency (time available to prepare), severity (intensity of impact) and certainty (confidence in the observation or prediction), as well as providing both categorical and textual descriptions of the subject event. It may also provide instructions for appropriate response by

⁴⁹ http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf. OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification, can be obtained from the OASIS President.

message recipients and various other details (hazard duration, technical parameters, contact information, links to additional information sources, etc.) Multiple <info> segments may be used to describe differing parameters (e.g., for different probability or intensity “bands”) or to provide the information in multiple languages.

Resource

The <resource> segment provides an optional reference to additional information related to the <info> segment within which it appears in the form of a digital asset such as an image or audio file.

Area

The <area> segment describes a geographic area to which the <info> segment in which it appears applies. Textual and coded descriptions (such as postal codes) are supported, but the preferred representations use geospatial shapes (polygons and circles) and an altitude or altitude range, expressed in standard latitude / longitude / altitude terms in accordance with a specified geospatial datum.

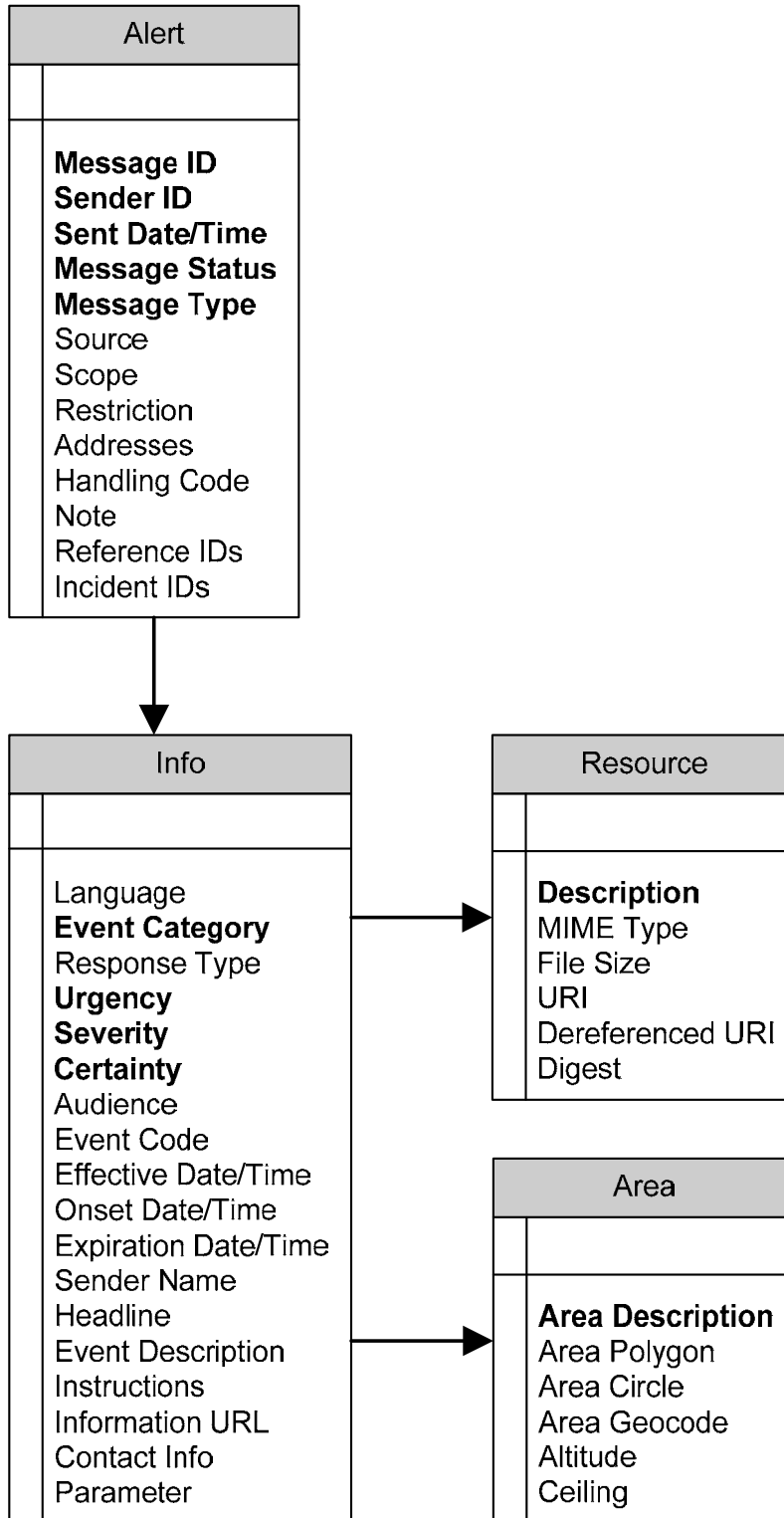


Figure 5: Awn Document Object Model

Appendix G – ISE Shared Spaces and Core Discussion

Document Purpose and Intended Audience

This paper responds to a tasking from members of the Information Sharing Council (ISC) to address the question “What is an Information Sharing Environment (ISE) Shared Space?” In developing the paper, we realize that “What is an ISE Core?” is also a relevant and appropriate question to address at this time. To address both questions completely and formally, this paper first provides in Section 2 the context for ISE Shared Spaces and ISE Core, as developed in the ISE Enterprise Architecture Framework.⁵⁰ Then, Section 3 provides both general and technical definitions of ISE Shared Space and ISE Core. Going beyond definitions, Section 4.1 presents three implementation models for ISE Shared Spaces. Section 4.2 provides implementation models for ISE Core as both common services and infrastructure. Taken all together, the sections in this paper provide overarching descriptive concepts and approaches that may be used by ISE participants in identifying existing infrastructure to implement the ISE (either a Shared Space or Core) or in planning for and establishing an ISE Shared Space or Core. Section 5 presents a summary and suggestions for further discussion.

While this paper is in response to a question from members of the Information Sharing Council (ISC), the intended audience also includes program managers and systems/network designers of information technology resources in ISE participant organizations that will be responsible for leveraging existing infrastructure, planning, designing, and installing their organization’s ISE Shared Spaces or Core.

Context⁵¹

As envisioned for today, the ISE infrastructure comprises two key components: (1) ISE Shared Spaces and the (2) ISE Core.⁵² These two components derive from a statement of need, a set of mandates, and a number of foundational concepts and assumptions.

Statement of Need

