

**ISE Enterprise Architecture Framework**

*Version 1.0*

*August 2007*



# **INFORMATION SHARING ENVIRONMENT ENTERPRISE ARCHITECTURE FRAMEWORK**

Prepared by the  
Program Manager, Information Sharing Environment

This page intentionally blank.

---

## TABLE OF CONTENTS

<b>List of Figures .....</b>	<b>iv</b>
<b>List of Tables .....</b>	<b>v</b>
<b>Executive Summary .....</b>	<b>vii</b>
<b>Chapter 1 – Introduction .....</b>	<b>1</b>
1.1 Purpose and Scope .....	1
1.2 ISE EAF Description Review and Release Approach .....	1
1.3 Definitions .....	2
1.3.1 Terrorism, Homeland Security, and Law Enforcement Information as it Relates to Terrorism .....	2
1.3.2 Information Sharing Environment .....	3
1.3.3 ISE Participants .....	4
1.4 Background .....	4
1.4.1 Rationale .....	4
1.4.2 Vision .....	5
1.4.3 ISE Operational Concept .....	6
1.4.4 Impacted Organizations .....	6
1.4.5 Key Expectations for the ISE EAF .....	7
1.5 ISE EAF Product Set .....	7
<b>Chapter 2 – Policy, Governance, and Requirements .....</b>	<b>9</b>
2.1 Policy and Governance .....	9
2.2 Enterprise Architecture Principles .....	10
2.2.1 ISE EAF Overarching Principles .....	10
2.2.2 ISE EAF Operating Principles .....	10
2.2.3 ISE EAF Technical Principles .....	11
2.2.4 ISE EAF Configuration Management .....	11
2.3 ISE Requirements .....	12
2.4 Mapping the Presidential Guidelines to the EAF .....	14
<b>Chapter 3 – ISE EAF Overview .....</b>	<b>15</b>
3.1 General Description .....	15
3.2 ISE Enterprise Architecture Framework (ISE EAF) .....	16
3.3 Architecture Partitions .....	18
3.4 ISE Implementer’s View and Segments .....	18
3.5 The Federal Transition Framework Catalog .....	20
3.6 Common Terrorism Information Sharing Standards .....	20
<b>Chapter 4 – Business Partition .....</b>	<b>23</b>
4.1 Introduction .....	23
4.2 Baseline Business Partition .....	24
4.2.1 ISE Baseline Business Reference Model .....	24
4.3 Target Business Partition .....	25
4.3.1 ISE Target BRM .....	25
4.3.2 Initial Set of Target Business Processes .....	27
4.3.3 ISE Business Process Modeling Methodologies .....	31

---

4.4 Business Partition Transition Strategy .....	32
<b>Chapter 5 – Data Partition .....</b>	<b>35</b>
5.1 Introduction.....	35
5.2 Baseline Data Partition .....	35
5.2.1 Functional Standards .....	36
5.2.2 Linkage between Business and Data Partitions .....	36
5.3 TO-BE Data Partition.....	37
5.3.1 Overview .....	37
5.3.2 Compliance with the FEA Data Reference Model .....	37
5.4 Data Partition Transition Strategy.....	40
5.4.1 The CTISS Development Process .....	40
5.4.2 Critical Success Factors.....	44
5.4.3 Observations and Issues.....	44
<b>Chapter 6 – Application and Service Partition.....</b>	<b>47</b>
6.1 Introduction.....	47
6.1.1 Overview .....	47
6.1.2 Terminology .....	47
6.1.3 Architectural Products .....	48
6.2 FEA Service Reference Model Mapping.....	49
6.3 Baseline Application and Service Partition .....	51
6.4 Application and Service Target Partition – ISE Core Segment.....	51
6.4.1 Overview .....	51
6.4.2 Transport.....	52
6.4.3 Network Management Function .....	54
6.4.4 ISE Portal Services .....	54
6.4.5 ISE Management Portal .....	56
6.4.6 ISE Core Services .....	57
6.5 Target Application and Service Partition – ISE Participant Segment.....	63
6.6 Application and Service Partition Transition Strategy .....	64
6.6.1 ISE Core Transition.....	64
6.6.2 Participant Enterprise Architecture Transition .....	65
<b>Chapter 7 – Technical Partition.....</b>	<b>67</b>
7.1 Introduction.....	67
7.2 Technical Reference Model Mapping .....	68
7.3 Common Terrorism Information Sharing Standards .....	70
7.4 Service-Based Architecture .....	72
7.5 Enterprise Application Integration.....	74
7.5.1 Data Integration Patterns .....	75
7.5.2 Function Integration Patterns .....	76
7.5.3 Example Pattern: Publishing a Service to ISE.....	77
7.6 Transport .....	78
7.7 Information Assurance.....	80
7.7.1 Information Assurance Overview .....	80
7.7.2 Information Assurance Categories .....	82
7.7.3 Four Partitions of the ISE Architect’s View .....	87

7.7.4 IA Controls and Countermeasures .....	87
7.8 Standards .....	88
7.9 Technical Partition Transition Strategy .....	91
<b>Chapter 8 – Implementer’s View .....</b>	<b>93</b>

Appendix A. Acronyms

Appendix B. Glossary

Appendix C. Bibliography

Appendix D. Architecture Principles

Appendix E. ISE Requirements

Appendix F. ISE Business Reference Model Figures

Appendix G. Example Enterprise Integration Pattern

Appendix H. ISE Business Process Descriptions

Appendix I. EAF to Presidential Guidelines Mapping

(Note: Individual appendices may be downloaded at Internet site [www.ise.gov](http://www.ise.gov))

## LIST OF FIGURES

Figure ES-1. The ISE Is a Virtual Environment to Share Terrorism Information.....	xi
Figure ES-2. The ISE Enterprise Architecture Framework Is Defined by Two Views and Four Partitions.....	xiii
Figure ES-3. Approved Guideline 2 Framework.....	xvi
Figure ES-4. Application and Service Partition of the ISE TO-BE Architecture.....	xix
Figure ES-5. ISE Enterprise Architecture Framework: Implementer’s View.....	xxi
Figure ES-6. IA Model.....	xxii
Figure ES-7. Suspicious Activity Report Process.....	xxiv
Figure 3-1. The ISE Is a Virtual Environment for Terrorism Information Sharing.....	16
Figure 3-2. ISE EAF Framework.....	17
Figure 3-3. OMB Guidance on the Use of Segment Architectures.....	19
Figure 4-1. The ISE BRM – Top Two Levels.....	25
Figure 4-2. The ISE Sub-Function Is Being Added to the FEA BRM.....	26
Figure 4-3. ISE Business Process Framework.....	27
Figure 4-4. Relationship Mapping of Mission Processes and ISE Core Services.....	29
Figure 4-5. Relationship Mapping of Service Processes and ISE Core Services.....	29
Figure 4-6. Overarching ISE Business Process Flow.....	30
Figure 4-7. Example Portion of a BPMN Diagram: Conduct Investigation.....	32
Figure 5-1. DRM Overview.....	38
Figure 5-2. DRM Abstract Model.....	39
Figure 5-3. CTISS Framework.....	40
Figure 5-4. CTISS Universal Core Development.....	41
Figure 5-5. CTISS Information Exchange Life Cycle.....	42
Figure 6-1. FEA Service Reference Model.....	48
Figure 6-2. Application and Service Partition of the ISE TO-BE Architecture.....	52
Figure 7-1. FEA Technical Reference Model.....	68
Figure 7-2. CTISS Framework.....	71
Figure 7-3. Service-Based Architecture.....	72
Figure 7-4. Example Pattern: Publishing a Service to the ISE.....	78
Figure 7-5. Typical Agency Connection to the ISE.....	79
Figure 7-6. IA Model.....	81
Figure 7-7. IA Relative to Four Partitions of the ISE Architect’s View.....	87
Figure 8-1. ISE Enterprise Architecture Framework: Implementer’s View.....	93

**LIST OF TABLES**

Table ES-1-1. Levels of Architectures .....	x
Table ES-1-2. ISE Architecture Partitions .....	xiv
Table 1-1. ISE Enterprise Architecture Framework Products .....	7
Table 3-1. ISE Architecture Partitions .....	18
Table 4-1. Business Partition Products .....	23
Table 4-2. Overarching ISE Business Process Descriptions.....	28
Table 5-1. Data Partition Products .....	35
Table 5-2. CTISS Information Exchange Life Cycle Support of the FEA DRM.....	44
Table 6-1. Application and Service Partition Products.....	49
Table 6-2. FEA Service Reference Model.....	50
Table 6-3. Mapping of ISE Core and Portal Services to SRM Service Domain and Type .....	50
Table 6-4. Discovery Service Capabilities .....	59
Table 6-5. Security Services Capabilities .....	60
Table 6-6. Mediation Service Capabilities .....	60
Table 6-7. Messaging Service Capabilities .....	61
Table 6-8. ESM Service Capabilities .....	62
Table 6-9. Storage Service Capabilities .....	62
Table 6-10. Collaboration Services Capabilities .....	63
Table 7-1. Technical Partition Products.....	67
Table 7-2. Technical Reference Model Mapping.....	69
Table 7-3. Data Integration Patterns .....	76
Table 7-4. Function Integration Patterns .....	76
Table 7-5. IA Categories .....	82
Table 7-6. ISE Technical Standards Under Consideration .....	89

This page intentionally blank.



# Executive Summary

## 1. Introduction

Section 1016 of the *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004*<sup>1</sup> 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 October 25, 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 December 16, 2005, the President issued a Memorandum for the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment that included requirements to *develop a common framework for the sharing of information* between and among executive departments and agencies and State, local, and tribal (SLT) governments, law enforcement agencies, and the private sector, and *define common standards* for how information is acquired, accessed, shared, and used within the ISE.<sup>2</sup>

The *Information Sharing Environment Implementation Plan*,<sup>3</sup> 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 program as a cross-community, perpetuating program 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

---

<sup>1</sup> *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, Public Law No. 108-458 (December 17, 2004). Section 1016 of IRTPA was amended on August 3, 2007 by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Public Law No. 110-53. This version of the ISE 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. 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.

<sup>2</sup> *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>.

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

instantiation of a nationwide counterterrorism ISE.<sup>4</sup> 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 counter-terrorism 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.”<sup>5</sup> This 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.”<sup>6</sup>

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,” the PM-ISE developed the ISE Enterprise Architecture Framework (ISE EAF)<sup>7</sup>. The ISE EAF and supporting Common Terrorism Information Sharing Standards (CTISS) help 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 ISE. Cross-ISE in nature, this ISE EAF provides descriptions of ISE business processes, information flows and relationships, services, and high-level data packet descriptions and exchange relationships. Overall this document meets three objectives:

- Provides a comprehensive, strategic description of the overall ISE architecture,<sup>8</sup>
- Establishes an architectural framework for implementing ISE capabilities; and
- Identifies key architectural decisions which have been made or must be made.

---

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

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

<sup>6</sup> Extracted from the Recommendations for Presidential Guideline 2, found at Internet site [www.ise.gov](http://www.ise.gov).

<sup>7</sup> 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.

<sup>8</sup> This is consistent with the requirement in the *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment* (White House: Washington, DC, 2005), that the “DNI shall direct the PM, in consultation with the ISC, to develop, in a manner consistent with applicable law, the policies, procedures, and architectures needed to create the ISE, which shall support the counterterrorism missions, roles, and responsibilities of executive departments and agencies.”

Consistent with IRTPA and EO 13388, this ISE EAF will drive long-term ISE technology improvement and information systems planning, investing, and integration to support the effective conduct of U.S. counterterrorism activities. The applicable types of information that traverse the ISE include terrorism information,<sup>9</sup> homeland security information,<sup>10</sup> and law enforcement information<sup>11</sup>.

Table ES-1-1 depicts the hierarchical relationships between 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 enterprise architecture planning. At the highest level, frameworks provide logical structures for classifying and organizing complex enterprise architecture information, and specifically the Federal Enterprise Architecture Framework (FEAF) provides “a structure for organizing Federal resources and for describing and managing Federal Enterprise Architecture activities.”<sup>12</sup> The ISE EAF, in turn, presents a logical structure of ISE business processes, information flows and relationships, services, and high-level data packet descriptions and exchange relationships. A companion document to the ISE EAF, the Federal Enterprise Architecture (FEA)-ISE Profile, 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. 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. Segment architectures

<sup>9</sup> The term “terrorism information” means “all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to: A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; C) communications of or by such groups or individuals; or D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.” [IRTPA, Section 1016(a)(4).]

<sup>10</sup> The term “homeland security information” means any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act. [Section 892(f)(1) of the Homeland Security Act (6 U.S.C. 482(f)(1))].




<sup>11</sup> For the purposes of the ISE, this addresses any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance. [Extracted from the Recommendations for Presidential Guideline 2.]

<sup>12</sup> CIO Council, *Federal Enterprise Architecture Framework, Version 1.1*, (CIO Council: Washington, DC, 1999), C-6.

drive decisions for a business case or group of business cases supporting a core mission area or common service. 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.<sup>13</sup>

The audience for this ISE EAF document, as Table ES-1-1 implies, are all stakeholders across the ISE and in particular the Chief Information Officers (CIOs) and enterprise architects of those Federal, State, local, and tribal (SLT) governments; private sector entities; and foreign allies that are participants in the ISE. 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. Based on the scope at the upper level, this ISE EAF reflects a subset of those FEAF components which are applicable to the ISE, and not the entire FEAF. As the establishment of the ISE will occur in two phases through June 2009, the ISE EAF will continue to evolve and incorporate newly developed mission and service business processes, to include information flows, and additional requirements into future published versions.

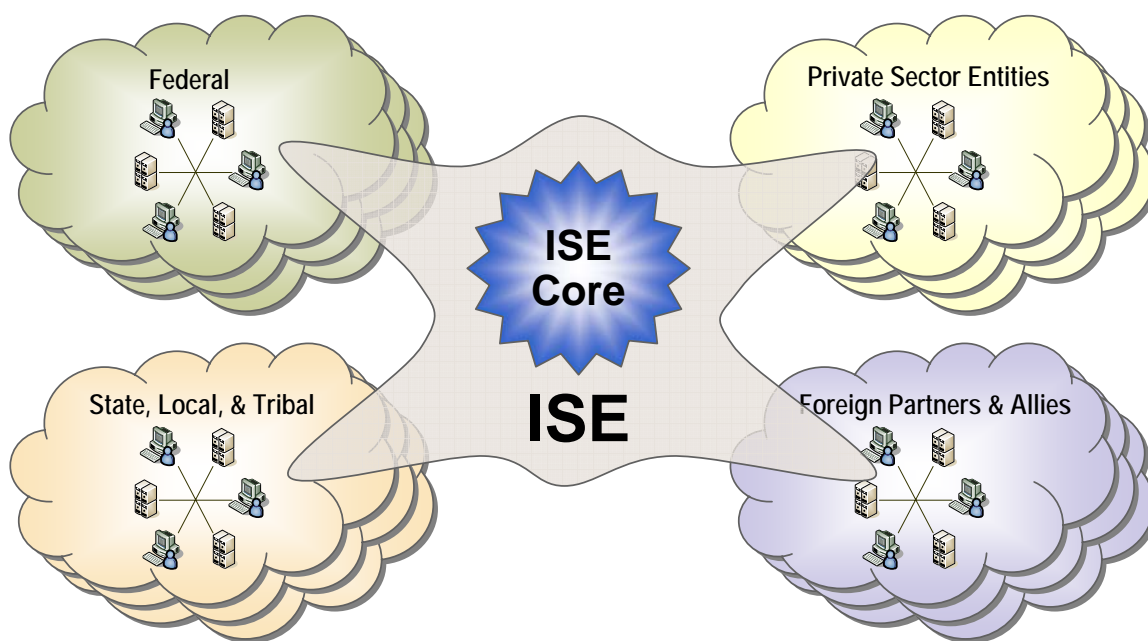
Table ES-1-1. Levels of Architectures

AUDIENCE	LEVEL	SCOPE	DETAIL	IMPACT
All Stakeholders 5 ISE Communities	FEAF ISE EAF FEA-ISE Profile	ISE	Low	Nationwide Strategic Outcomes
 All Stakeholders	Enterprise Architecture	Agency/ Organization	Low	Strategic Outcomes
 Business Owners	Segment Architecture	Line of Business	Medium	Business Outcomes
 Users and Developers	Solution Architecture	Function/ Process	High	Operational Outcomes

<sup>13</sup> Office of Management and Budget, *FEA Practice Guidance*, (OMB: Washington, DC, 2006), 1-4, 1-5.

## 2. Enterprise Architecture Framework Concepts

Figure ES-1 illustrates the general ISE 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 construct developed from the ISE EAF, will link ISE participants and create a distributed, protected, and trusted environment for sharing information. Consistent with IRTPA, the ISE will leverage the National Counterterrorism Center (NCTC) that will continue to serve as the central and shared knowledge bank on known and suspected terrorists and international terror groups. Consistent with the IRTPA, the NCTC will ensure that agencies have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analyses.



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

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 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; this activity is explained in more detail in Chapter 7.

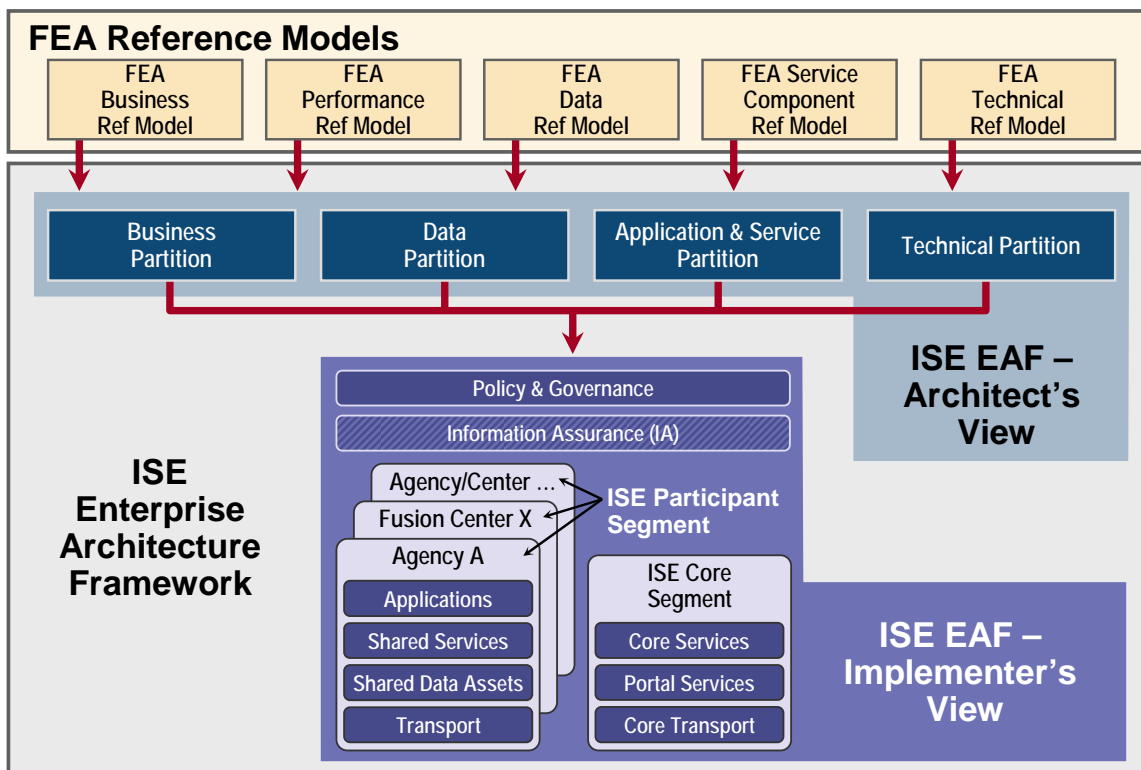
The ISE derives desired capabilities by leveraging, to the maximum extent practicable, existing systems, processes, and policies. The future ISE will enable the sharing of information across three security domains, including Sensitive but Unclassified (SBU), Secret/Collateral, and Top Secret (TS)/Sensitive Compartmented Information (SCI). Across these security domains, the ISE serves five communities: Defense, Foreign Affairs, Homeland Security, Intelligence, and Law Enforcement. Within these communities, there are many agencies, including those in the departments of Treasury, Interior, Health and Human Services, Commerce, Justice, Energy, State, Homeland Security, Defense, and Transportation. There are also agencies from the Intelligence Community, as well as SLT governments, and, eventually, 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.