The long-term vision for information sharing within the ISE is to allow authorized users (investigators, analysts, others with various missions) to search, discover, and access data when needed. Search and discovery involves conducting queries of disparate information and finding data from sources a user may otherwise not know exist. Users will be allowed access to structured, unstructured, finished, unfinished, and source information as appropriate, depending on their mission needs, clearances, and other

⁵⁰ ISE Enterprise Architecture Framework, version 1.0, August 2007, available at http://www.ise.gov/docs/eaf/ISE-EAF_v1.0_20070830.pdf.

⁵¹ This section highlights the references and key concepts that led to the formation of the ISE Share Space vision and definition. Much has been written about the ISE in general and interested readers are referred to <http://www.ise.gov/pages/vision.html>.

⁵² ISE Enterprise Architecture Framework, version 1.0, August 2007, available at http://www.ise.gov/docs/eaf/ISE-EAF_v1.0_20070830.pdf.

access privileges.⁵³ Achieving this vision requires development and/or implementation of several expanded features of highest priority:

- First, systems must be compatible and have the capability to interconnect. Information can only be searched, discovered, and accessed if the user has the necessary cyber connectivity.
- Second, there must be a robust access and identity management capability, allowing users to access only that data for which they are authorized. Organizations will not make their information available to others unless adequate protection is provided. Without access and identity management services to provide that protection, organizations will block access to their data.
- Third, systems must provide proper levels of protection for information that moves between users or organizations at each security level.
- Fourth, because of the management difficulties associated with multiple accounts and passwords, long-term technical capabilities should support single sign-on for users.⁵⁴
- Fifth, there must be an agreed standard for user vetting and account provisioning and de-provisioning. Today's schemes vary by organization.
- Finally, there must be agreement on system certification and accreditation standards; multiple standards are currently in use.

These dependencies are representative components of what is commonly referred to as *system trust*. Without system trust, organizations are reluctant to share their information because of the risk that information could be lost, corrupted, or otherwise compromised.

The long-term ISE vision requires organizations to develop and accept a level of system trust much higher than that which exists today. Growing that trust depends on policy and cultural changes that support authorized access for all ISE participants. While ISE participants currently share information and have made significant progress since 9/11, further enhancement opportunities are envisioned. Sharing mechanisms today include, but are not limited to, the ability for a user to access information that another organization has made available in a protected access repository; the use of subscription services to direct selected data to authorized consumers; posting of information on Web pages; and relay of information by e-mail. Such sharing techniques remain valuable and will continue to be used for sharing information pending implementation of the envisioned end-state.