### 3. The ISE Enterprise Architecture Framework

As Figure ES-2 depicts, the Federal Enterprise Architecture (FEA) Reference Models (RMs) provide the basis for the ISE EAF. All elements of the ISE EAF are mapped back to elements of the FEA RMs with the FEA management processes applied by the OMB leveraged in support of implementing the ISE. The four ISE EAF partitions are mapped to the five FEA RMs to enable tracking the development of the ISE EAF across agencies using standardized OMB policies and processes that structure EA development and budgeting processes. The ISE EAF also provides an overarching mapping of the ISE into not only Federal civil systems, but also national security systems.<sup>14</sup>

---

<sup>14</sup> 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 personnel management applications).”



**Figure ES-2. The ISE Enterprise Architecture Framework Is Defined by Two Views and Four Partitions**

Two primary views are used to describe the ISE EAF: 1) the Architect's View and 2) the Implementer's View. While the term "view" is typically used to refer to different aspects of an architecture, the OMB suggested the term "partition" rather than the more common terms "architecture" or "view" to differentiate the ISE approach as a framework from the approach typically used in departmental and agency EAs. The Architect's View comprises four partitions:

- 1) Business,
- 2) Data,
- 3) Application and Service, and
- 4) Technical.

The Architect's View is used to provide structural alignment of the ISE architectural components into the FEA structure to ensure strategies, business processes, investments, data, systems, and technologies within the ISE are integrated and compatible with those across the Federal government. The content of each of the four partitions is summarized in Table ES-1-2. The Implementer's View illustrates the more technically detailed elements of the architecture that may be implemented at the segment and solution architecture levels within agencies and other ISE participant organizations. This information is also important for developing the FEA-ISE Profile.

**Table ES-1-2. ISE Architecture Partitions**

EAF Partition	General Description
Business Partition	Identifies the 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 a universal core vocabulary and information exchange structure 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. Patterns are exemplar designs used to illustrate best practices when applying technologies and standards.

From the Implementer's View, the ISE consists of (a) the ISE Core Segment<sup>15</sup> and (b) multiple ISE Participant Segments. The ISE Core Segment provides common ISE Core Services, Portal Services, and Core Transport that are necessary to interface all ISE participants into the ISE. The Core Transport interlinks existing participant infrastructures together. The ISE Core Services, such as mediation, discovery, and security, are used by all participants to conduct cross-ISE information sharing. The ISE Portal Services provide additional capabilities through establishing a user interface. Overall, the Core Segment services necessary to interface and interconnect ISE participants are planned, implemented, and operated by service providers designated as Implementation Agents<sup>16</sup>.

The ISE Participant Segment consists of those assets owned and operated by ISE participating organizations that share terrorism information with other ISE participants. ISE Participant Segments contain shared applications, shared services, and shared data, as well as the hardware, software, and transport components necessary to support these shared assets. Interfacing with the ISE Core and ISE Participant Segments provide structure and focus to diverse ISE participant counterterrorism support systems that will contribute to an enhanced nationwide information sharing capability in the ISE.

<sup>15</sup> OMB defines the term "segment" as "individual elements of the enterprise describing core mission areas, and common or shared business services and enterprise services"; OMB, *FEA Practice Guidance*, (OMB: Washington, DC, 2006), A-2. In the case of the ISE, this may be established through an information sharing segment architecture, similar to that approach followed by the Department of Justice.

<sup>16</sup> Further information regarding the use of ISE Implementation Agents can be found in Chapter 12 of the *ISE Implementation Plan*.



Brief descriptions of each partition are provided in the sections that follow (detailed descriptions are provided in the main body of this document). The detailed descriptions are organized as a description of the current or “AS-IS” architecture, the envisioned or “TO-BE” architecture, and a transition strategy to move from the AS-IS to the TO-BE.

#### 4. Business Partition

While participants of the ISE are responsible for their individual counterterrorism missions, the ISE supports the improved effectiveness of their business processes by enabling access outside their organizations to additional terrorism information. Business processes addressing the administrative requirements of the ISE, and the ISE mission and service functions contribute to this mission enhancement. The ISE Business Processes are grouped into three categories:

- **Enabling Processes:** Enabling business processes are processes that form a management framework and a set of administrative business needs that support the ISE.
- **Mission Processes:** Mission business processes are those processes performed by various ISE organizations that directly support counterterrorism activities or feed other processes that do. In other words, these processes represent the actual use of information via the ISE to support counterterrorism missions.
- **Service Processes:** Service processes are those that functionally support the mission processes, but are common and recurring in nature (such as access and collaboration). These are leveraged directly for a number of mission processes.

The ISE EAF Business Partition Transition Strategy includes:

- Using a new FEA Business Reference Model (BRM) sub-function #262 for “Information Sharing”;
- Identifying mission processes that could benefit from ISE capabilities;
- Re-engineering those identified processes, as needed, to take advantage of new information sharing capabilities; and
- Establishing agency projects, as necessary, to implement ISE capabilities in support of the re-engineered processes.

The Guideline 2 framework, depicted in Figure ES-3, 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. The NCTC and State and major urban area fusion centers are critical components in the ISE. The NCTC has the primary responsibility within the Federal government for the analysis of terrorism information. The Federal government will promote the establishment of a network of fusion centers

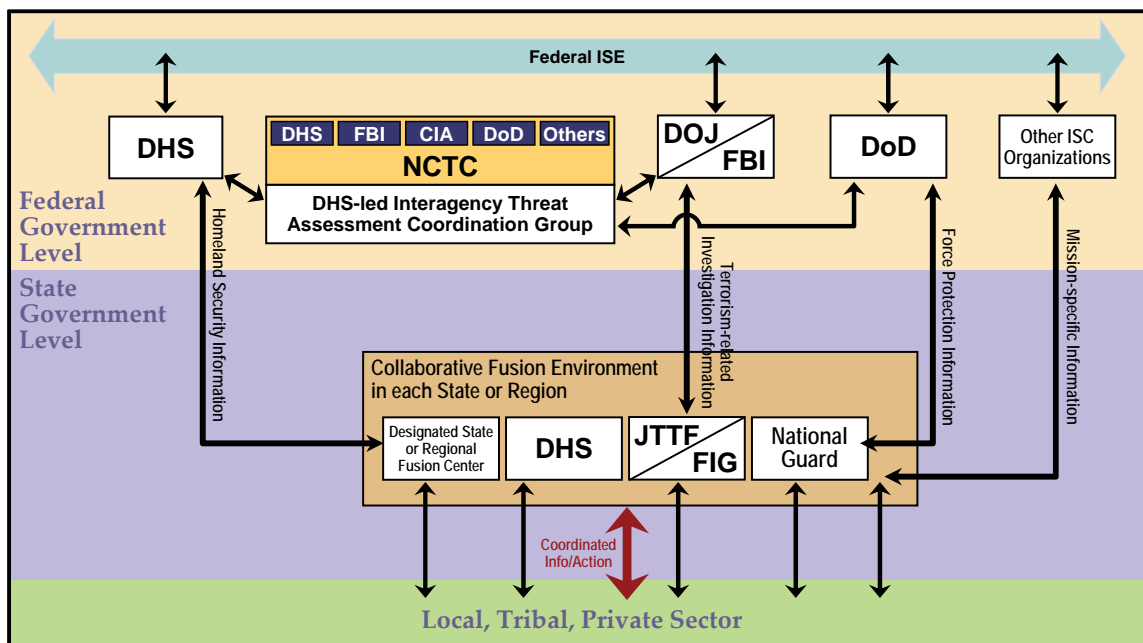


Figure ES-3. Approved Guideline 2 Framework<sup>17</sup>

to facilitate effective nationwide terrorism information sharing. 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. A Collaborative Fusion Environment refers to the fact that this will include a State or major urban area fusion center, an FBI JTTF/ FIG, a DHS office, and a National Guard office.

Business processes continue to be developed for the ISE focusing on priority services and mission processes. Once defined, these business processes will identify other information data flows, participant organizational roles, expected improvements and requirements for incorporation into subsequent versions of the ISE EAF.

## 5. Data Partition

Guideline 1 of the President's Memorandum directed that common standards be developed "to maximize the acquisition, access, retention, production, use management, and sharing of terrorism information within the ISE consistent with the protection of intelligence, law enforcement, protective, and military sources, methods and activities." The CTISS Working Group, chartered under the Information Sharing Council (ISC), is leveraging the National Information Exchange Model (NIEM) and the Department of Defense (DoD)/Intelligence Community (IC) Universal Core (U-Core) to establish the baseline ISE Data Partition particularly by defining the CTISS metadata and data standards categories.

<sup>17</sup> Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Ibid., 71.

NIEM was initiated by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) to provide the foundation and building blocks for national-level interoperable information sharing. NIEM is a framework to:

- Provide the means for stakeholders to identify their information exchange requirements for both emergency and normal operations;
- Develop standards, a common vocabulary, and a repository of information exchange package documentation (IEPD);
- Provide implementation support, training, and technical assistance; and
- Provide governance and processes to maintain NIEM.

The DoD/IC U-Core was developed jointly by the Department of Defense and the Intelligence Community to provide information sharing across their representative agencies and the enterprise. The U-Core consists of information on the nature, the location, and the timeframe of information exchanges that support the defense and intelligence communities. The U-Core design leverages information exchange successes coming from the Community of Interest construct and the Cursor on Target implementations. It is defined and implemented through an extensible exchange schema and leverages commercial (Geographic Markup Language, and Extensible Markup Language {XML}) and DoD/IC (Intelligence Community-Information Security Marking) standards. The U-Core is developed and controlled under the oversight of the Senior Enterprise Services Governance Group (SESGG), an advisory body to the Director, Information Policy (IP), Office of the DoD Chief Information Officer (CIO), and the Deputy Associate Director of National Intelligence for IC Enterprise Architecture, Office of the ADNI CIO.

CTISS will leverage data standards from NIEM and the DoD/IC U-Core to facilitate information exchanges between different domains or communities of interest by establishing a common framework for these exchanges. Exchange schemas are developed or customized by sub-setting, extending, and constraining reference schemas, and these developed exchange schemas are then fully documented through CTISS as functional standard issuances. Other agencies are then able to discover these functional standards and determine if the exchanges are applicable to their needs.

The ISE Data Partition will develop, harmonize, and manage the data components and vocabularies for inter-domain exchanges. The ISE will use CTISS functional standards to describe the structure, content, and other products of the information exchange. The TO-BE ISE scope will provide many more opportunities for inter-domain exchanges (e.g., Suspicious Activity Report (SAR), terrorist watchlist, cargo screening, people screening, emergency management, case management, and infrastructure protection) to be developed for the ISE.

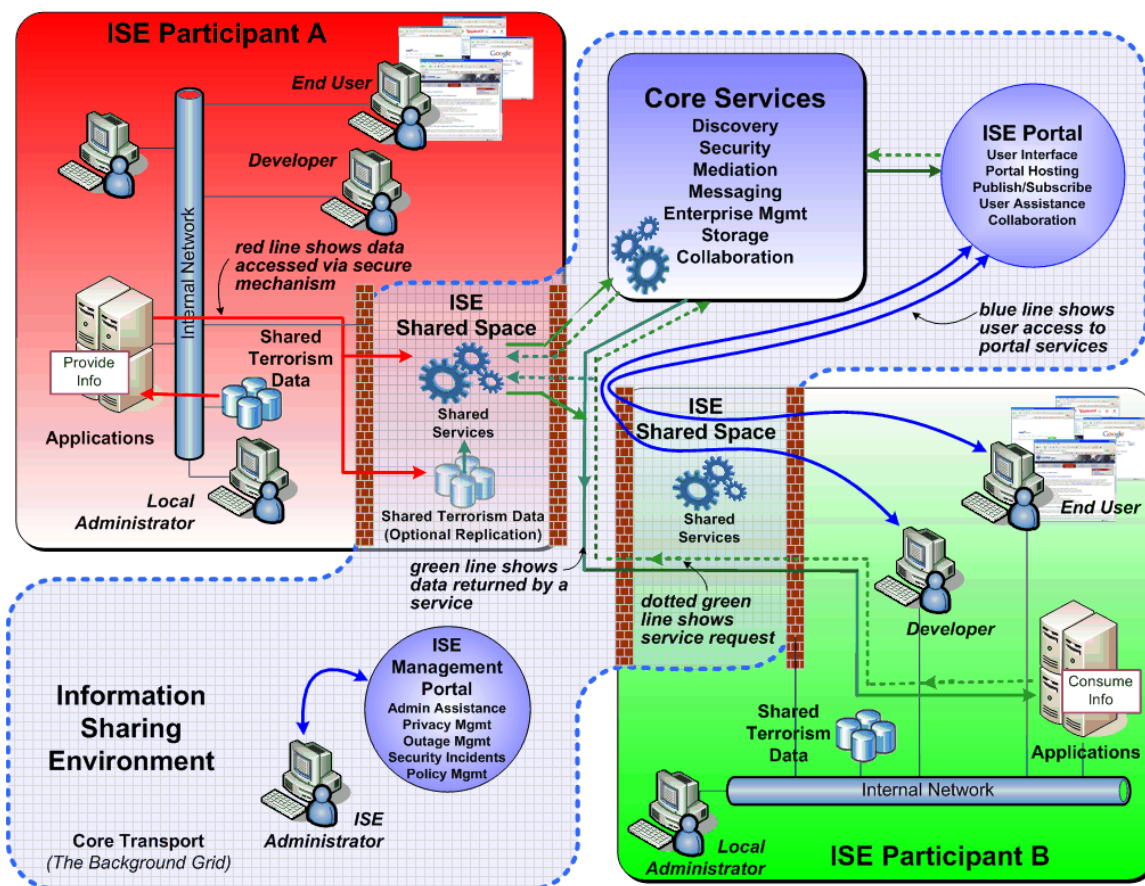
## 6. Application and Service Partition

The Application and Service Partition of the ISE EAF is intended to describe those components of the ISE architecture that provide a function or process that will facilitate information sharing. An objective of the ISE is to reuse existing ISE participant capabilities wherever applicable and bring these capabilities together in a unified and logical manner using a service-based architecture approach.

The baseline ISE Application and Service Partition is formed by the legacy information resource assets that ISE participants, such as Federal agencies, State, local, and tribal governments or private or foreign partners and allies have developed over the years. These assets include systems, applications, databases, and services. Historically these existing assets have usually been developed independently by organizations to solve specific, mission unique problems. The upshot is stovepipe systems that limit themselves from being integrated, and do not share information effectively across organizational boundaries or other communities.

Figure ES-4 shows the notional target architecture for the ISE. Three separate instances of the configuration shown in the figure exist to support the three security domains: SBU, Secret/Collateral, and TS/SCI. The target architecture for the Application and Service Partition in each security domain has two parts: (1) the ISE Core Segment and (2) the ISE Participant Segment. The ISE Participant Segment consists of those applications and services shared by each participant (denoted in the figure as “Shared Services,”) and the necessary transport and infrastructure necessary to host those applications and services, represented in the figure by the icons in each participant’s ISE Shared Space. The ISE Shared Space denotes infrastructure where the CTISS is implemented and where each ISE participant makes terrorism information accessible through their own Shared Space. This infrastructure remains outside a participant’s internal network, yet is still under the management and control of that ISE participant.

The ISE Core consists of three major components: ISE Core Transport, ISE Core Services, and ISE Portal Services. The portals are represented by the ISE Portal, which provides the primary human interface to the ISE, and the ISE Management Portal, which provides the management and administration interface. The ISE Core Services are those services required to provide a service-based architecture and are used by nearly all ISE participants. The ISE Core is essential for interconnecting all the various ISE Shared Spaces existing across the ISE as a functioning system-of-systems.



**Figure ES-4. Application and Service Partition of the ISE TO-BE Architecture.**  
This configuration exists at three security levels: SBU, Secret/Collateral, & TS/SCI.

The transition from baseline to target architecture consists of developing an initial operating capability (IOC). The required steps for IOC are as follows:

- 1) Select one or more business processes, e.g., SAR, which could benefit from improved cross-ISE information sharing. Develop revised processes as necessary. Establish pilot projects to evaluate the re-engineered processes, and follow ISE EAF guidelines to implement infrastructures that contribute to a nationwide SAR capability;
- 2) Establish the ISE transport initial operating capability (IOC) for the three security domains (SBU, Secret/Collateral, and TS/SCI) and the associated network management function and ISE Management Portal;
- 3) Establish the ISE Portal and Core Services capabilities; and
- 4) Manage the subsequent transition of additional business processes to share and consume information via the ISE.

Since individual participating organizations contribute to the ISE Participant Segment, the target architecture must be developed, in part, by each participant. The Office of the PM-ISE will work to coordinate the development of the ISE Participant Segment. The *FEA-ISE Profile*<sup>18</sup> provides guidance on the development of individual ISE participant Segments necessary for implementing those target architectures.

To participate in the ISE, each organization will also need to make its information resources available. This will require an ISE participant, in accordance with statutory authorities and civil liberties and privacy protections, to:

- 1) Determine terrorism information, homeland security information, and law enforcement information with a terrorism nexus available for sharing from its organization;
- 2) Expose this internal terrorism information to other ISE participants; and
- 3) Revise its own business processes, as needed, to take advantage of the capabilities and information provided by the ISE.

Transitioning from the current environment to the target ISE Core is a multi-year process that can be implemented incrementally, leading with limited-scope implementations and growing to more complex and difficult ones.

## 7. Technical Partition

The Technical Partition identifies the technologies and in particular those technical standards of the CTISS that will be used to implement the ISE. The ISE Technical Partition is based on the FEA Technical Reference Model (TRM), and provides a four-level taxonomy of (1) Service Areas, (2) Service Categories, (3) Service Standards, and (4) Illustrative Specifications or Technologies. The Technical Partition identifies technologies in the FEA TRM that are applicable to the ISE and includes additional technologies required by the ISE which are not currently in the TRM. Technologies are of three types: (1) a technical component (e.g., a Web browser), (2) a standard, or (3) a pattern. Patterns are exemplar designs used to illustrate best practices when applying technologies and standards.<sup>19</sup>

Many existing systems across ISE participants are based on client-server or n-tier architectures. In addition, many have also begun investigating service-based architectures. The ISE will leverage existing capabilities to the maximum degree possible; many existing baseline technologies will be included in the target architecture.

---

<sup>18</sup> Office of the PM-ISE, *FEA-ISE Profile*, (currently under development with scheduled release during 4<sup>th</sup> Quarter 2007).

<sup>19</sup> The ISE EAF uses enterprise integration (EI) patterns based on the Enterprise Integration Patterns Symbology as introduced in Hohpe, Gregor and Bobby Woolf, *Enterprise Integration Patterns* (Addison-Wesley, ISBN: 0321200683, 2004).

The target ISE architecture is represented by five key technology areas:

- 1) Service-based Architecture,
- 2) Enterprise Integration Patterns,
- 3) Information Assurance Technologies,
- 4) Transport Technologies, and
- 5) CTISS (includes Exchange Protocol and Services standards categories).

Many standards are included under the CTISS umbrella. These include standards such as those for services, information assurance, and transport. Most standards exist today and are in common use, and they have been previously developed by standards organizations.

## 8. Implementer's View

The Implementer's View consists of the components shown in Figure ES-5. ISE Enterprise Architecture Framework: Implementer's View. This view takes the results of the ISE Architect's View and organizes these into a model to guide participation in the ISE down to the segment and solution architecture levels.

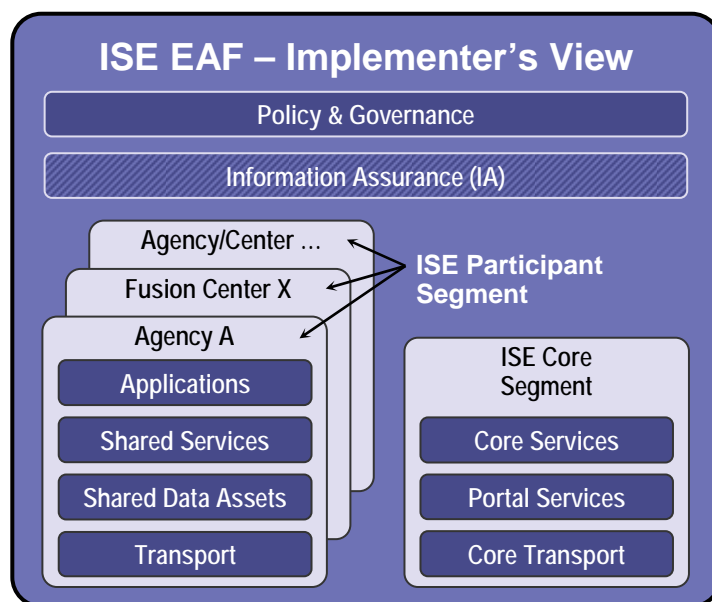


Figure ES-5. ISE Enterprise Architecture Framework: Implementer's View

**Policy and Governance** and **Information Assurance (IA)** span both the ISE Participant 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. Risk management is an inherent responsibility of governance and is critical to establishing and maintaining a known and acceptable level of risk for the ISE to enable assured information sharing.

A basic risk management approach should identify 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), and a determination if the residual risk is acceptable or if additional protective measures are required. The purpose of this process is ultimately a *risk decision* by the appropriate governance bodies and accrediting authorities for the ISE to ensure a known and acceptable level of risk (not risk avoidance) commensurate with mission requirements. This decision should be focused on the “responsibility to provide” information while also protecting sources and methods. There are many different risk management models in use within the Federal government and across all of the ISE communities. The proposed risk management model for the ISE will be based on the National Institute for Standards and Technology (NIST) Risk Management Framework (RMF), and, for National Security Systems, the RMF developed by Director of National Intelligence (DNI)/DoD C&A Transformation effort (which is based on the NIST framework).

A more detailed discussion of governance and risk management is outside the scope of this particular document, but the topic is mentioned here due to its crucial impact on the IA approach for the ISE.

**Information Assurance (IA)** manages accessibility of information in the three security domains, while safeguarding information. IA also protects sources and methods of collection from unauthorized use or disclosure. An IA Model for the ISE is presented in Figure ES-6. The IA model incorporates the three critical dimensions of IA Categories, ISE EAF Architect’s View Partitions, and IA Controls. Each of these dimensions can be

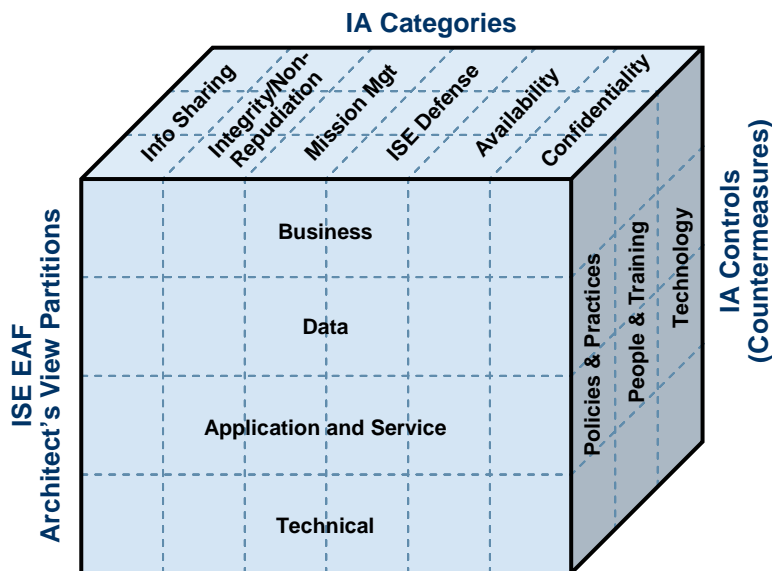


Figure ES-6. IA Model<sup>20</sup>

<sup>20</sup> This IA Model represents an initial approach to align information assurance concepts and capabilities with the ISE EAF partitions. This model may continue to evolve during the development of the FEA-ISE Profile and will be presented in greater detail, including its application, in the Profile and future versions of the ISE EAF.



divided into its principal elements, the intersection of which will identify IA Controls to apply to ISE partitions in order to support capabilities in the IA Categories.

From Figure ES-5, there are two main segments shown in this view: ISE Core Segment and ISE Participant Segment.

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 services required to provide a service-based architecture and are used by nearly all ISE participants.
- Portal Services support the ISE Portal and ISE Management Portal functions and provide additional services (e.g., publish/subscribe, collaboration, etc.) through a user interface.
- Core Transport includes the hardware, software, and transport media that support transmission and reception of information within and across the ISE.

As explained earlier, the ISE Core is inferred herein as an independent entity; however, in practice it will be implemented as an extension to existing capabilities of one or more Information Technology (IT) Implementation Agents to provide these capabilities to all the ISE participants.

The **ISE Participant** Segment shown on the left in Figure ES-5 (Agency A, Fusion Center X, Agency/Center...) represents the components managed by an ISE participant, such as agencies or fusion centers that use or provide information via the ISE.

- Within an organization, applications developed provide capabilities to address the counterterrorism mission. These applications may incorporate information and services provided by other participants throughout the ISE.
- Shared Services are those provided by a specific ISE participant. These services typically provide other participants with access to data or capabilities "owned" by that participant.
- Shared Data Assets are those information assets shared by ISE participants via the ISE.
- Transport includes the hardware, software, and transport media that support transmission and reception of message traffic from ISE participant systems to the ISE Core Transport Component.

These components, taken together, provide the building blocks for each organization to interconnect in the ISE.

## 9. Business Process Application Example

To demonstrate the application of the ISE EAF by an ISE participant throughout this document, an example will map the SAR business process across the four ISE EAF partitions. Developed by the PM-ISE and mission partners, this SAR business process flow is depicted graphically in Figure ES-7. 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. Figure ES-7 represents a sample information exchange (voice and data) for law enforcement and protective services that takes place in the end-to-end reporting and sharing of suspicious activities from the point of observation to the point information enters and traverses the ISE. This figure depicts the business process initially from a citizen seeing what is believed to be suspicious activity, to an officer responding to the scene, and then informing the dispatch precinct of events. Responsible organizations at the local level review the report and determine that the report should be disseminated to all appropriate agencies that may have an interest in the information. When the information is received at the fusion centers, some type of analysis that was conducted by the local agency would be conducted at the Fusion Centers. Fusion center interfaces to Federal agencies are also

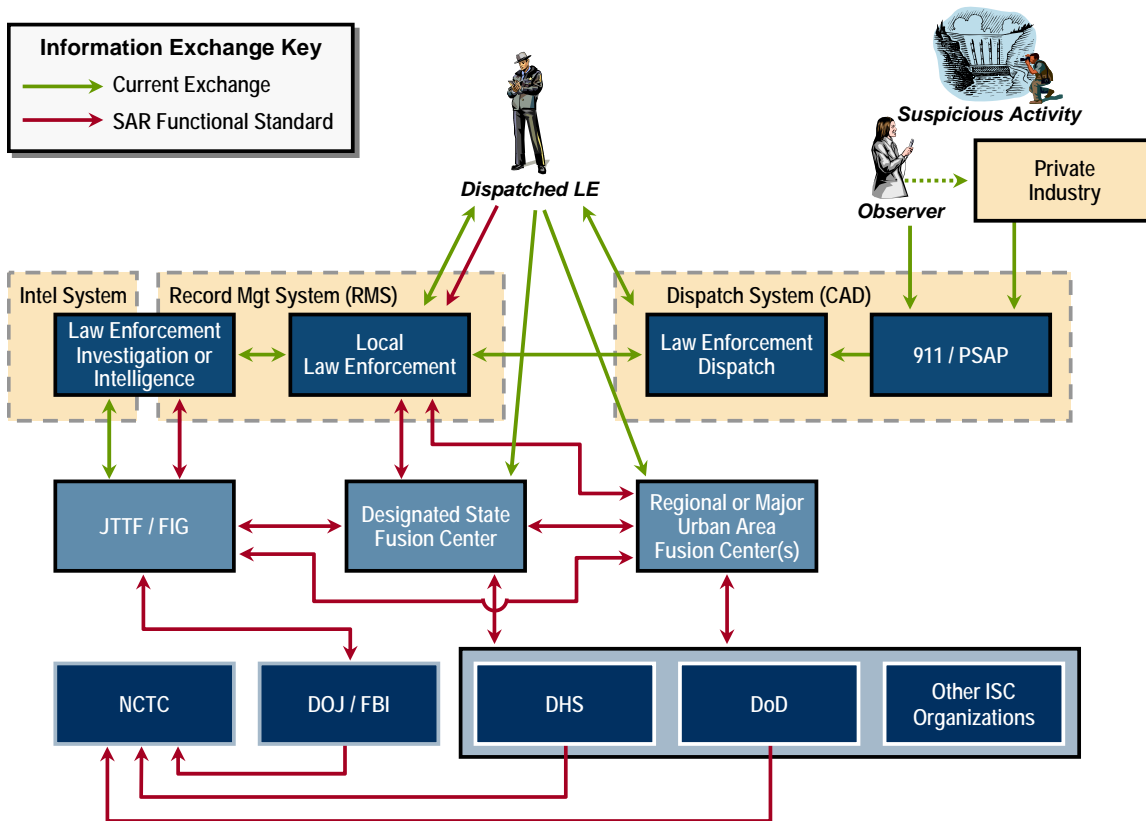


Figure ES-7. Suspicious Activity Report Process

depicted. Detailed information flow and description are further documented in the SAR functional standards issuance under CTISS; however the general implementation of SAR into ISE participant Shared Spaces will serve as a “use case” for the ISE EAF to provide greater clarity for implementation purposes. Subsequent versions of the ISE EAF will incorporate additional business processes and information exchanges as similar examples to provide implementation guidance.

This page intentionally blank.

## Chapter 1 – Introduction

### 1.1 Purpose and Scope

Section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004*<sup>21</sup> calls for the President to “create an Information Sharing Environment (ISE) for the sharing of terrorism information” among Federal, State, local, and tribal (SLT) governments, and, where appropriate, with private sector entities and foreign partners and allies, 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.”

This document provides a description of the ISE EAF<sup>22</sup>. 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; and
- To identify key architectural decisions which have been made or must be made.

The *Intelligence Reform and Terrorism Prevention Act* requires a description addressing the impacts of the ISE on enterprise architectures of participating agencies.<sup>23</sup> Similarly, the December 2005 Presidential Memorandum directs building the ISE upon existing Federal government resources that include standards, systems, and architectures.<sup>24</sup> This document contains a basic description of the ISE EAF, and it will be used as the basis for discussion with the ISE community.

The audience for this document includes the Chief Information Officers (CIOs) and enterprise architects of those Federal, State, local, and tribal governments, private sector entities, and foreign partners and allies that are participants in the ISE.

### 1.2 ISE EAF Description 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

---

<sup>21</sup> IRTPA, Section 1016.

<sup>22</sup> 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.

<sup>23</sup> IRTPA, Section 1016e(2).

<sup>24</sup> *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment*, *Ibid.*, Section 1.

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 will be made in accordance with PM-ISE configuration management procedures implemented by the ISE Enterprise Architecture Working Group.

### 1.3 Definitions

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

#### 1.3.1 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:

- 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.”<sup>25</sup>

---

<sup>25</sup> IRTPA, Section 1016(a)(4).

**Homeland security information** is defined in the Homeland Security Act as “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.”<sup>26</sup>

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:

- 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.”<sup>27</sup>

### 1.3.2 Information Sharing Environment

The *Intelligence Reform and Terrorism Prevention Act* calls for the creation of an “information sharing environment.”<sup>28</sup> It requires the President to: create an environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties; designate the organizational and management structures that will be used to operate and manage the ISE; and determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.<sup>29</sup> The *Intelligence Reform and Terrorism Prevention Act* requires that the ISE provide and facilitate “the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector” and, to the greatest extent practicable, “a decentralized, distributed, and coordinated environment” that:

---

<sup>26</sup> 6 U.S.C. Sec 482(f)(1).

<sup>27</sup> Extracted from the Recommendations for Presidential Guideline 2, found at Internet site [www.ise.gov](http://www.ise.gov).

<sup>28</sup> IRTPA, Section 1016(a).

<sup>29</sup> IRTPA, Section 1016(b)(1).

- 1) Connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, the private sector;
- 2) Ensures direct and continuous online electronic access to information;
- 3) Facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations, and operations;
- 4) Builds upon existing systems capabilities currently in use across the Government;
- 5) Employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;
- 6) Facilitates the sharing of information at and across all levels of security;
- 7) Provides directory services, or the functional equivalent, for locating people and information;
- 8) Incorporates protections for individuals' privacy and civil liberties; and
- 9) Incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.<sup>30</sup>

### 1.3.3 ISE Participants

Unless otherwise specified in this document, the term "ISE participants" means all Federal, State, local, and tribal (SLT) entities, private sector organizations and foreign partners and allies that participate in the ISE.

## 1.4 Background

### 1.4.1 Rationale

Currently, departmental and interagency communities facilitate terrorism information sharing within a specific discipline or a particular component of the counterterrorism community with the goal of making information and capabilities available to accomplish mission-specific requirements. In this regard, many of these entities have achieved some degree of success. The result, however, is the emergence of multiple, mission-specific information sharing systems with disparate policies, business rules, cultures, and technologies. This has unintentionally impeded the sharing of terrorism information among the various communities and across counterterrorism domains.

The ISE is an approach used to describe a collection of systems, organizations, processes, and information needed to collect, process, store, analyze, and share terrorism information. Pursuant to the November 2006 response to Presidential

---

<sup>30</sup> IRTPA, Section 1016(b)(2).



Guideline 2<sup>31</sup>, this encompasses Federal agencies and extends to SLT governments, the private sector, and the international community.

### **1.4.2 Vision**

The vision for the ISE is to create a powerful new national capability to share, search, and analyze terrorism information. It 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, information, and systems. It will interface to ongoing development 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 DoD/IC Universal Core being addressed by the Department of Defense and the Director of National Intelligence/CIO, the Continuity Communications EA and the National Command and Coordination Capability (NCCC) under development by the DHS, and the National Information Exchange Model (NIEM) development under the leadership of the Department of Justice and the Department of Homeland Security.

The envisioned ISE will enable the sharing of information within three security domains, including 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 fusion centers, and, where appropriate the private sector and foreign partners and allies.

---

<sup>31</sup> *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment, Ibid., Section 1.*

### 1.4.3 ISE Operational Concept

The ISE operational concept, outlined in Chapter 3 of the *Information Sharing Environment Implementation Plan*, provides important guidance on the scope of the ISE. It provides a vision for the top-level components of the architecture. Each participating ISE department, agency, or organization is an element, and these are connected by communication networks which transmit information between other ISE entities through the capabilities of the ISE Core infrastructure. The operational concept assigns important roles to the NCTC, and State and major urban area fusion centers. The NCTC has the primary responsibility within the Federal government for analysis of terrorism information. The ISE will provide interfaces that support establishing a network of fusion centers to facilitate effective nationwide terrorism information sharing. 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. A Collaborative Fusion Environment refers to the fact that this will include a State or major urban area fusion centers, an FBI Joint Terrorism Task Force (JTTF)/Field Intelligence Group (FIG), a DHS office, and a National Guard office.

### 1.4.4 Impacted Organizations

The ISE serves five communities:

- Defense,
- Foreign Affairs,
- Homeland Security,
- Intelligence, and
- Law Enforcement.

These communities span the Federal, SLT, private, and foreign partners and allies. Within each of these entities, there 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 participants. In the example of SAR, 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 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.

### 1.4.5 Key Expectations for the ISE EAF

The *Intelligence Reform and Terrorism Prevention Act* provides specific requirements, guidance, and envisioned capabilities for the ISE. The ISE is to be a “virtual space” in which participants can place, discover, retrieve, and use terrorism information. This virtual space requires an overarching architecture that establishes the guidelines and standards needed for interoperability among the ISE participants. The ISE EAF will be used to guide the implementation of the ISE capability. The ISE EAF has to account for existing (AS-IS) capabilities, while setting the direction and incremental steps toward the envisioned (TO-BE) capability.

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 agencies. Once implemented, the ISE will enable sharing terrorism information outside of the current information lanes and among Federal government agencies and their SLT, foreign, and private sector partners. Strategically, the TO-BE ISE EAF represents the conceptual view for a federation of networks across the ISE that becomes a “virtual network” of partnering systems, users, and services.

## 1.5 ISE EAF Product Set

The ISE EAF 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 Enterprise Architecture Framework Products**

Title	Description
<b>ISE EAF</b>	A high-level description of the components, structure, and unifying characteristics of the ISE to include the four partitions.
<b>FEA-ISE Profile</b>	A guide for ISE Federal departments and agencies which describes what each must do to connect to the ISE, expose data to the ISE, and access data and services provided by the ISE.
<b>ISE Requirements Specification</b>	A high-level specification of the ISE requirements. Requirements are allocated to components of the ISE EAF including the ISE Participant Shared Space, ISE Core Transport, ISE Core Services, and ISE Portal.

This page intentionally blank.

## Chapter 2 – Policy, Governance, and Requirements

### 2.1 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, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the ISE.”<sup>32</sup>

Given the complexity of managing ISE implementation, it is critical to establish a governance structure by which activities are executed, and that 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.

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** – Addresses and resolves important issues requiring specific expertise. Business process, architecture, and standards working groups 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.

---

<sup>32</sup> IRTPA, Section 1016(f)(2)(A).

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

## 2.2 Enterprise Architecture Principles

Principles are underlying and fundamental elements of sound enterprise architectures. They guide the development of an architecture by providing criteria for selecting among alternative architectural choices. They are developed from industry best practices and standards. Highlights are provided below.

### 2.2.1 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<sup>33</sup> In general, architecture principles are intended to influence the development, maintenance, and use of an enterprise architecture. ISE EAF overarching principles include:

- 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; and
- The Federal architecture simplifies government operations.

### 2.2.2 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:

- 1) The Federal Enterprise Architecture (FEA) is an ISE point of linkage;<sup>34</sup>
- 2) Terrorism information sources and methods must be protected;<sup>35</sup>
- 3) Information security policies and practices are applied to systems;<sup>36</sup>
- 4) The NCTC serves as an aggregation and coordination point for the ISE;<sup>37</sup>
- 5) Fusion Centers are SLT information dissemination points;<sup>38</sup>

---

<sup>33</sup> CIO Council, *Architecture Principles for the U.S. Government*, (CIO Council: Washington, DC, 2007) found at Internet site [www.cio.gov](http://www.cio.gov).

<sup>34</sup> Derived from OMB, *Circular A-11* (OMB: Washington, DC, 2007) and *Federal Enterprise Architecture Program EA Assessment Framework*, 2.1 (OMB: Washington, DC, 2005).

<sup>35</sup> 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>.

<sup>36</sup> Derived from the *E-Government Act of 2002*, Public Law No. 107-347 (January 23, 2002).

<sup>37</sup> Derived from IRTPA, Section 1021.

- 6) Increased situational awareness posture is a driver for the ISE;<sup>39</sup>
- 7) The ISE will define participant roles and responsibilities;<sup>40</sup>
- 8) Federal laws and mandates will be followed within the ISE EAF; and
- 9) The ISE will identify laws and mandates that impede information sharing and recommend changes.

### **2.2.3 ISE EAF Technical Principles**

Though the ISE will be a virtual environment, its physical infrastructure and access will include information technology 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 the Department of State. The following list describes the ISE EAF Technical Principles to be applied:

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

### **2.2.4 ISE EAF Configuration Management**

The ISE EAF will evolve over time as additional business processes, information flows and exchanges, services, and technologies are defined and incorporated into the ISE. The ISE EAF Working Group (ISE EAF WG) is responsible for the ISE EAF configuration management process and managing this incremental change.

---

<sup>38</sup> Derived from Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Section 3.4.

<sup>39</sup> Derived from Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Section 3.2.

<sup>40</sup> Derived from IRTPA, Section 1016.

## 2.3 ISE Requirements

Requirements define capabilities that the ISE must provide. They may specify functionality, efficiency and policy, compatibility, performance, or design constraints. Functional requirements define what the ISE must do. Non-functional requirements would include process and policy necessities on a system or program's operation. Compatibility requirements define features the ISE must have in order to operate with interfacing systems. Performance requirements define how well something must be performed. Design and policy constraints limit the architectural alternatives available. Often time technology and design cannot be implemented because of limiting policy directions. Additionally, further requirements will stem from mission users and their information needs as identified by analysis of the EAF Business Partition.

Explicit top-level requirements are specified in a set of authoritative source documents.

The *Intelligence Reform and Terrorism Prevention Act* of 2004 is the primary source document. Section 1016, provides the authority for the creation of an Information Sharing Environment (ISE), defines the requirements for this ISE, and grants authority to implement policies.<sup>41</sup>

Executive Order 13388 of October 2005<sup>42</sup> provides additional guidance on the ISE, including the creation of an Information Sharing Council (ISC) with defined members to provide advice and assist in the ISE implementation.

The Office of Management and Budget (OMB) Circular A-11 of 2006<sup>43</sup> and the *Enterprise Architecture Assessment Framework*<sup>44</sup> establish and define criteria, policies, and requirements for new Federal government information technology architectures and systems assessment and linkage. Circular A-130<sup>45</sup> establishes policy for the management of Federal information resources, including the use of enterprise architectures in the capital planning and investment control process.