For the intervening period, there is a continued need to enhance the amount and timeliness of information being shared. After considering a number of potential

⁵³ The long-term vision of the ISE includes the sharing, as appropriate, of various forms of source, or raw, data. If a user has access only to finished products and the authors of those products have failed to "connect the dots" then the user will not have the information needed to connect the dots either.

⁵⁴ This requires a community-accepted identity management approach.

approaches, the concept of ISE Share Spaces and ISE Core has been developed for information sharing today.

Mandates

The Intelligence Reform and Terrorism Prevention Act, as amended (IRTPA), requires the ISE to facilitate the sharing of terrorism, homeland security, and weapons of mass destruction information⁵⁵ within and among all levels of governments and the private sector.

To accomplish this sharing, the concept of ISE Shared Spaces has been developed to address immediate shortfalls and is documented within the *ISE Enterprise Architecture Framework (ISE EAF)*. ISE Shared Spaces are where information is shared based upon clearly identified ISE-level mission needs for such information and commonly agreed to business processes and information flows. The ISE Core is the infrastructure made up of enterprise services, networks and systems that interconnect the individual ISE Shared Spaces into a functioning system of systems.

Many specific examples demonstrate that sharing today is occurring using the ISE Shared Spaces and ISE Core approach. The Terrorist Identities Datamart Environment (TIDE), hosted by the National Counter-Terrorism Center (NCTC) and distributed by the Terrorist Screening Center (TSC) is one example. Also, law enforcement information shared by Department of Justice (DOJ) through OneDOJ and Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE) through Regional Sharing System are both standardized shared spaces. However, both of these examples can be improved to ensure the information is accessible by all appropriate ISE participants.

Recognizing the breadth of participants the ISE is intended to unify, ISE Shared Spaces and the ISE Core also provide the means for ISE participants with national security system (NSS)⁵⁶ network assets, historically sequestered with only other NSS systems, to interface with ISE participants having only civil network assets. Furthermore, ISE Shared Spaces and ISE Core also provide the means for foreign partners to interface and share terrorism information with their U.S. counterparts.

In short, ISE Shared Spaces and the ISE Core allow ISE participants to leverage, for information sharing purposes, their technologies and processes that are tightly coupled to their missions to support the larger national counterterrorism (CT) mission called for

⁵⁵ As recommended in the *ISE Implementation Plan*, the ISE has also been expanded to include the sharing of law enforcement information related to terrorism. Formal definitions of ISE-related information are available at <http://www.ise.gov/pages/scope.html>.

⁵⁶ 40 U.S.C. Section 11103(a) defines a *national security system* as “a telecommunications or information system operated by the Federal government, the function, operation, or use of which: (A) involves intelligence activities; (B) involves cryptologic activities related to national security; (C) involves command and control of military forces; (D) involves equipment that is an integral part of a weapon or weapons system; or (E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions. (2) Limitation.—Paragraph (1) (E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personal management applications).”

by the President in *National Strategy for Information Sharing (NSIS)*, the Congress in IRTPA, and the 9/11 Commission.

Foundational Concepts and Examples

Establishing and applying standards to information is a commonly-used mechanism to enhance organizational ability to share that information. The standards for ISE Shared Spaces and the ISE Core are documented by the Common Terrorism Information Sharing Standards (CTISS) Program.⁵⁷ Consistent with the discussion above, CTISS are formally defined as business process-driven, performance-based common standards for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. .

As stated in the *ISE Implementation Plan*, “terrorism information sharing and interoperability with the ISE need to be integral attributes of departments’ and agencies’ overall information resource planning and enterprise architectures.”⁵⁸ As such, both ISE Shared Spaces and the ISE Core include a capital planning and investment perspective consistent with requirements specified through the White House Office of Management and Budget (OMB) regarding the Capital Planning and Investment Control (CPIC) and Federal Enterprise Architecture (FEA) programs.

A key challenge in this work is identifying, organizing, and prioritizing the information sharing needs of the national CT mission. Using the framework of information or knowledge management cycles,⁵⁹ information sharing needs can be grouped into two categories: (1) supporting, enabling, and improving dissemination activities with structured, vetted, and finished information products and (2) supporting, enabling, and improving the sharing of information used and needed throughout the cycle. The general belief is that improvements in category 1 are easier to achieve than in category 2. Fortunately, ISE Shared Spaces and the ISE Core can support, enable, and improve sharing in both categories.

Definitions

General

ISE Shared Space: An ISE Shared Space is where standardized terrorism information, as defined through the Common Terrorism Information Sharing Standards (CTISS), is made available by one ISE participant to others, as appropriate. Additionally, ISE

⁵⁷ As defined in *ISE Administrative Memorandum-300*, available at <http://www.ise.gov/docs/ctiss/ise-asm300-ctiss-issuance.pdf>.