The *Electronic Government (EGOV) Act of 2002*<sup>46</sup> establishes the framework for using Internet-based technology to share information. The ISE will implement services to provide ISE capabilities.

---

<sup>41</sup> IRTPA, Ibid.

<sup>42</sup> Executive Order 13388, Ibid.

<sup>43</sup> Office of Management and Budget, *Circular A-11*, Ibid.

<sup>44</sup> Office of Management and Budget, *Federal Enterprise Architecture Program EA Assessment Framework 2.1*, (OMB: Washington, DC, 2005), found at Internet site <http://www.whitehouse.gov/omb/egov/a-2-EAAssessment.html>.

<sup>45</sup> Office of Management and Budget, *Circular A-130*, (OMB: Washington, DC, 2000), found at Internet site <http://www.whitehouse.gov/omb/circulars/index.html>.

<sup>46</sup> *E-Government Act of 2002*, Public Law No. 107-347 (January 23, 2002).



*Guidelines and Requirements in Support of Information Sharing (December, 2005)*<sup>47</sup> sets five guidelines for information sharing between agencies.

- Guideline 1 addresses common standards for how information is acquired, accessed, shared, and used within the ISE;
- Guideline 2 addresses State, local, tribal, and private sector participation in the ISE;
- Guideline 3 addresses SBU information;
- Guideline 4 addresses information sharing with foreign partners; and
- Guideline 5 addresses ISE privacy rights and other legal protections.

Responses to Guidelines 2, 4, and 5 have been prepared by the PM-ISE and are published on the PM-ISE Web site ([www.ise.gov](http://www.ise.gov)). Response to Guideline 3 is under development. These response guidelines provide additional sources of ISE requirements.

The *Information Sharing Environment Implementation Plan* defines the scope of the ISE, required resources, planned work activities, and the roadmap or order of implementation for capabilities of the ISE.

The Common Terrorism Information Sharing Standards (CTISS) Working Group, established by the PM-ISE, created a document defining the categories and initial set of common standards for use by the ISE.<sup>48</sup>

The Intelligence Community (IC) EA documents define the environment, requirements, and components of the service-based architecture (SBA) prescribed for development and use by the IC. The ISE will leverage the IC effort whenever possible.<sup>49</sup> Additional sources include:

- Office of Management and Budget Circular A-130;
- Privacy Act of 1974 (5 U.S.C. section 552a);
- National Intelligence Strategy, Enterprise Objective 5 and 7;
- Intelligence Community Directive, Number 1, Section F.2.d.3; and
- Executive Order 12333.

Similarly, the DoD has invested heavily in the Global Information Grid (GIG) architecture and is implementing GIG capabilities. Additionally, other Federal agencies have made

---

<sup>47</sup> *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment* (December 16, 2005), Section 2.

<sup>48</sup> Office of the PM-ISE, *Common Terrorism Information Sharing Standards (CTISS), Version 2.0* (June 2007).

<sup>49</sup> Intelligence Community Enterprise Architecture (*Data Architecture Division*, <https://www.icmwg.org/>).

similar investments. The ISE will leverage these when possible. GIG concepts are described in a series of Net-Centric Implementation Documents (NCIDs).<sup>50</sup>

In most architecture development efforts, a few key requirements have a very significant impact on the ultimate outcome. These are sometimes referred to as design drivers. The ISE key requirements identified below are extracted and summarized from a more complete list of requirements provided in Appendix E.

- The ISE will build on existing systems and resources. It is not feasible or affordable to build an entirely new capability.
- The ISE will use a service-based architecture approach because this provides a flexible, adaptable structure which can build on existing systems and evolve.
- The ISE will enable the sharing of information, as well as appropriate data protection, at each specified level of security within and among agencies and security classification levels.
- The ISE must protect privacy and civil liberties associated with shared information.
- Collocated fusion facilities will be used at the State level to create a coordinated channel for SLT entities to publish information to the ISE and discover information in the ISE.

A complete set of requirements is under development and will be published in an *ISE Requirements Specification* that will replace the current Appendix E.

## 2.4 Mapping the Presidential Guidelines to the EAF

The *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment* and the associated Guideline Reports are key sources of requirements for the ISE. Guideline 2 is especially important since it defines a common framework for sharing information between and among executive departments and agencies, and State, local, and tribal governments, law enforcement agencies, and the private sector. Appendix I provides a detailed mapping of EAF attributes to the Presidential Guidelines.

---

<sup>50</sup> Defense Information Systems Agency, GIG Net-Centric Implementation Documents Overview (NCID000, 11 August 2005).

## Chapter 3 – ISE EAF Overview

### 3.1 General Description

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.”<sup>51</sup> 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 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.”<sup>52</sup> With respect to the ISE EAF, enterprise refers to a collection of organizations joined together to achieve a future state of effective sharing of terrorism information.

The Federal government has adopted a federated architecture approach. The FEA describes the top level of the federation. It provides broad guidance applicable across the Federal government. Each department has a departmental EA as required by Clinger-Cohen.<sup>53</sup> These department-specific architectures must map back to the FEA to demonstrate alignment and allow for investment management across the entire Federal government enterprise. Within each department, agencies may develop subsidiary architectures, which link back to the departmental EA and provide additional mission-specific details. Similarly, many SLT governments have or are developing enterprise architectures. Input from these partners will be reflected in future ISE EAF versions as appropriate.

In general, enterprise architectures 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).

Figure 3-1, illustrates a high-level, conceptual view of the ISE. The purpose of the ISE is to provide a common environment for Federal, State, local, and tribal governments, and foreign partners and allies, and private sector entities to share information. The ISE includes an ISE Core which provides services used by all participants. It includes a connection capability and shared virtual space, indicated by the transparent cloud in the figure. Each participant uses services to expose selected counterterrorism-related data assets to the designated shared space.

---

<sup>51</sup> 29 U.S.C. 203(r)(1).

<sup>52</sup> U.S. Government Accountability Office, *Report GAO-06-219* (U.S. Government Printing Office: Washington, DC, 2005), 7.

<sup>53</sup> *The Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)*, Public Law No. 104-106, (February 10, 1996).

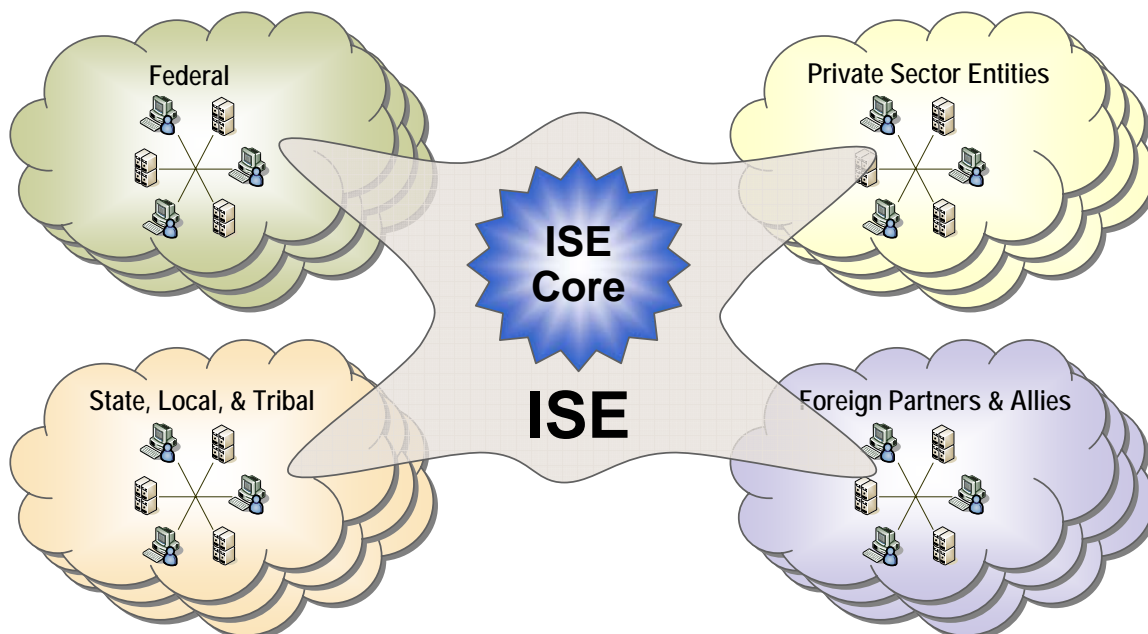


Figure 3-1. The ISE Is a Virtual Environment for Terrorism Information Sharing

### 3.2 ISE Enterprise Architecture Framework (ISE EAF)

An architecture framework is a logical approach to organizing voluminous and highly complex information in a meaningful way. Enterprises are quite complex and so are the processes, policies, and technologies that support them. By organizing the complexity into a set of predefined architectural products, the complexity is reduced allowing one to understand what functions the enterprise is required to perform and how those functions can best be supported by technology. Further, by using a framework, one can ensure consistency within the architecture because everyone is working from a commonly accepted set of constructs and a logical flow process. In the case where the ultimate solution will span multiple organizations and technology platforms, the use of such a framework will be vital to ensuring success.

OMB has suggested the term “enterprise architecture framework” for the ISE enterprise architecture to highlight the fact that the ISE is a cross-agency construct. The ISE EAF is illustrated in Figure 3-2. It is based on the Federal Enterprise Architecture Framework (FEAF)<sup>54</sup>, modified to reflect the needs of the ISE. It also reflects the guidance provided in the OMB EA Assessment Framework.<sup>55</sup>

<sup>54</sup> CIO Council, *A Practical Guide to Federal Enterprise Architecture, Version 1.0* (CIO Council: Washington, DC, 2001).

<sup>55</sup> Office of Management and Budget, *Enterprise Architecture Assessment Framework 2.1* (OMB: Washington, DC, 2006).

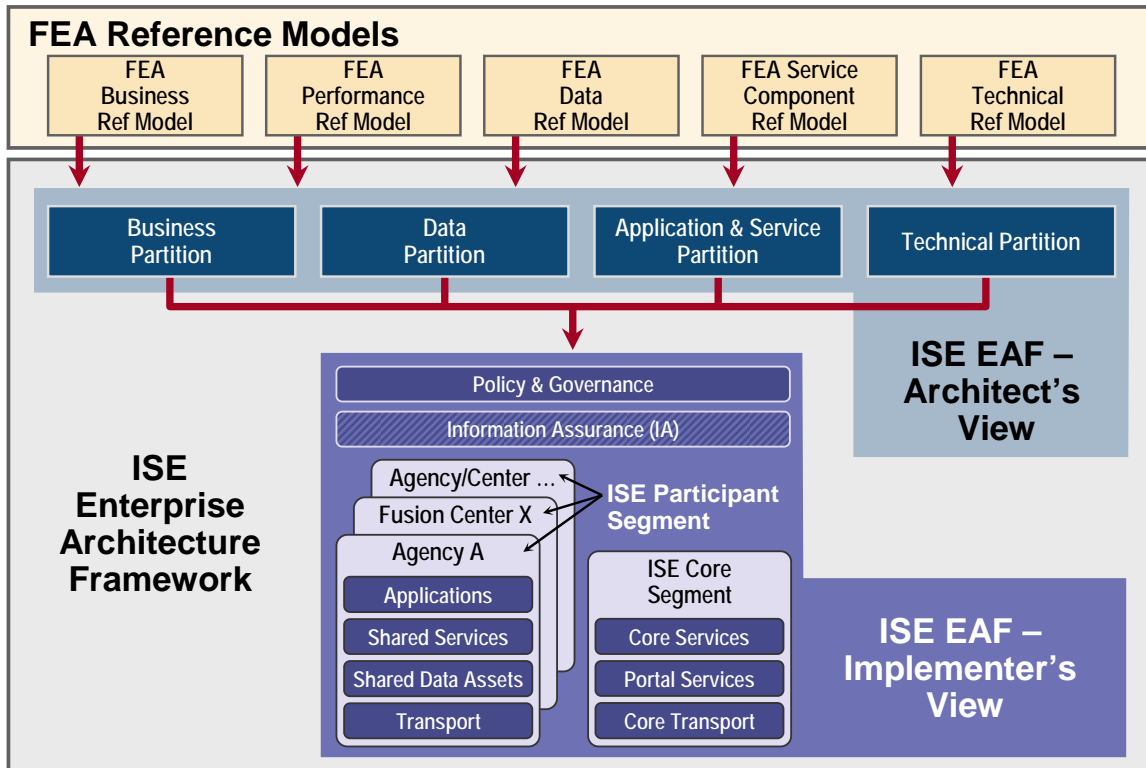


Figure 3-2. ISE EAF Framework

An architecture is typically presented via multiple views or, in the ISE case, partitions. The ISE is described in terms of four partitions:

- 1) the Business Partition,
- 2) the Data Partition,
- 3) the Application and Service Partition, and
- 4) the Technical Partition.

For the ISE, the **Business Partition** presents the business activities and processes supporting the ISE. The **Data Partition** defines data (structured and unstructured) and data models for the terrorism information that will be shared in the ISE. The **Application and Service Partition** describes the applications, services, data assets<sup>56</sup>, transport, and infrastructure that support the ISE business processes. The **Technical Partition** describes the technology and standards that will be used to develop and implement the ISE.

The **Implementer's View** shows the major components that must be developed or integrated to implement the ISE at the segment and solution architecture levels. It is a useful view for planning and managing the development of ISE capabilities.

<sup>56</sup> Data asset refers to a container in which data is stored, for example a data warehouse or database is a data asset. These assets are part of the Applications and Services partition.

### 3.3 Architecture Partitions

The selected EAF includes four “partitions”<sup>57</sup> as indicated in Table 3-1.

**Table 3-1. ISE Architecture Partitions**

EAF Partition	General Description
<b>Business Partition</b>	Identifies the business functions, processes, and information flows that facilitate information sharing in the ISE.
<b>Data Partition</b>	Identifies and describes the data required to enable the ISE business processes through the functional standards of the CTISS. Defines a universal core vocabulary and information exchange structures for sharing information across the various ISE business processes.
<b>Application and Service Partition</b>	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.
<b>Technical Partition</b>	The technologies, technical standards of the CTISS, and patterns used to implement the applications and services. Patterns, described in detail in Chapter 7, are exemplar designs used to illustrate best practices when applying technologies and standards.

The architectural products to be included in the description of each EAF partition are summarized in later sections.

### 3.4 ISE Implementer’s View and Segments

The **Implementer’s View** shows the major components that must be developed or integrated to implement the ISE. It is a useful view for planning and managing the development of ISE capabilities. It is defined in terms of segments and components of segments.

The OMB has issued guidance on using architectural segments to define an enterprise architecture<sup>58</sup>. Enterprise, segment, and solution architectures provide different 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. Figure 3-3 shows the relationship of the ISE EAF, enterprise architectures, segment architectures, and solution architectures. As an example, the Department of Justice (DOJ) has defined an Information Sharing Segment as part of the DOJ EA. This Information Sharing Segment includes multiple solution architectures for individual systems such as the FBI’s National Data Exchange System (N-DEx) and the Regional Data Exchange System (R-DEx).

<sup>57</sup> The OMB suggested the term “partition” rather than the more common terms “architecture” or “view” to differentiate the ISE approach from the approach typically used in departmental and agency EAs.

<sup>58</sup> Office and Management and Budget, *FEA Practice Guidance* (OMB: Washington, DC, 2006).




AUDIENCE	LEVEL	SCOPE	DETAIL	IMPACT
All Stakeholders 5 ISE Communities	FEAF ISE EAF FEA-ISE Profile	ISE	Low	Nationwide Strategic Outcomes
 All Stakeholders	Enterprise Architecture	Agency/ Organization	Low	Strategic Outcomes
 Business Owners	Segment Architecture	Line of Business	Medium	Business Outcomes
 Users and Developers	Solution Architecture	Function/ Process	High	Operational Outcomes

Figure 3-3. OMB Guidance on the Use of Segment Architectures

The components that will ultimately make up the ISE can be seen as belonging to one of two segments (see Figure 3-2):

- 1) the ISE Core Segment; or
- 2) The ISE Participant Segment<sup>59</sup>.

### The ISE Core Segment

The ISE Core Segment can be viewed as the basic infrastructure that will facilitate and/or support the ISE environment at large. The ISE Core Segment will contain the core transport component that will be used to interconnect the separate networks of each ISE participant and allow exchange of information. It must also contain the necessary infrastructure components to implement a service-based architecture, as described further in Chapter 6. These infrastructure components include Core Services such as directory and search capability, policies, and other resources which must be shared.

<sup>59</sup> OMB defines the term “segment” as “individual elements of the enterprise describing core mission areas, and common or shared business services and enterprise services”; FEA Practice Guidance, Ibid.

## The ISE Participant Segments

Each organization participating in the ISE will also operate components that will become a part of the ISE. These components are simultaneously part of the ISE EAF and part of the agency's enterprise architecture. Each organization should consider defining an information sharing segment within its enterprise architecture. This segment 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.

### 3.5 The Federal Transition Framework Catalog

OMB's *Federal Transition Framework (FTF) Catalog* is a compliance tool used by OMB to oversee and align Capital Planning and Investment Control (CPIC) processes for cross-agency initiatives across the Federal government.<sup>60</sup> The development of agency target architectures will be facilitated by the FTF that can be used by agencies to ensure that the Federal transition strategy is reflected in their own EA transition strategies and budget submissions. Consistent with ISE goals, this action will assist agencies with aligning information technology programs with appropriate inter-agency initiatives.

The FTF Catalog is published at least annually by OMB. The Catalog provides written description and information references for inter-agency initiatives included in the FTF. The ISE FTF catalog entry addresses all FEA reference models and will be included in the FEA Program EA Assessment Framework 2.1.<sup>61</sup>

### 3.6 Common Terrorism Information Sharing Standards

The ISC Chair has designated the CTISS Working Group as the primary body for defining ISE common standards. The CTISS effort is defining standards categories, standards defining bodies, core standards, and business process-driven functional standards. These standards are necessary to establish an integrated, nationwide enterprise of information sharing organizations and resources.

To do this, common standards are identified as both *functional standards* and *technical standards*. Functional standards document data and detailed functional activity descriptions on a focused area that uses ISE business processes to share mission products. Functional standards are based on ISE information exchanges supporting specific sets of business requirements in an operational setting, and capture the information exchanged between ISE participants. CTISS information exchanges are generally composed of schemas (for data exchange) and documentation (for understanding the business context and usage). Technical standards document a

---

<sup>60</sup> Office of Management and Budget, *Federal Transition Framework Catalog of Cross Agency Initiatives, Version 1.0* (OMB: Washington, DC, 2006) found at Internet site <http://www.whitehouse.gov/omb/egov/a-2-EAFTF.html>.

<sup>61</sup> Office of Management and Budget, *Federal Enterprise Architecture Program EA Assessment Framework 2.1*, Ibid.



specific technical methodology to implement information sharing capability in ISE systems.

The PM-ISE chartered the ISE CTISS Working Group to:

- 1) Identify categories of the CTISS based on relevant authorities;
- 2) Develop the baseline CTISS;
- 3) Identify ongoing standards efforts related to information sharing;
- 4) Initiate interconnections and alignment to these ongoing efforts; and
- 5) Identify and suggest appropriate next steps to implement the baseline CTISS.

The CTISS Version 2.0 document addresses items 1 and 2 above. The CTISS Working Group identified general categories, a set of standards bodies, and a baseline set of core standards. A more complete description of the CTISS is provided in the discussion of the Data Partition (Sections 5.2, 5.4.1) and the Technical Partition (Section 7.3).

This page intentionally blank.

## Chapter 4 – Business Partition

### 4.1 Introduction

The Business Partition describes how the ISE will meet its counterterrorism mission objectives from a business point of view. This partition leverages an analysis of the existing environment as well as the requirements and constraints affecting the envisioned environment.

Systems are typically made up of collections of people, information, processes, and technologies. These elements, when integrated, deliver capabilities against critical success factors or key performance indicators of the enterprise.<sup>62</sup> The Business Partition identifies the business functions, processes, and organizations necessary to support the ISE mission, vision, and strategic goals, and guide technology and policy development. Defining explicit and usable business processes is a critical component that affords the ISE and other communities the ability to better share terrorism information and other mission services resources.

The artifacts used to describe the Business Partition are summarized in Table 4-1 and will continue to evolve and be evaluated against requirements discovered by the ISE Business Process Working Group (BPWG). Not all artifacts are used in both the baseline (B) and target (T) partitions.

**Table 4-1. Business Partition Products**  
*Note: B/T refers to whether the product is used in the baseline or target view.*

Business Partition		
Product Name	B/T	General Description
<b>ISE BRM</b>	B/T	A version of the FEA Business Reference Model (BRM) highlighted to represent the FEA BRM domains, lines of business, sub-functions, and processes within each sub-function within the ISE scope.
<b>ISE Business Processes</b>	B/T	A list of the ISE business processes, including a name, short description, and category.
<b>Business Process/Org Matrix</b>	B/T	A matrix view of organizations that participate in each business process.
<b>Business Process/Strategic Goals</b>	B/T	An alignment between Business Process (BP) flow and the Strategic Goals Map.
<b>Business Process Model (BPM)</b>	T	A diagram tracing the sequence or events by each actor in a BP, showing more detail than the Use Case. Portrayed using the Business Process Modeling Notation (BPMN) or equivalent.

<sup>62</sup> Paraphrased from Interoperability Clearinghouse, *Glossary of Terms*, found at Internet site <http://www.ichnet.org>.

Documenting and analyzing information exchanges to support ISE participant business processes is critical in identifying potential information gaps. Specifically, this analysis will support the:

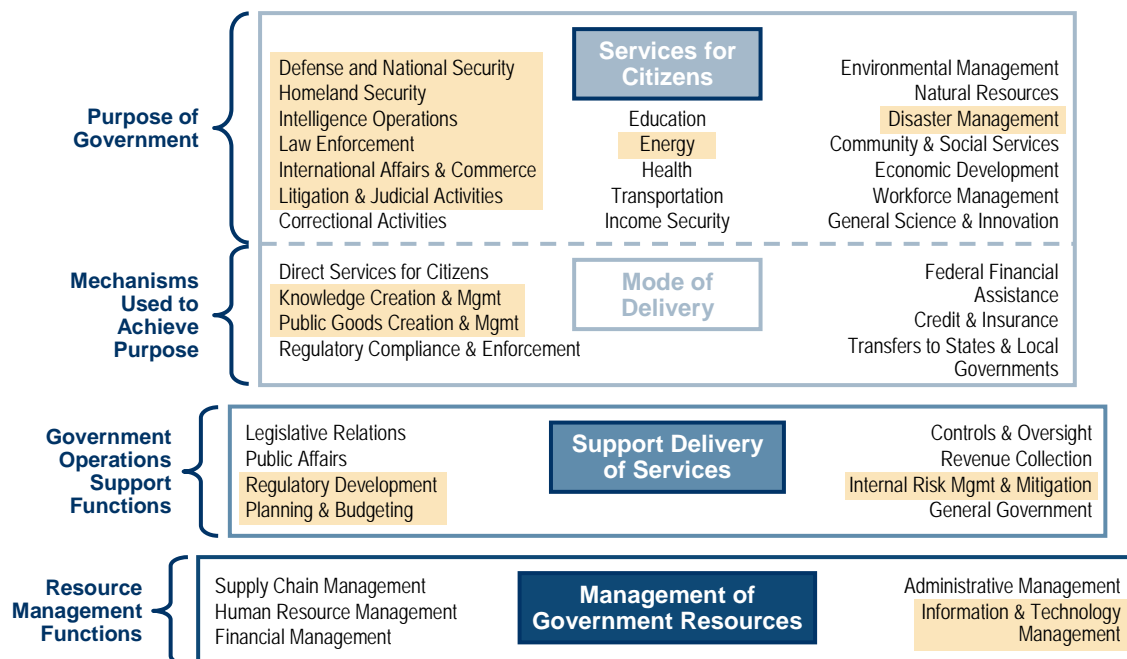
- **Removal of Information Silos.** The removal of information silos promotes greater cross-ISE sharing of resources and other data.
- **Acceptance of notional standards for inter-ISE data.** Normalizing standards and schema allows agencies, organizations, and Communities of Interest to adapt.
- **Exposure of attributes and other services through web services.** Exposing attributes through services that prove beneficial for the efficiency of passing credentials between entity resources.
- **Collection of process metrics.** Process metrics may serve as a baseline against which to measure performance improvements derived as a result of the ISE. In addition, metrics will serve as the foundation of a performance reference model (PRM) to reflect the projected performance metric for this segment architecture.

## 4.2 Baseline Business Partition

There are various information sharing initiatives underway by ISE participant organizations with counterterrorism missions. CIA and the Defense Intelligence Agency (DIA) have proof-of-concept designs that bridge the technology and business partitions. The ISE promotes information sharing across *all* communities with a counterterrorism role. The Baseline Business Partition consists of all counterterrorism processes in which counterterrorism information is shared across organizational boundaries. The Target Business Partition is defined by analyzing business processes which benefit from additional, improved cross-organization information sharing.

### 4.2.1 ISE Baseline Business Reference Model

The ISE BRM is a hierarchical list of the business domains, lines of business, sub-functions, and processes within the scope of the ISE that are taken from the Federal Enterprise Architecture reference model. In June 2007, OMB approved the addition of an "Information Sharing" Sub-Function under the Technology Management line of business in the BRM to help identify ISE investments, and to establish performance metrics for ISE deployment. Going forward, the top three levels of the ISE BRM correspond to the FEA BRM, with only the elements applicable to ISE selected. The top two levels are shown in Figure 4-1. Items highlighted in yellow indicate a relationship between a BRM sub function and an existing ISE FTF catalog entry. The descriptions of these items are provided in the FEA BRM and not repeated here.



**Figure 4-1. The ISE BRM – Top Two Levels**

The lowest level of the ISE BRM identifies ISE specified business processes. The baseline ISE BRM will only provide the name of each ISE business process and a brief description of the process’s purpose. More complete models of the business processes will be developed in the Target ISE BRM. For example, in the case of implementing suspicious activity reporting (SAR) capability into an ISE Participant’s EA, the organization would identify in their EAs an appropriate mapping to the BRM that includes the subfunctions of “Intelligence Analysis and Production” and “Intelligence Collection” under the “Intelligence Operations” line of business, and the subfunction “Criminal Investigation and Surveillance” under the “Law Enforcement” line of business, and the subfunction “Information Sharing” under the “Information and Technology Management” line of business.

### 4.3 Target Business Partition

The information flows in the Business Partition will remain stable during the transition from the existing to the envisioned partition. This expectation is supported by the relatively few changes to the FEA BRM in the last annual update.

#### 4.3.1 ISE Target BRM

OMB added Information Sharing as a new BRM sub-function under the Information and Technology Management Line of Business within the “Management of Government Resources” business area. Information is a resource and the sharing of information is a government management activity, thus it justifiably maps under the Information and Technology Management Line of Business in the FEA BRM. Figure 4-2 portrays the

Target ISE BRM input. This definition is: “Information Sharing relates 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.”<sup>63</sup>

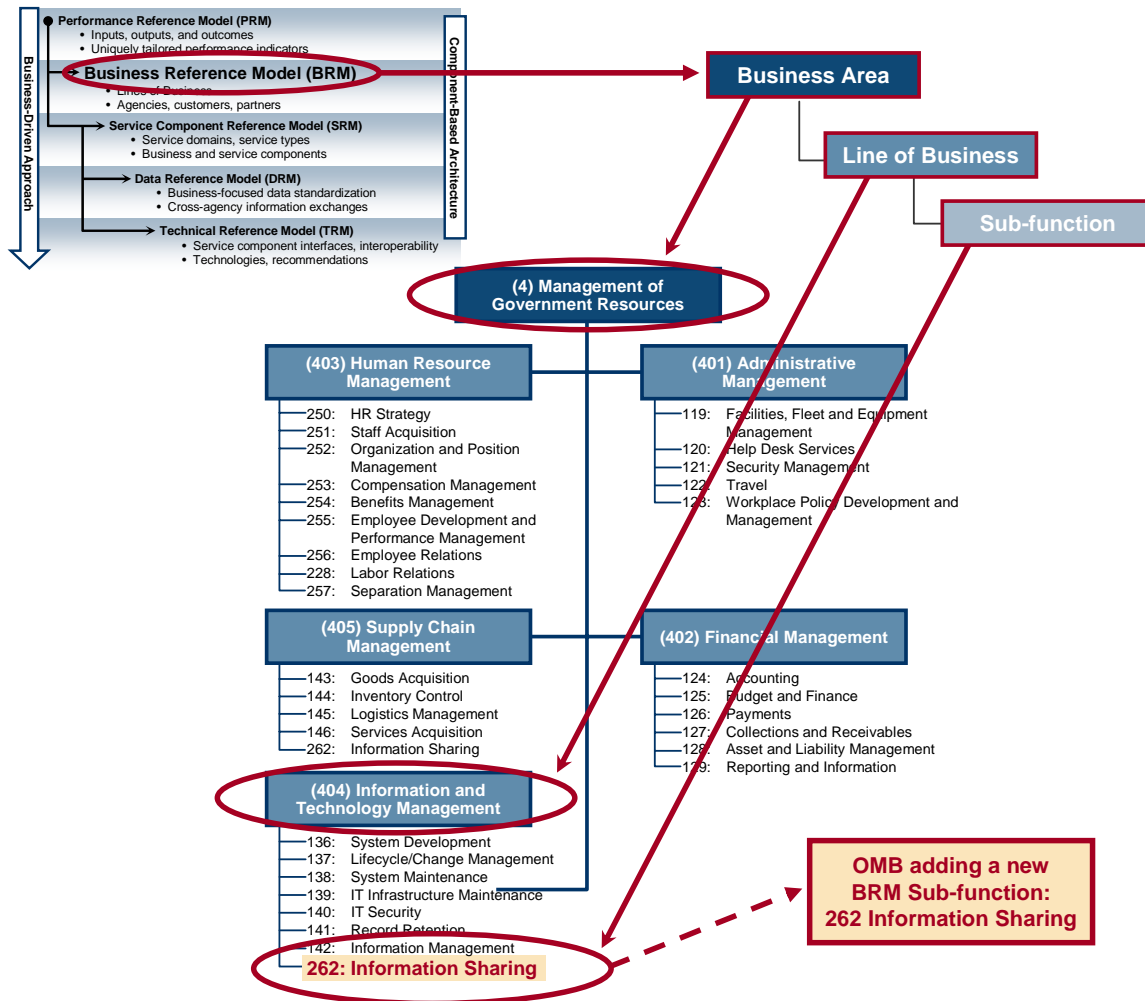


Figure 4-2. The ISE Sub-Function Is Being Added to the FEA BRM

This new BRM sub-function will provide a single, distinct place for budgeting information sharing investments. This makes it possible to easily identify ISE investments (among other agency investments in information sharing) and establish performance metrics for ISE deployment. In the case of SAR, a participant would identify this subfunction in their investment portfolio that directly supports the storage and dissemination infrastructure supporting cross-community SAR.

<sup>63</sup> OMB, *FEA Consolidated Reference Model Document, Version 2.2*, (OMB: Washington, DC, 2007), 45.

### 4.3.2 Initial Set of Target Business Processes

An initial set of business processes describing the ISE mission have been identified. By using business process information flows, ISE participants are able to determine the availability of appropriate information based upon mission requirements. Further, analysis is required of information flows supporting identification of ISE information exchanges (described further in Chapter 5), and the terrorism information gaps that may exist within and among ISE participants. The ISE Business Process Framework, illustrated in Figure 4-3, shows the three types of ISE business processes and links the ISE Mission Drivers to the ISE Mission Processes.

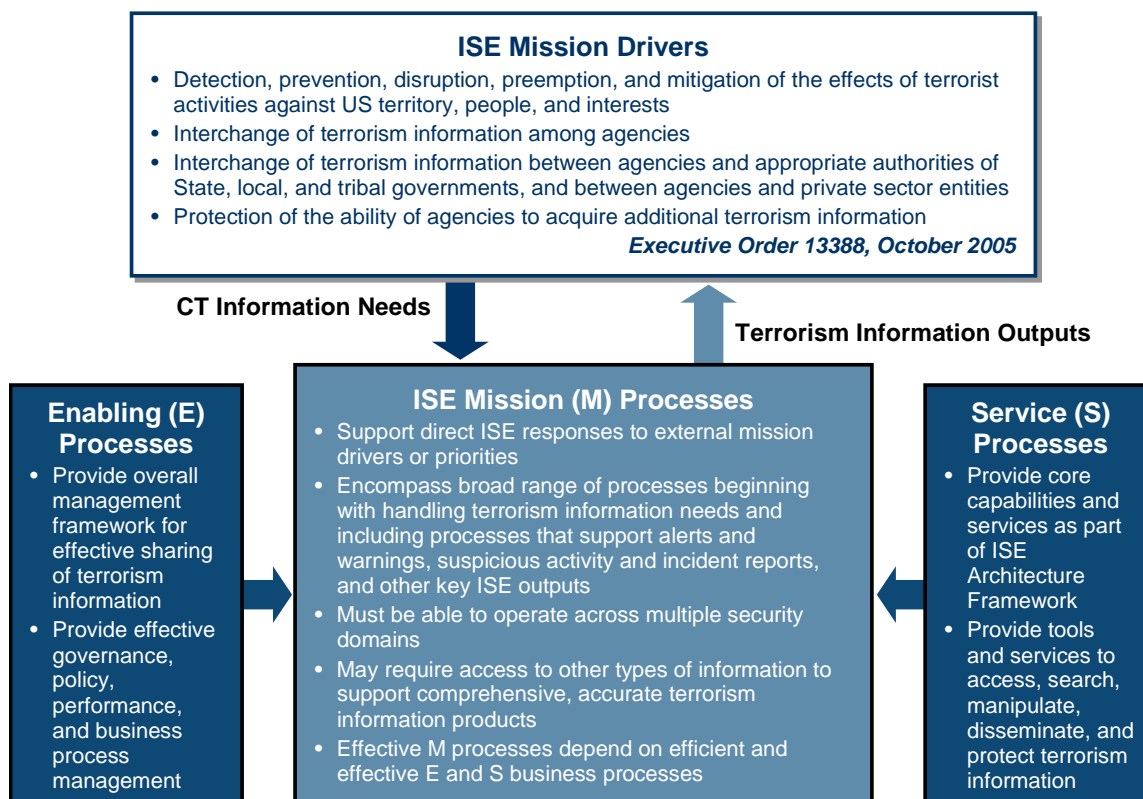


Figure 4-3. ISE Business Process Framework

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

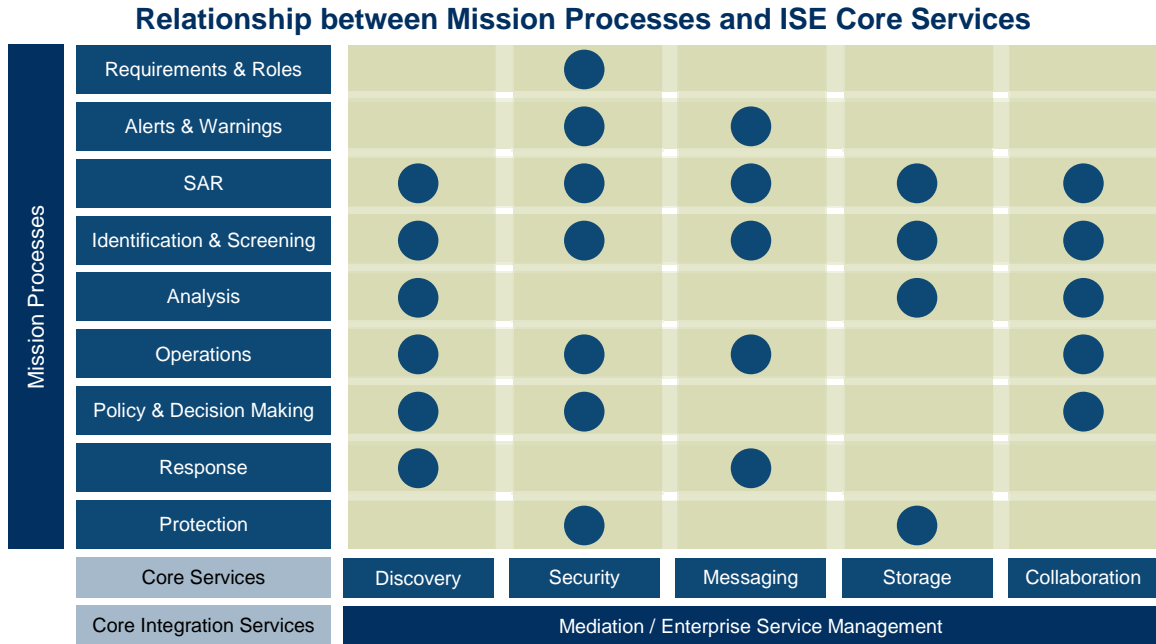
An initial list of the ISE business processes is provided in Table 4-2. Details for the business processes are provided in the ISE EAF Business Partition Description.

**Table 4-2. Overarching ISE Business Process Descriptions**

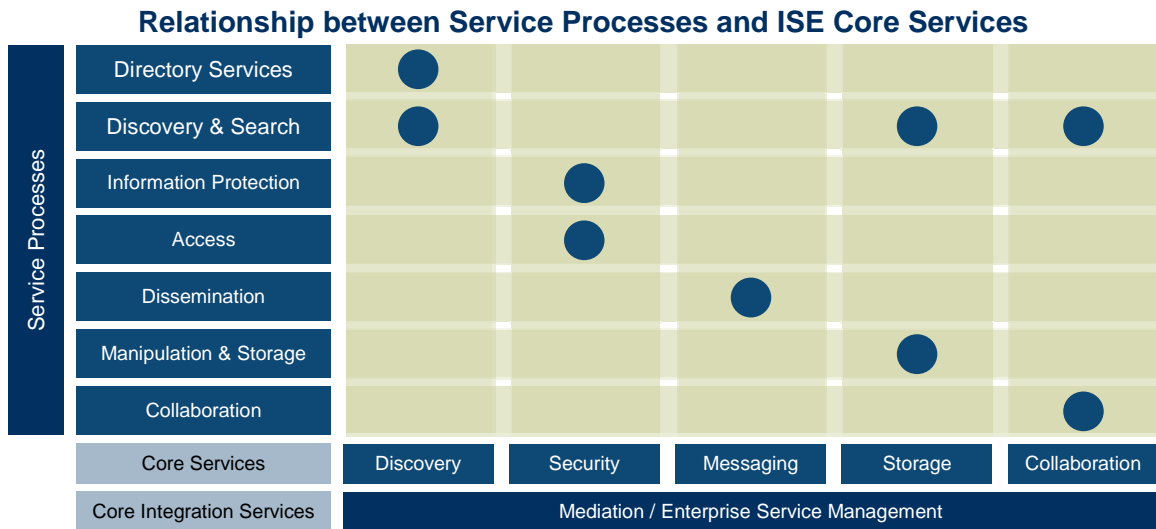
Mission Processes	Enabling Processes	Service Processes
Information Requirements and Roles	Issuances	Access
Alerts and Warnings	Information Sharing Agreements	Discovery and Search
Suspicious Activity Reporting (SAR)	Business Process and Performance Management	Manipulation and Storage
Identification and Screening	Training/Cultural Change	Directory Services
Analysis	Security Framework	Dissemination
Operations	Standards and Architecture	Information Protection
Policy and Decision Making	Privacy and Civil Liberties Protection	Collaboration
Response	Governance and Management	
Protection		

As discussed in Chapter 3, the ISE Core consists of three major components: ISE Core Transport, ISE Core Services (Discovery, Security, Messaging, Storage, Collaboration, Mediation, and Enterprise Service Management), and ISE Portal Services (User Interface, Portal Management, Publish/Subscribe, and User Assistance). The portals are represented by the ISE Portal, which provides the primary human interface to the ISE, and the ISE Management Portal, which provides the management and administration interface. The ISE Core Services are those services required to provide a service-based architecture and are used by nearly all ISE participants. ISE Core Services enable the execution of ISE business processes across information sharing systems in the ISE. A detailed description of the ISE Core Transport, ISE Core Services, and ISE Portal Services is found in Chapter 6. A mapping of Mission Processes and Service Processes to the ISE Core services is illustrated in Figure 4-4 and Figure 4-5 below.





**Figure 4-4. Relationship Mapping of Mission Processes and ISE Core Services**



**Figure 4-5. Relationship Mapping of Service Processes and ISE Core Services**

ISE business process development is an ongoing effort. Updated groupings and a list of ISE business processes and definitions will be provided in a subsequent version of the ISE EAF Description. A matrix of the ISE business processes to the current BRM sub-functions is provided in Appendix F.