⁵⁸ PM-ISE, *ISE Implementation Plan* (Washington: PM-ISE, 2006), page 107.

⁵⁹ For discussion here, the Intelligence Cycle has 5 activities: planning and direction, collection, processing, analysis and production, and dissemination. This cycle is used for example only, other information or knowledge management cycles, like law enforcement investigation cycle or the [O-O-D-A Loop](#), are equally relevant.

participants may create or use an ISE Shared Space to make services accessible, as appropriate, to other ISE participants.

ISE Core: The ISE Core provides infrastructure and services necessary for the interconnection and use of information made available through ISE Shared Spaces. The ISE Core exists within and across three information security domains (i.e., TS/SCI, Secret/Collateral, and CUI/SBU).

Technical

ISE Shared Space: An ISE Shared Space consists of hardware and software that serve as the 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 other data stewardship requirements are met and that the ISE Shared Space capability supports established ISE mission processes.

ISE Core: The ISE Core has three major components: core services, portal services, and core transport. ISE Core Services provides ISE-level services used in operating the ISE (e.g., Discovery, Mediation, Security, Storage, Messaging, Collaboration, Information Security). ISE Core Portal Services provide the infrastructure for those services used in interfacing ISE portals 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.

Models

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 to be considered:

- Establishing an information flow-driven model for an ISE Shared Space,
- Logical view model (or system-independent operational descriptions), and
- Hosting and implementation model.

These models support ISE participants in their development of enterprise, segment, and solution architectures⁶⁰ that clearly identify the structure and attributes of the organization's ISE Shared Spaces in sufficient detail to support fiscal year programmatic plans for information technology business case justification, acquisition, installation, operations, and management.

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. 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 ISE participant's information. These essentials are easily identified from the defined information flows from mission business processes that define 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. Functional standards of the CTISS define the business processes, information flows, and structured data (data elements and schema) that make up terrorism information products within these information flows for storage in an ISE Shared Space. A current example of this is Suspicious Activity Reporting (SAR), which has a well-defined information flow and associated Functional Standard (ISE-FS-200) and defined data and information for sharing in an ISE Shared Space.
- *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 (i.e., 'entity'). For example, they may be processes associated with the immigration mission business process which specifically aligns with DHS' Immigration and Customs Enforcement agency.

⁶⁰ Segment architecture refers to a business-driven approach to defining and designing, in addition to other supporting architectural components, each ISE participant's ISE Shared Space. It leverages the Federal Enterprise Architecture Consolidated Reference Model (CRM), the *ISE EAF*, and the *Federal Transition Framework Catalog* to build a layered architecture. Solution architecture refers to a business-driven approach to develop shareable assets and information technology components in support of business processes identified in the ISE EAF and participant segment architectures.

Logical 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, search, and directory services for access and use. A common 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. A common 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.
- *Hybrid*: Allowing direct access, with appropriate access management safeguards, to selected applications within an ISE participant's infrastructure. For example, 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 DOJ's Joint Automated Booking Systems (JABS).

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 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 EA*. 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 an ISE Shared Space, Department X remains ultimately responsible for the data stored and consumed within the third party resources servicing Department X's ISE Shared Space.

ISE Core

Elements of the ISE Core are resourced, planned, installed, and operated by designated ISE Implementation Agents. 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 (may also be 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.

Hosting and Implementation Model

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

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

Summary and Additional Issues for Discussion

ISE Shared Spaces and the ISE Core are key concepts in developing system trust within the ISE today. Both have general and technical definitions, and a variety of models must be considered when selecting existing systems or developing an ISE Shared Space or the ISE Core that meets the agreed upon standards for improving mission-related information sharing.

Different combinations of the models may be followed by an ISE participant for implementation. In all cases, however, an ISE Shared Space and the ISE Core must be based upon a clearly identified ISE-level mission need for such information and commonly agreed to business processes and information flows. Such a standardized

approach resolves the information processing and usage problem by providing places where alignment of information sharing policies, business processes, technologies, and systems occurs.

The concepts here support discussions and planning efforts concerning difficult implementation issues critical to success, such as:

Concept	Applicable FEA ISE profile area
Connectivity	Component framework / Data management
Search and Discovery	Service interface & integration / interface
Access and Identity Management	Service access & delivery identity management
Information Security	Information & Technology Management / Information Security
Funding and resource management	Management of Government Resources / Financial & HR Management
Governance	Business Management Services / Management of Process

This page intentionally blank.

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

(202) 331-2490

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