As depicted in Figure 4-6, the PM-ISE Overarching Business Process Flow shows the continuous interrelationships and dependencies that significantly impact the critical services identified by the PM-ISE mission drivers. The critical path requires the mission, services, and enabling functions to align in order to carry out key programmatic activities. The SAR evaluation environment will assess and improve proposed ISE-SAR processes to identify the requirements and processes needed to ensure information is discoverable and available to State and major urban area fusion centers. The effective output of this pilot will greatly enhance the nation's ability to route critical information to the people on the ground supporting the mission for the nation.

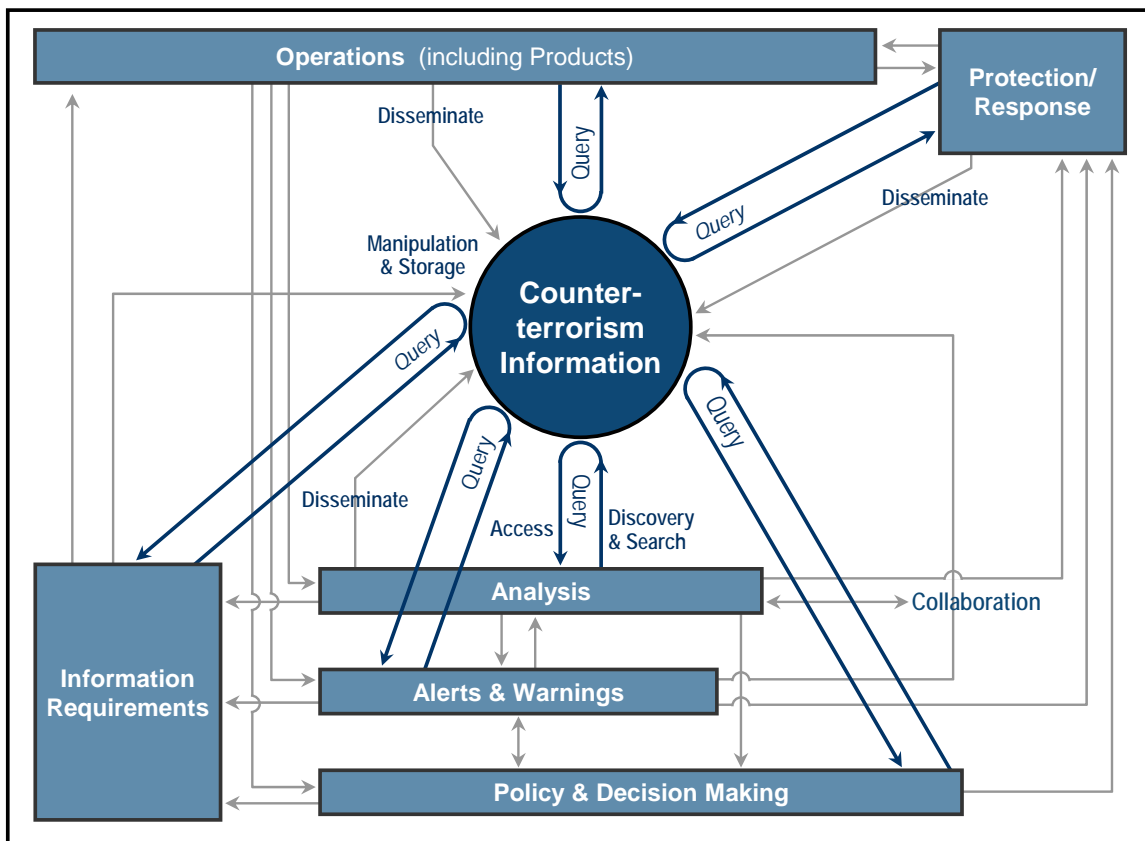


Figure 4-6. Overarching ISE Business Process Flow

The ISE BPWG is working with stakeholders to show the alignment and function of SARs across the ISE. As documents become available, the ISE BPWG will further engage all key players as appropriate.

### 4.3.3 ISE Business Process Modeling Methodologies

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

- 1) Business Process Descriptions – a brief description in the ISE BRM; and
- 2) Business Process Models – a 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 H. The list of business processes includes areas that are currently implemented and areas where gaps exist. 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, to include the types of information required for sharing (records, databases, documents, etc.). Each event, activity, responsible party and their 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. ISE Participants are currently working to model business processes to identify such information needs.

The Federal Bureau of Investigation (FBI) provided a BPMN example for the “Conduct Investigation” business process as shown in Figure 4-7. This model can be tailored to include the business activities and information needs of other ISE users. This example merely indicates the type of information exchange that would be illustrated through modeling of the ISE business processes using BPMN.

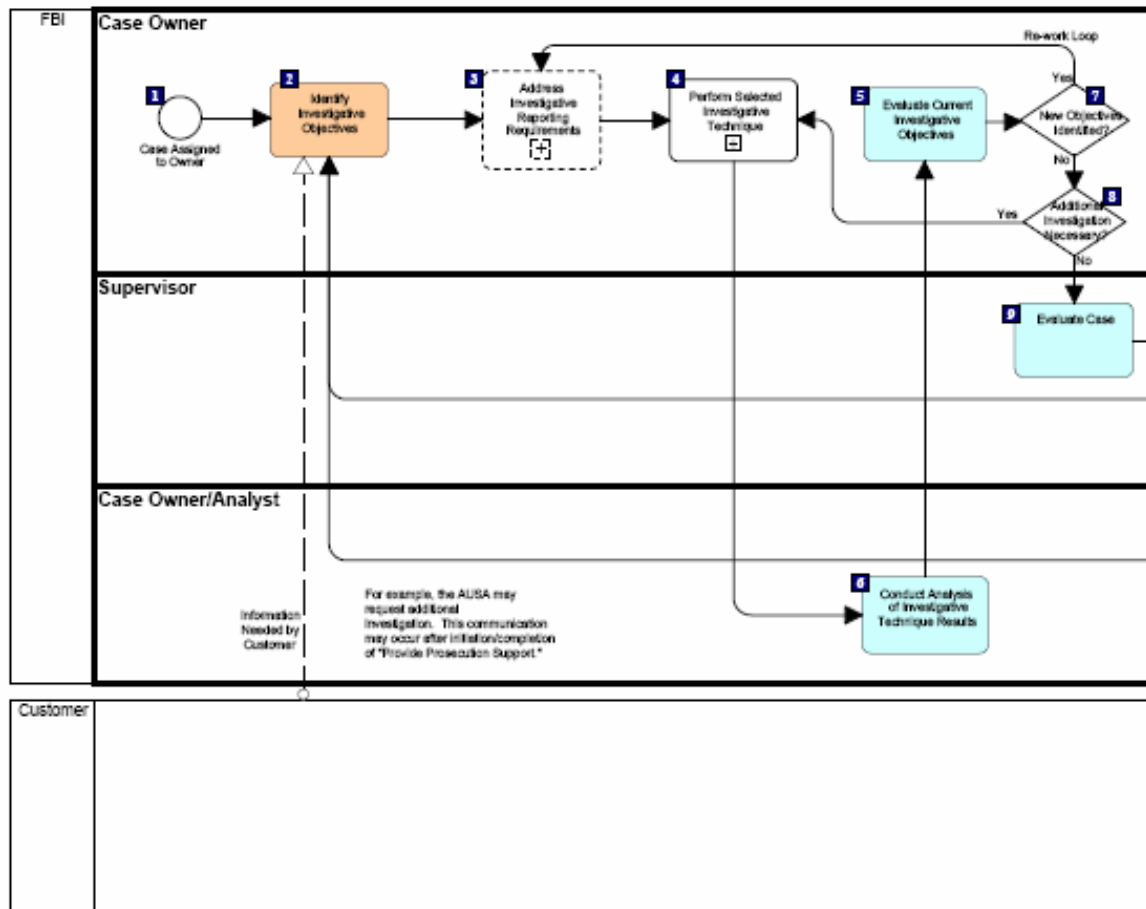


Figure 4-7. Example Portion of a BPMN Diagram: Conduct Investigation<sup>64</sup>

#### 4.4 Business Partition Transition Strategy

The OMB EA Assessment Framework requires a transition strategy from an EA baseline to its target architecture. Chapter 6 describes the concept of an ISE Shared Space. The ISE Shared Space is designated to host ISE participant shared services and data. For example, in the case of SAR, the Shared Space of a participant would be the access point, and optionally the repository, for SAR data. ISE participants will determine their services and data appropriate for sharing based upon applicable policy and internal processes. Those shared services and data will be placed in a separate area behind the organization's network firewall, but within the ISE Shared Space. The ISE Shared Space is the key to the ISE Core which is the information transport for the participants' capabilities.

<sup>64</sup> Figure adapted from U.S. Department of Justice, Federal Bureau of Investigation, Business Process Reengineering Investigative Results (Version 1.1, 15 June 2006).

The Information Sharing BRM sub-function is similar to the BRM sub-function for archiving. The (262) Information Sharing BRM sub-function is not meant to host the mapping of an agency's mission-related activities for collecting and processing information. It provides a bin for the components necessary to build and allow access to an organization-hosted ISE Shared Space. ISE participants need to determine how they will build an ISE Shared Space to include a secured physical space outside of internal networks, expose data, and provide access to and use of shared services.

Submission of the ISE sub-function Line of Business Initiative Plan is one part of the transition strategy for the Business Partition of the ISE baseline to target architecture. OMB acceptance and incorporation of the FEA BRM sub-function into the overall FEA BRM provides a clear framework to illustrate the target ISE EAF business partition. ISE BRM sub-function items highlighted in the baseline architecture with associated processes would then transition to the new FEA BRM sub-function.

The ISE EAF Business Partition Transition Strategy includes:

- Established FEA BRM sub-function (262) "Information Sharing";
- Identification of processes that could benefit from ISE capabilities;
- Re-engineering of those identified processes by ISE participants, as needed; and
- Establishment of participant projects, as necessary, to implement ISE capabilities in support of the re-engineered processes.

For the target ISE EAF Business Partition, additional detail will be added to the baseline partition incorporating the reengineered ISE business processes. The target partition conceptual approach will show the business process information flows using the organizations and capabilities of 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.

This page intentionally blank.

## Chapter 5 – Data Partition

### 5.1 Introduction

The Data Partition of the ISE EAF identifies the vocabulary and information exchange structures necessary to support the ISE mission, vision, and performance goals. Baseline (AS-IS) and target (TO-BE) views are currently under development, however a summary of the key features of each are provided in this section. The products used to describe the Data Partition are summarized in Table 5-1. Not all products are used in both the baseline and target views.

**Table 5-1. Data Partition Products**

*Note: B/T refers to whether the product is used in the baseline or target view.*

Data Partition		
Product Name	B/T	General Description
<b>Controlled Vocabulary</b>	B/T	A list of data elements and their definitions based initially on the CTISS vocabulary. This will include lists for Core (consisting of Universal and Common Data Components) and for each community.
<b>Logical/Concept Data Model</b>	B/T	A model of universal entities which include Common Data Dictionary, Entity Relation Diagrams, and other documents. These are the elements shared by the ISE communities.
<b>Functional Standards</b>	B/T	The controlled vocabulary is used to construct functional standards of use to business processes. The functional standard is a complete specification of an ISE information exchange, including the content and structure of the exchange and documentation to explain the business context.
<b>Information Exchange to BP Matrix</b>	T	This is a matrix which shows which information exchanges are used by which business processes.

### 5.2 Baseline Data Partition

As discussed in Section 3.6, the PM-ISE has designated the CTISS Working Group (CTISS WG) as the primary body for developing and harmonizing ISE common standards. The CTISS effort is defining standards categories, standards defining bodies, core standards, and business process-driven functional standards. These standards are necessary to establish an integrated, nationwide enterprise of information sharing organizations and resources.

NIEM and the DoD/IC Universal Core (U-Core) are both being leveraged under the CTISS to provide the ISE Baseline Data View. Harmonization with other ISE participants currently not using NIEM and the DoD/IC U-Core exclusively for terrorism information sharing will be through the CTISS process.

NIEM was initiated by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) to provide the foundation and building blocks for national-level

interoperable information sharing. NIEM complies with directives specified in the Homeland Security Presidential Directive-5 (HSPD-5)<sup>65</sup>, the Homeland Security Act of 2002<sup>66</sup>, and Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. The DoD/IC Universal Core (U-Core) was developed jointly by the DoD and IC to provide information sharing across their representative agencies and the enterprise. The U-Core consists of information on the nature, the location, and the timeframe of information exchanges that support the defense and intelligence communities. The U-Core design leverages information exchange successes coming from the Community of Interest construct and the Cursor on Target implementations.

### 5.2.1 Functional Standards

As defined in Section 3.6, functional standards will contain the business context, information exchanges, and provide implementation guidance. Based on the information provided in these standards, an ISE participant may be able to implement the exchange as is or may be able to modify or extend it 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 the 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 assurance are present.

### 5.2.2 Linkage between Business and Data Partitions

The functional standards are intended to provide instruction to ISE participants when implementing a specific exchange of data. The business requirements and information flows between participants are described by business processes as contained in the ISE EAF Business Partition. Ultimately, the linkage between the ISE 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 business processes will provide the requirements for shared data that will ultimately be documented in a functional standard. The process for deriving additional data requirements from business processes is consistent with the information exchange development life cycle, as described in Section 5.4.1.

The relationship between the ISE EAF Business and Data Partitions will be shown in a matrix cross referencing the identified ISE Business Processes and information

---

<sup>65</sup> 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>.

<sup>66</sup> *Homeland Security Act of 2002*, Public Law 107-296 (November 25, 2002).



exchanges. This matrix will be developed as the business processes and information exchanges are defined.

## **5.3 TO-BE Data Partition**

### **5.3.1 Overview**

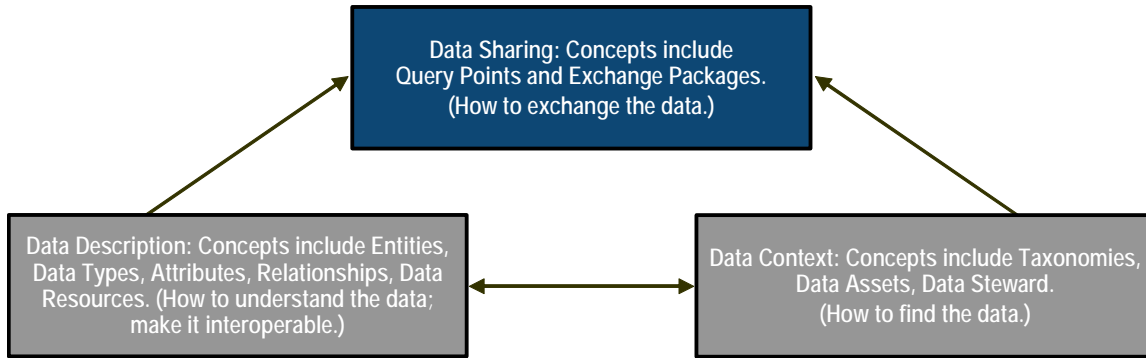
The Target Data Partition will include all the products of the baseline, but these products will be more fully developed. Functional standards will be developed following the concepts and assumptions put forward by the CTISS baseline standards process for metadata and data. ISE communities will work with standards defining bodies to fill critical gaps in available standards.

### **5.3.2 Compliance with the FEA Data Reference Model**

An objective of the ISE is to use metadata in a way which 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, and
- Data Sharing.

An overview of the DRM is given in Figure 5-1, and the abstract model is provided in Figure 5-2.



“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 5-1. 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 which 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 which 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 which 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.

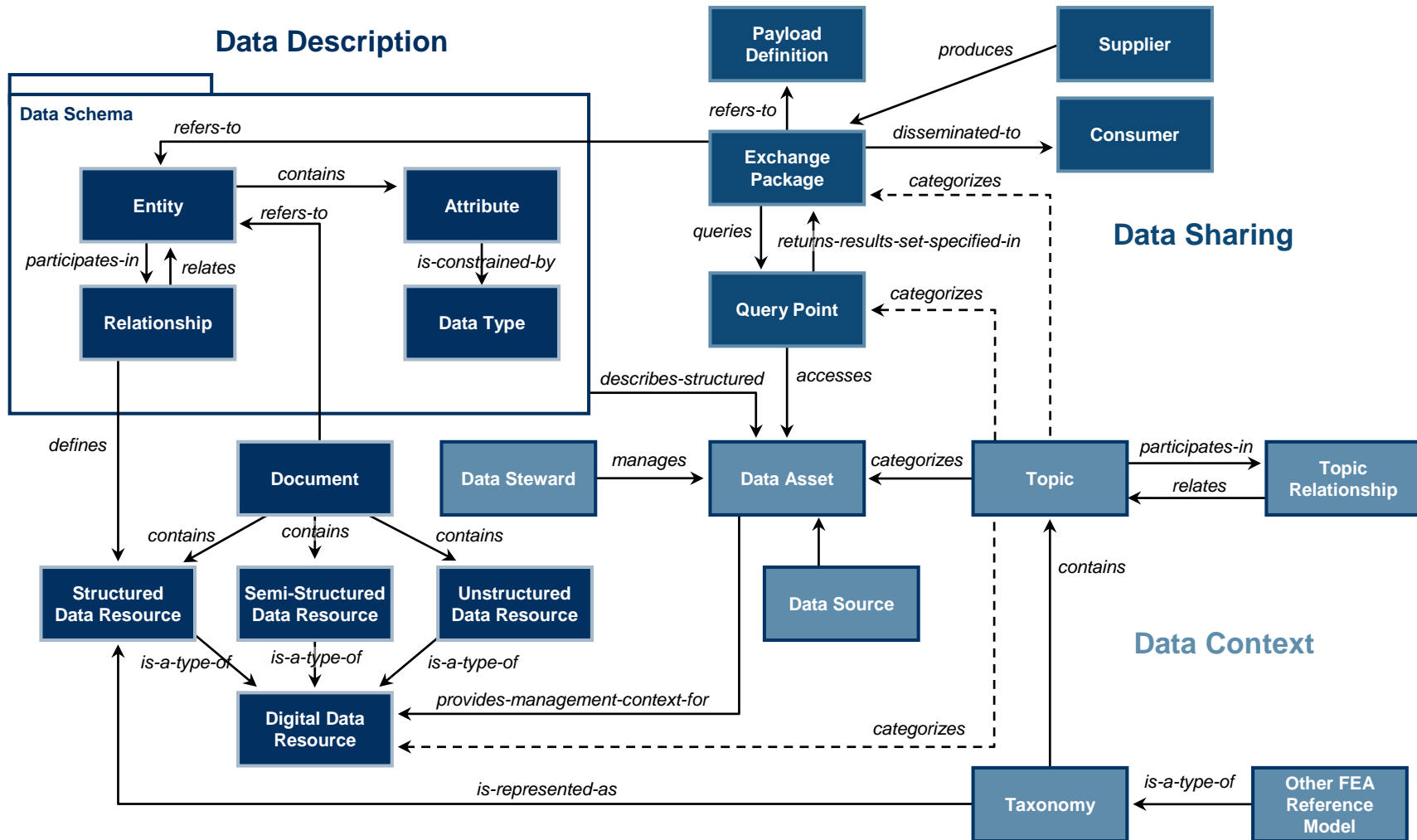


Figure 5-2. DRM Abstract Model<sup>67</sup>

<sup>67</sup> 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](http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf).

## 5.4 Data Partition Transition Strategy

### 5.4.1 The CTISS Development Process

The CTISS Framework (see Figure 5-3) provides standards categories, standards defining bodies, and core and functional standards. Defining bodies organize and define standards content under their purview, and identify, develop, and release core standards that will be leveraged and tailored for development of specific ISE business process-driven functional standards. Defining bodies also provide valuable insight for establishing oversight and guidance processes into standards implementation activities used across the ISE Community.

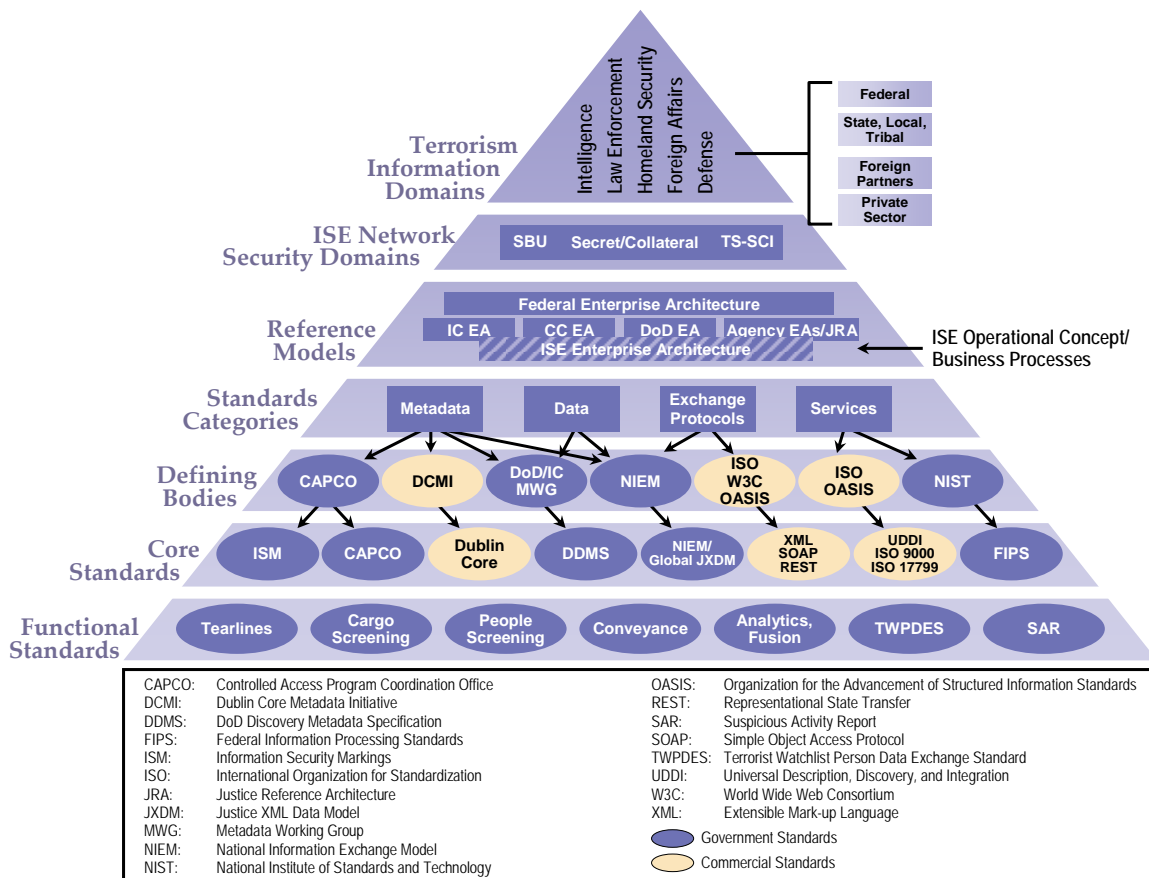


Figure 5-3. CTISS Framework<sup>68</sup>

<sup>68</sup> Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Ibid.

NIEM is a defining body involved with the Metadata, Data, and Exchange Protocols standards categories. U-Core is a defining construct in partnership with the DoD and IC communities that defines and governs a lightweight standard approach for information sharing across the enterprise. Figure 5-4 depicts how NIEM and the DoD/IC U-Core 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, standards, and processes that will serve as the foundation for ISE information exchanges. Other data elements particular to the information sharing business process will also be integrated with CTISS Universal Core elements to define and standardize the overall information exchange.

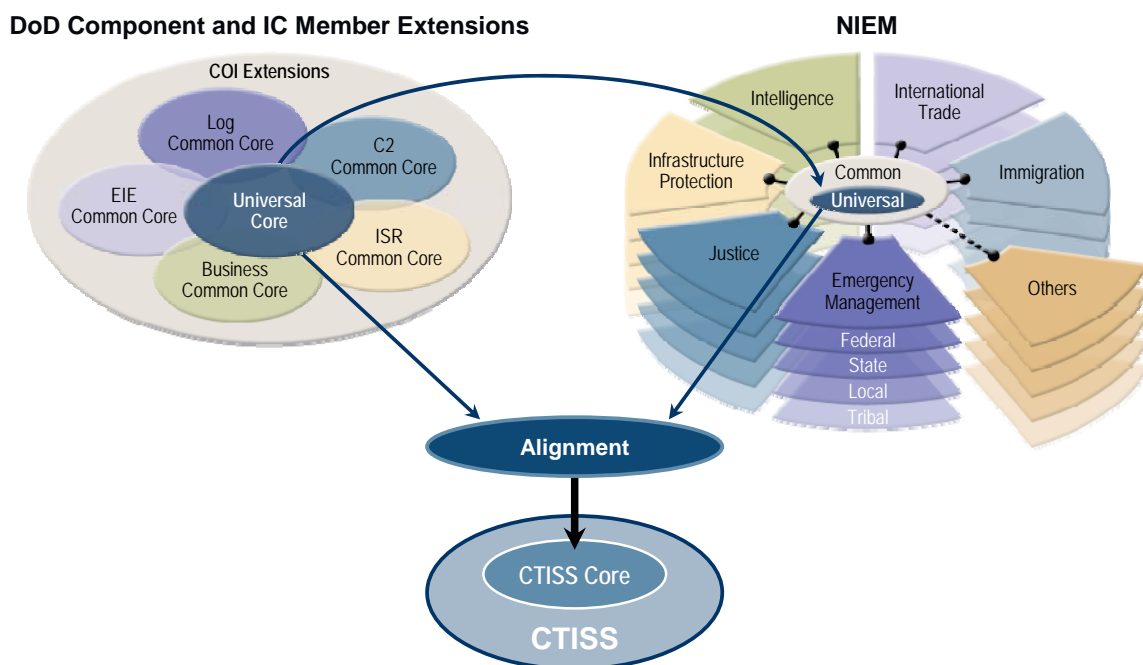


Figure 5-4. CTISS Universal Core Development

In order for an organization to participate in 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 5-5 illustrates the steps of the CTISS functional standard life cycle an ISE participant might follow when developing a standard.

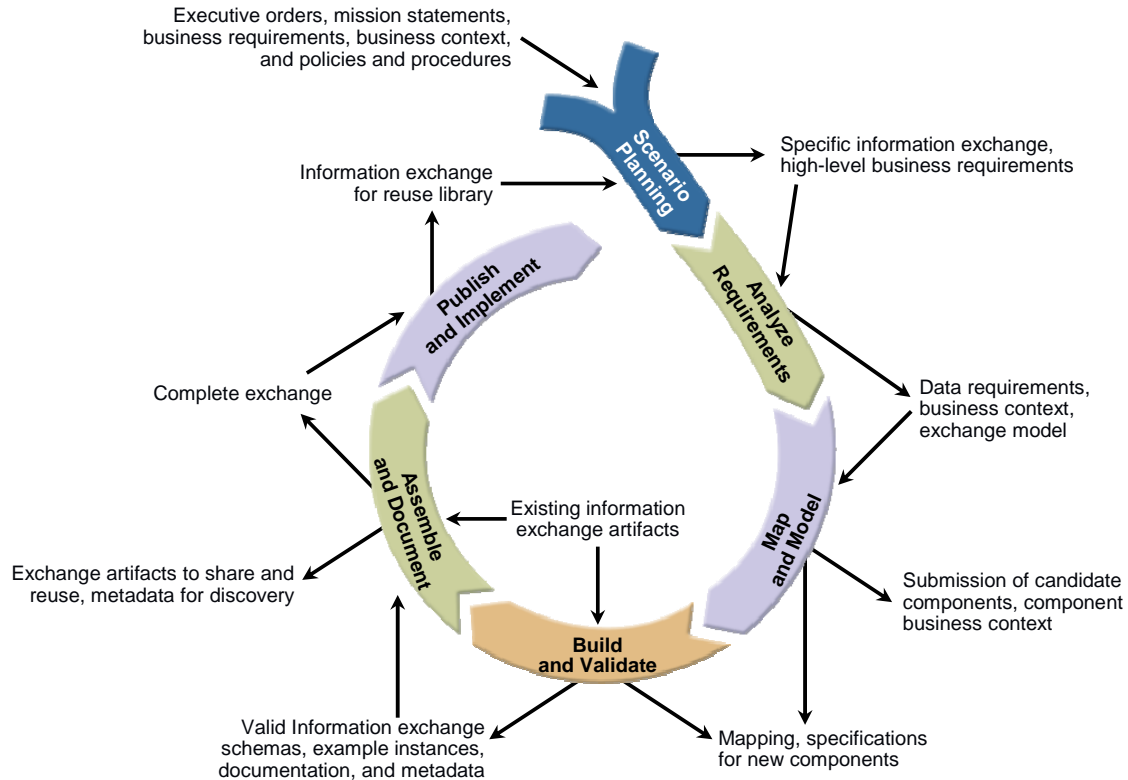


Figure 5-5. CTISS Information Exchange Life Cycle<sup>69</sup>

## 1) 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. 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.

## 2) 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.

<sup>69</sup> Derived from the Information Exchange Package Document (IEPD) Life Cycle found in *NIEM Concept of Operations*, (NIEM Program Management Office: Washington, DC, 2007), 33.

3) Map and Model.

Searches are executed to determine if there are existing exchange packages that satisfy the requirements. The COI<sup>70</sup> 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.

4) 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 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.

5) Assemble and Document

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

6) Publish and Implement

The last stage of the information exchange lifecycle is publishing and implementing. The CTISS functional standard is published within a CTISS information exchange and CTISS Federated Registry that is available to other COIs for reuse. The COI may opt to publish the information exchange only in its domain.

---

<sup>70</sup> COI is used throughout this section to refer to a COI working on a particular data exchange model in support of the ISE program.

The CTISS process will fully support the FEA DRM. Table 5-2 summarizes the FEA DRM support provided by the CTISS information exchange development process.

**Table 5-2. 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

#### 5.4.2 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. There should be a loose technical governance structure around the COIs that assures that there is not duplicate work being conducted across COIs.

#### 5.4.3 Observations and Issues

Because ISE implementers will follow and incorporate the CTISS, there needs to be a mechanism for assuring compliance. 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, XML and Web services, service-based architectures, 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 adapted. 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.



A long-term strategy should consider formal semantic representations for the CTISS data and metadata elements to provide a stable foundation supporting precise common meanings, accurate translations, semantic search, semantics-based information extraction and integration, and effective analysis of shared information. Evaluation studies and prototypes are needed to pave the way for a semantic technology implementation roadmap that will provide the ISE and its stakeholders the benefits of semantic capabilities. For example, the Web Ontology Language (OWL) and Resource Description Framework Schema are beginning to be adopted as standards as the World Wide Web evolves into the Semantic Web. Creation of a prototype that evaluates the use of OWL for data exchange in the ISE should be considered.

This page intentionally blank.

---

## Chapter 6 – Application and Service Partition

### 6.1 Introduction

#### 6.1.1 Overview

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 architecture 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-based architecture approach using services as described in Section 7.4 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 service-based architecture.

#### 6.1.2 Terminology

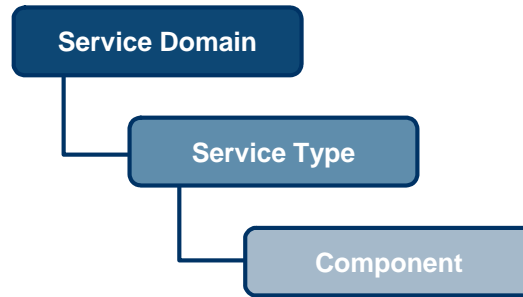
One of the constructs used to organize the Application and Service Partition is the FEA Service Reference Model (SRM).<sup>71 72</sup> The SRM uses the word “service” to indicate activities performed by an enterprise on behalf of its customers. These activities are either fully automated, software-driven 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 which 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.

---

<sup>71</sup> OMB, *FEA Consolidated Reference Model Document, Version 2.2, Ibid.*, 46-63.

<sup>72</sup> 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.



**Figure 6-1. FEA Service 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 are comprised 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 predetermined functionality that may be exposed through a business or technology interface<sup>73</sup>.” 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-based principles, as stated above. Service-based architecture refers to “line-of-business services” as those services which automate a unique portion of a business process typically not reusable by others. Service-based architecture refers to “core services” as services required by a majority of developers and users. 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, by contrast, are newly developed services that encapsulate business processes for exposure via the ISE.

### 6.1.3 Architectural Products

The products used to describe the Application and Service Partition are summarized in Table 6-1. Some products are applicable to both the baseline (B) partition and the target (T) partition while others are applicable to the target partition only.

<sup>73</sup> Office of Management and Budget, *Ibid.*, 46.

**Table 6-1. Application and Service Partition Products**  
*Note: B/T refers to whether the product is used in the baseline or target view.*

Application and Service (A&S) Partition		
Product Name	B/T	General Description
<b>Terrorism Data Asset</b>	B/T	Data assets (in the DRM sense of the term) that could potentially be useful for counterterrorism (not necessarily currently accessible for sharing) (e.g., the FBI fingerprint database, a terrorist watchlist, criminal records, intelligence reports).
<b>Core Service Description</b>	T	A description of each service provided as part of the ISE Core Services available in the ISE. This includes a complete description of the contract for invoking the service.
<b>Shared Service Description</b>	T	A description of each service provided by agencies participating in the ISE. This includes a complete description of the contract for invoking the service.
<b>Application Description</b>	B/T	A list and description of the applications composing the ISE EA. Services and data assets are typically components of a larger application or system. Applications that may provide services or data assets to the ISE are listed and described. The applications list is used to categorize data assets and services (e.g., the FBI Sentinel application).
<b>SRM Mapping</b>	T	A mapping of ISE Core Services, ISE Portal Services, and Shared Services to the FEA SRM.

## 6.2 FEA Service Reference Model Mapping

The FEA Service Reference Model, shown in Table 6-2, 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 not shown in the table. These SRM Service Components map to the ISE Core Services and ISE Portal Services.

Table 6-3 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. A more detailed mapping will be provided as an architectural product on the ISE Web Site.

**Table 6-2. FEA Service Reference Model**

Service Domains	Service Types	
<b>Customer Services</b>	<ul style="list-style-type: none"> <li>• Customer Relationship Management</li> <li>• Customer Preferences</li> </ul>	<ul style="list-style-type: none"> <li>• Customer Initiated Assistance</li> </ul>
<b>Process Automation Services</b>	<ul style="list-style-type: none"> <li>• Tracking and Workflow</li> <li>• Routing and Scheduling</li> </ul>	
<b>Business Management Services</b>	<ul style="list-style-type: none"> <li>• Management of process</li> <li>• Organizational Management</li> </ul>	<ul style="list-style-type: none"> <li>• Investment Management</li> <li>• Supply Chain Management</li> </ul>
<b>Digital Asset Services</b>	<ul style="list-style-type: none"> <li>• Knowledge Management</li> <li>• Records Management</li> </ul>	<ul style="list-style-type: none"> <li>• Content Management</li> <li>• Document Management</li> </ul>
<b>Business Analytical Services</b>	<ul style="list-style-type: none"> <li>• Analysis and Statistics</li> <li>• Visualization</li> <li>• Business Intelligence</li> </ul>	<ul style="list-style-type: none"> <li>• Knowledge Discovery</li> <li>• Reporting</li> </ul>
<b>Back Office Services</b>	<ul style="list-style-type: none"> <li>• Data Management</li> <li>• Human Resources</li> <li>• Financial Management</li> <li>• Asset/Materials Management</li> </ul>	<ul style="list-style-type: none"> <li>• Development and Integration</li> <li>• Human Capital/Workforce Management</li> </ul>
<b>Support Services</b>	<ul style="list-style-type: none"> <li>• Security Management</li> <li>• Search</li> <li>• Communication</li> </ul>	<ul style="list-style-type: none"> <li>• Collaboration</li> <li>• Systems Management</li> <li>• Forms Management</li> </ul>

**Table 6-3. 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

For example, the SRM mapping for the SAR includes content management, data management, and security management.

## 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 amongst organizations; however these include 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, provide 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.<sup>74</sup>

Numerous existing systems and data assets in the Federal government contain useful information that could be leveraged for terrorism information sharing. However, many of these existing systems have been developed independently to solve a specific problem without necessarily accounting for the need to share information effectively across agencies. 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. Ultimately the ISE Electronic Directory Service (EDS) will provide “Green Pages” that enable categorization and listing of counterterrorism-related information sharing resources to support users searching for specific data and capabilities. This will then become a continually updated architectural product of the Application and Service Partition.

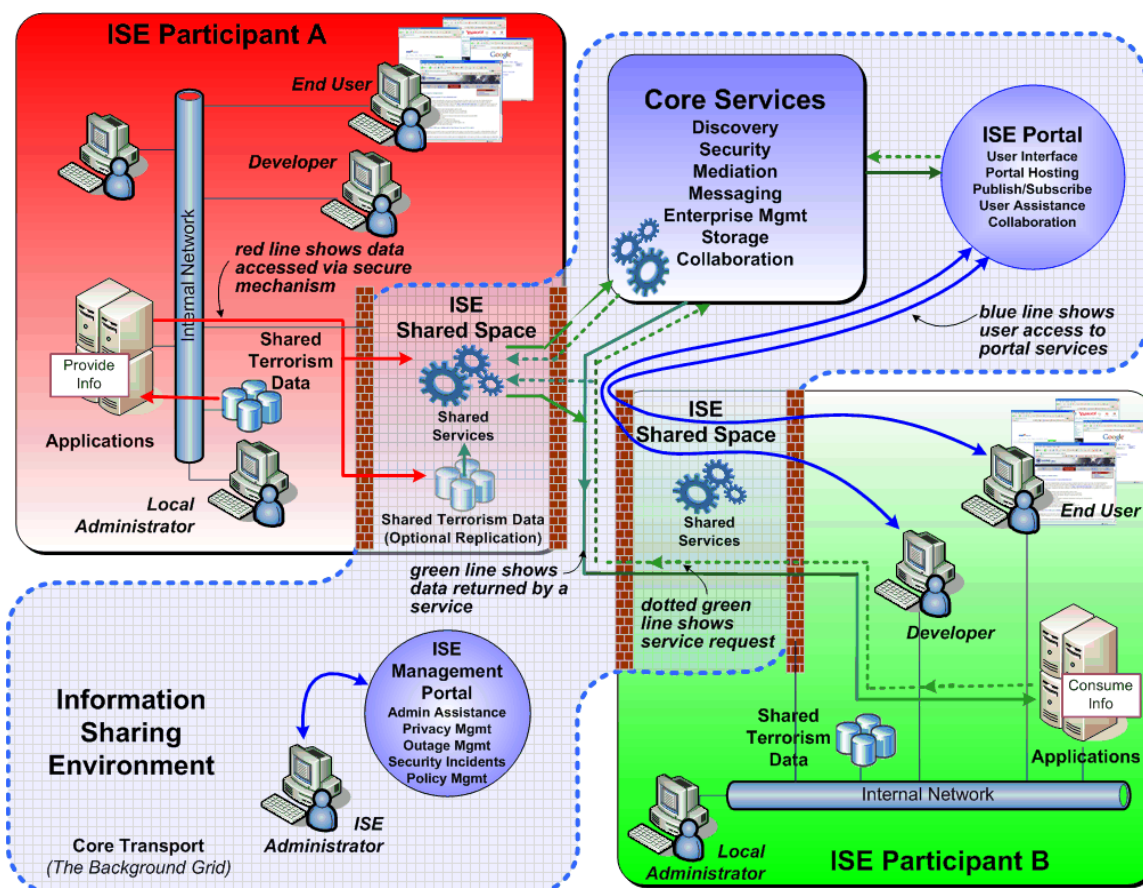
## 6.4 Application and Service Target Partition – ISE Core Segment

### 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 exist to support the three security domains: 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 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 6.4.4. The IMP is the primary management and administration interface to the ISE. Its functions are described in Section 6.4.5. 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 6.4.6.

<sup>74</sup> OMB, *The Data Reference Model Version 2.0*, Ibid.

Note that the ISE Core is described herein as an independent entity. 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 NCTC.



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

## 6.4.2 Transport

Information sharing between ISE participants requires a means to connect those organizations to one another. This connectivity is achieved by the component of the ISE referred to as the Core Transport as described in Section 7.6. The Core Transport architecture 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: SBU, Secret/Collateral, and TS/SCI. The State and major urban area fusion centers and private entities typically won't include an SCI network. The network management function, which is described in more detail in Section 6.4.3, 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.) which 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 IT Implementation Agent should have current transport capabilities that can be leveraged for the ISE. As mission processes and requirements are better understood, the IT Implementation Agent should develop additional transport capability. Continuing with the SAR example, the initial transport capability exists within agencies. However, as SAR and ISE mission processes become better defined, new transport capability 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 Information Technology Implementation Agent<sup>75</sup> to develop the ISE transport infrastructure. This 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 telecommunication service provider. There are multiple full-service providers that 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 others. 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

---

<sup>75</sup> Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Ibid.

identify their policy guidance approach to transport including identification of requirements documented using standard operating procedures, system administrator instructions, and other policy guidance documentation.

### 6.4.3 Network Management Function

A network management function will be provided by the same Implementation Agent organization which 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 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 all security domains: 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.

### 6.4.4 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 UDDI (Universal Description, Discovery, and Integration) registry.

The description should include any special considerations for or limitations to the use of the service, and a point of contact.

- A user can perform a federated search.<sup>76</sup> A federated search allows a user 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 a user the ability to formulate a query based on a set of parameters and subsequently narrow the search through more specific parameter refinement. For example, in the case of SAR, this service would allow all participants to query data elements stored within SAR records.

**Portal Hosting:** The ISE Portal provides the capability for any agency to provide access to a specific agency portal. For example, Participant A may elect to provide a separate portal to information and capabilities relative to its mission area. That participant portal can be viewed as a “sub-portal” of the ISE portal. This provides ISE Portal users the ability to reach the participant portal from the ISE portal. This provides 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 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). In the case of SAR, this could be an output of the overall SAR analysis.
- **Subscribe to Alerts:** Both users and automated processes can subscribe to alerts. Subscription processes can be tailored in terms of delivery, priority, and distribution.<sup>77</sup>
- **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.<sup>78</sup>
- **Subscribe to Information Feeds:** Users can subscribe to information feeds. Subscription can be tailored in terms of delivery, priority, and distribution. In the example of SAR, access to the SAR data might be accomplished with this service.
- **Subscribe to information about ISE Status:** These include events such as planned outages, problems, and resolutions.

---

<sup>76</sup> Office of the PM-ISE, *Ibid.*, Section 5.4. This capability is also referred to as “Enterprise Search” in the reference, although “federated search” is the commonly accepted terminology.

<sup>77</sup> Office of the PM-ISE, *Ibid.*, Section 5.2.

<sup>78</sup> *Ibid.*, Section 5.2.

**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:

- 1) Automated self help provides “how to” information, usually called Frequently Asked Questions (FAQ) documents;
- 2) The ISE Knowledge Base provides both “how to” and problem resolution information. This information is provided by ISE management and end-user forums; and
- 3) 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 which provide on-demand help for user profiling and customization, and portal presentation/foundation for integration of ISE Core Services and capabilities. User Assistance services include Section 508 accessibility validation tools as well.

**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.

The ISE Portal is the primary end-user interface to the ISE. Other capabilities, in addition to those described above, may be added as the ISE evolves.

### 6.4.5 ISE Management Portal

The IMP is intended to provide a central interface for ISE management and administration activities. The ISE Management Portal is implemented over commercial portal technology and may vary for each of the three security domains. The ISE Management Portal(s) 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 allows ISE status to be reflected in local reporting locations; allows users and processes to implement alternate service choices; and allows users and processes to return to normal processing following a resolution.

**Subscribe to Information Feeds:** Users can subscribe to information feeds concerning ISE management and administration. This 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 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:

- 1) Automated self help provides “how to” information;
- 2) 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;
- 3) ISE real-time support is available through on-line chat; and
- 4) 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.

#### 6.4.6 ISE Core Services

The ISE EAF Core Services represent the common capabilities required by ISE users. The top drivers defining the requirements of the ISE EAF Core Services are directly derived from several authoritative source documents. The Information Reform and Terrorism Prevention Act of 2004 mandates the ISE build upon existing systems’ capabilities. This promotes reuse of architectural elements as well as minimization of unnecessary duplicated system capability.

Core Services provide core software infrastructure in support of the ISE's service-based architecture, often referred to as "middleware". They provide the ability to integrate information consumers and providers. They provide 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:

- 1) Discovery;
- 2) Security;
- 3) Mediation;
- 4) Messaging;
- 5) Enterprise Service Management;
- 6) Storage; and
- 7) Collaboration.<sup>79</sup>

For example, all seven of these ISE Core Services would be leveraged into systems that support the SAR 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 that can be accessed via the ISE Portal. 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 (for SAR, this service capability would assist users in identifying the location of pertinent SAR databases);
- 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; and
- Permit discovery services to be integrated at design or run-time to create other composite services.

These capabilities are summarized in Table 6-4.

---

<sup>79</sup> 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 6-4. Discovery Service Capabilities**

Capability	Description
<b>Metadata Discovery</b>	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; serves as a clearinghouse for official standards and documents.
<b>Person Discovery</b>	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.
<b>Service Discovery</b>	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 invoking their use.
<b>Content Discovery</b>	This capability provides a way to perform federated searches for enterprise content 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 the users of ISE by supporting authentication, authorization and access control processes. 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. In the example of SAR, this service would provide the necessary protections for storing information and controlling access to SAR databases and the stored information. 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; and
- Leverage existing industry standards and specifications from standards bodies.

Table 6-5 below summarizes the capabilities offered by the Security Services category of the ISE.

**Table 6-5. Security Services Capabilities**

Capability	Description
<b>Policy Decision Service (PDS)</b>	Accepts authorization queries and returns authorization decision assertions, conforming to the Security Assertion Markup Language (SAML) Protocol.
<b>Policy Retrieval Service (PRS)</b>	Exposes security policies in Extensible Access Control Markup Language (XACML) format and can be used for service providers to retrieve policies for their resources.
<b>Policy Administration Service</b>	Used by management applications to add, update, and delete authorization policies stored as Policy Sets.
<b>Certificate Validation Service (CVS)</b>	Revocation status checking is performed by allowing clients to delegate the certificate validation tasks.
<b>Principal Attribute Service</b>	Provides query and retrieval interfaces to access attributes for users.
<b>Public Key Infrastructure (PKI)</b>	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. Mediation Services include data transformation and adaptation. In the case of SAR, this service would accommodate the interfacing of disparate SAR systems between different ISE participants Table 6-6 below describes the capabilities offered by mediation services.

**Table 6-6. Mediation Service Capabilities**

Capability	Description
<b>Protocol Adaptation</b>	Allows entities in the enterprise to interoperate without either party having to conform to the other's protocols or technologies.
<b>Data Transformation</b>	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 utilize 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. Alert and notification applications are specific examples that are built on top of Messaging services. Continuing with the SAR example, 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 by “connecting the dots”. The newly identified threat would be communicated back to participants via Messaging services. Table 6-7 below briefly described specific capabilities offered by Messaging services:

**Table 6-7. Messaging Service Capabilities**

Capability	Description
<b>Notification Services</b>	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.
<b>Alerts by topic</b>	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).
<b>Enterprise Messages</b>	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

Enterprise Service Management 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 6-8.

**Table 6-8. ESM Service Capabilities**

Capability	Description
<b>Monitoring and ensuring QoS of critical components</b>	Generates a report about service health and notifies Service Providers about any unusual signs.
<b>Monitoring Service Level Agreements (SLAs) compliance</b>	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.
<b>Providing detection and handling of exceptions</b>	Enables defining exception conditions, detecting and alerting exceptions, and automatically taking corrective actions to handle exceptions in real-time.
<b>Providing insight into the usage of services</b>	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.
<b>Providing distributed management of services</b>	Offers IT asset managers and service providers the ability to configure, manage, and track distributed services remotely.
<b>Accepting and responding to customer feedback</b>	Will provide 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. In the example of SAR, this service would be applicable to the storage of information according to the data formats outlined in the SAR functional standard.

Table 6-9 summarizes the capabilities offered by the Storage services.

**Table 6-9. Storage Service Capabilities**

Capability	Description
<b>Data Source Integration</b>	A set of guidelines and specifications that describe how to create ISE enterprise data sources for access via the ISE Federated Search.
<b>Enterprise Content Delivery Network</b>	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 6-10 describes the capabilities offered by the Collaboration service.

**Table 6-10. Collaboration Services Capabilities**

Capability	Description
<b>Conferencing</b>	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).
<b>Person Discovery</b>	Securely allows use of a global directory service to find people and devices on the network.
<b>Integrated Voice over Internet Protocol Services</b>	Enables voice and video conferencing over Internet Protocol (IP) networks.
<b>Collaborative Workspaces</b>	Provides a place where a group of users can publish, manage, retrieve and share information of all file types. (In the example of SAR, collaborative workspaces would provide the shared space environment for collaborating SAR information gathered by ISE participants.)
<b>Application Sharing</b>	Allows authorized users the ability to share an application running on a user's computer simultaneously with other users.
<b>Application Broadcasting</b>	Allows users to select either an application or a portion of their desktop that they can broadcast to all members of the collaboration session.

## 6.5 Target Application and Service Partition – ISE Participant Segment

The Target Partition of 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 participant target architecture will be an integral part of the EA and Capital Planning and Investment Control (CPIC) performed by each in accordance with OMB guidance. The *FEA-ISE Profile* document will provide guidance on this process.

In addition, the development of federal agency target architectures supporting the ISE will be facilitated by the FTF, a catalog of cross-agency information technology initiatives, including the ISE. The Catalog, published annually by OMB, contains

descriptions of each initiative. Upon updating the FTF with the business, data and services outlined in the EAF, it can be used by agencies to ensure that the Federal Transition Strategy is reflected in their own EA transition strategies and budget submissions. The goal is to assist participants with alignment of IT programs with relevant cross-participant initiatives.

## **6.6 Application and Service Partition Transition Strategy**

Transitioning from the current environment to Target Architecture is a multi-year process. Recognizing this, the *Information Sharing Environment Implementation Plan* adopted a two-phase implementation approach. Phase 1 encompassed those actions scheduled for completion by June 2007—the first steps in a continuous process to improve the way terrorism information is shared across the Federal government; between Federal agencies and SLT governments; and, as appropriate, with private sector organizations and foreign partners. Phase 1 actions addressed the highest priority information-sharing requirements.

Phase 2 includes activities scheduled for completion between June 2007 and June 2009. These activities will often require substantial design and implementation of business processes, supplemented in some cases by fundamental engineering work or incorporation of new technologies. Accordingly, the *Information Sharing Environment Implementation Plan* identifies specific Phase 2 actions but acknowledges that they are not currently defined at the same level of detail as those in Phase 1. Phase 2 activities will require additional planning and design before definitive plans and schedules can be developed and finalized. Moreover, Phase 2 activities will often result in more significant funding requirements involving multiple ISE participants spanning several years.

Since transition to the Target Architecture can be performed incrementally, high priority capabilities resulting in immediate benefits can be implemented early, while lower priority items can be added in the future as time and resources permit.

The transition plan has two major elements:

- ISE Core Transition; and
- Agency Enterprise Architecture Transition.

### **6.6.1 ISE Core Transition**

The ISE Core Baseline does not currently exist as the ISE is a new initiative through IRTPA. The first step in the transition from Baseline to Target Architecture consists of development of an Initial Operating Capability. One or more participants should be selected to provide the ISE Core capabilities as Implementation Agents. Participants should be selected based on their ability to implement the functional and technical capabilities defined by the architecture by building on current capabilities of their internal systems. The steps required to provide the ISE Core are:

- 1) Identify the ISE transport for the three security domains;
- 2) As required, develop additional transport capabilities;
- 3) Establish the network management function and ISE Management Portal capability;
- 4) Establish the ISE Portal Services capability;
- 5) Establish the ISE Core Services capability;
- 6) Establish services to search and access existing business processes/applications for integration into the ISE's service-based architecture; and
- 7) Manage subsequent migration and evolution to a full operational capability.

### 6.6.2 Participant Enterprise Architecture Transition

Each participating organization in the ISE would need to migrate to its ISE-supporting Target Architecture. This would be achieved as part of the normal EA development and IT investment processes within each organization. In the case of the Federal government, annual EA improvements would be made based on the needs of the agencies in accordance with OMB guidance. The *FEA-ISE Profile* will provide specific guidance relative to the ISE.

Fundamentally, each participant should accomplish three things:

- 1) Connect to the ISE Core so that it can access the Core Services and the data and services provided by other participants within the ISE;
- 2) Expose internal terrorism information to other participants by implementing federated search capabilities and custom access services for each of its data assets (In the example of SAR, this would be defining a repository for SAR data using data element definitions in the SAR functional standard); and
- 3) Revise its business processes and supporting systems, as necessary, to take advantage of the capabilities and information provided by the ISE. For example with SAR, participants would incorporate technical requirements for shared space integral to their enterprise architecture and incorporate required investments into their CPIC processes.

Each ISE participant will follow its own process to develop and implement its target architecture in conjunction with the ISE mission process segment architecture, but should include these general steps:

- 1) Consistent with overall guidance, establish terrorism information sharing governance and policies consistent with the ISE EAF Policy and Governance direction. For example with SAR, a participant would adopt ISE guidelines addressing acquisition and retention of replicated SAR data and establish appropriate configuration and program management boards. This would include

implementation of guidelines for replicating SAR data in the shared space and purging SAR records when required.

- 2) Identify and expose counterterrorism data for sharing across the ISE. For example with SAR, participants would store replicated SAR information for access by other ISE participants using appropriate security and storage protocols.
- 3) Develop specialized services related to counterterrorism functions available for wider use via the ISE.
- 4) Provide access to the ISE for participant staff by connecting appropriate participant network assets to the ISE Core Transport. For example with SAR, participants would provide a point of presence from the participant repository of replicated SAR information to the ISE and participants external to the agency/organization.
- 5) Use ISE Core Services to provide information assurance for ISE-exposed assets.
- 6) Update counterterrorism business processes to take advantage of other participants' information not previously available in the ISE.
- 7) Upgrade participant applications to support reengineered business processes and take advantage of ISE Core services, own participant services, and other participants' services and data exposed via the ISE.

## Chapter 7 – Technical Partition

### 7.1 Introduction

The Technical Partition identifies the particular standards and technologies that will support the implementation of the ISE, focusing on the TO-BE architecture. A summary of key features is provided in this section. Detailed products are included in the ISE Technical Partition Description. A summary of products, shown in Table 7-1 below, are applicable to the target Technical Partition.

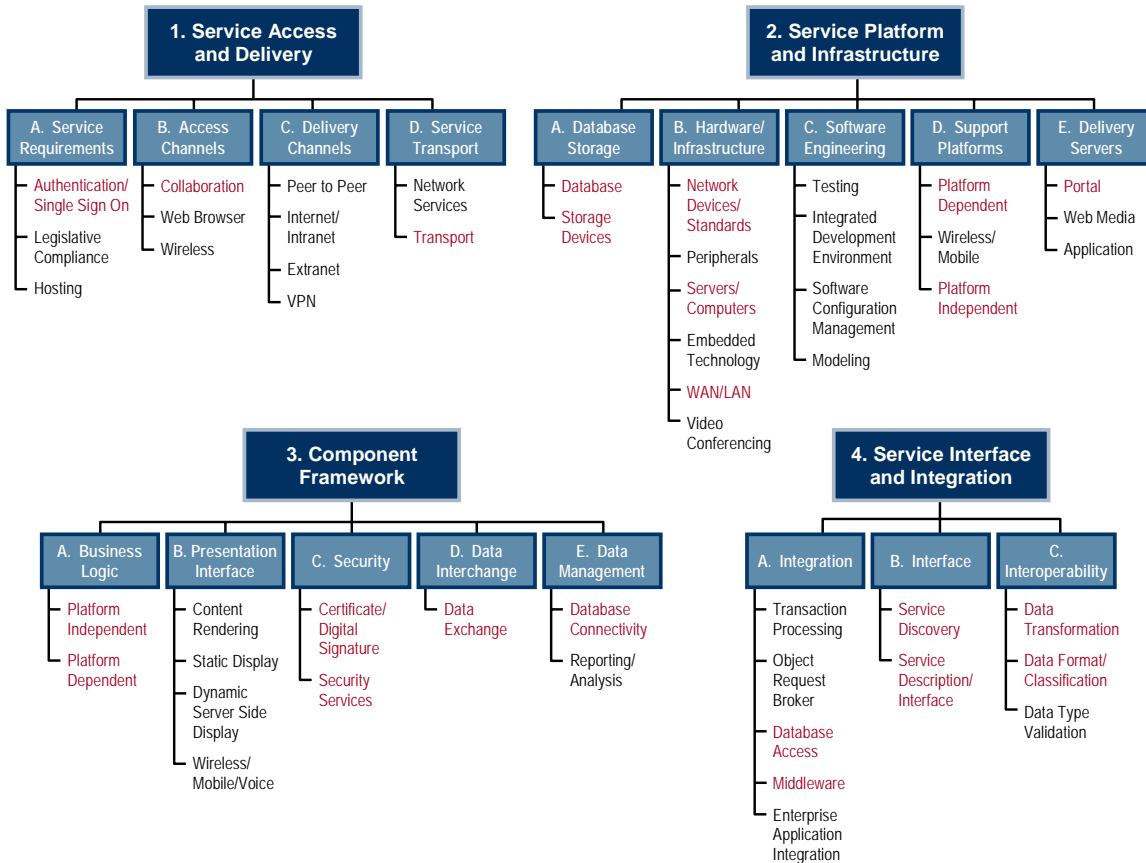
**Table 7-1. Technical Partition Products**

Technical Partition Products		
Product Name	B/T <sup>80</sup>	General Description
<b>ISE Technical Reference Model</b>	T	Identifies the types of infrastructure hardware, software, and telecommunications required to provide the ISE infrastructure and describes their functional characteristics, capabilities, and interconnections. A subset of the FEA TRM.
<b>Enterprise Application Integration Patterns</b>	T	A generic pattern that shows how service-based components may be integrated to accomplish a particular function, such as providing service access to a database.
<b>Transport Description</b>	T	A generic pattern that provides guidance to participants in regards to establishing connectivity between their networks and the ISE Core Transport.
<b>Information Assurance Description</b>	T	A generic pattern that provides guidance to participants in regards to implementing information assurance capabilities, e.g., PKI.
<b>CTISS List (Exchange Protocols &amp; Services)</b>	T	A categorized list of standards that apply to the various components of the ISE EAF, categorized by technology area.
<b>ISE Technical Partition to FEA TRM Map</b>	T	A mapping of ISE Technology Patterns and Standards to the FEA TRM.

<sup>80</sup> B/T refers to whether the product is used in the baseline or target view.

## 7.2 Technical Reference Model Mapping

The FEA Technical Reference Model (TRM) provides three-level taxonomy. Using this taxonomy as a basis, the ISE Technical Partition is organized as shown in Figure 7-1.



**Figure 7-1. 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, and
- 4) Service Interface and Integration.

Each service area has 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 the figure for further reference.

The ISE 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 participating agencies for integration with the ISE. Several



examples include web browser, wireless, mobile, and voice. The ISE Technical Partition will also include technologies required by the ISE currently not inserted in the TRM. Table 7-2 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 7-2. Technical Reference Model Mapping**

Service Area	Service Category	Standard or Technology	Section # Herein
1	A	Authentication Single Sign-on	7.7
1	B	Collaboration	7.5
1	D	Transport	7.6
2	A	Database	7.5
2	A	Storage Devices	7.5
2	B	Network Devices/Standards	7.6
2	B	Servers/Computers	7.6
2	B	WAN/LAN	7.6
2	D	Platform Dependent	7.4
2	D	Platform Independent	7.4
2	E	Portal	7.5
3	A	Platform Independent	7.4
3	A	Platform Dependent	7.4
3	C	Certificate/Digital Signature	7.7
3	C	Security Services	7.7
3	D	Data Exchange	7.4
3	E	Database Connectivity	7.4
4	A	Database Access	7.5
4	A	Middleware	7.4
4	B	Service Discovery	7.4
4	B	Service Description/Interface	7.4
4	C	Data Transformation	7.4
4	C	Data Format/Classification	7.4

For example with SAR and an ISE participant's Shared Space, related standards or technologies might include database, storage devices, network devices/standards, platform independent, servers, computers, security services, database connectivity, and database access.

### 7.3 Common Terrorism Information Sharing Standards

The ISE Technology Partition will also leverage common standards defined by the CTISS to supplement those found in the FEA TRM.<sup>81</sup> The CTISS effort is defining the standards categories, standards defining bodies, core standards, and business process-driven functional standards to establish an integrated, nationwide enterprise of information sharing organizations and resources.

The PM-ISE chartered the ISE CTISS Working Group, with membership from ISC member organizations, to:

- 1) Identify categories of the CTISS based on relevant authorities.
- 2) Develop the baseline CTISS.
- 3) Identify ongoing common standards efforts related to information sharing.
- 4) Initiate interconnections and alignment to these ongoing efforts.
- 5) Identify and suggest appropriate next steps to implement the baseline CTISS.

The CTISS Working Group, in collaboration with the Information Sharing Council (ISC), developed the CTISS Version 2 document<sup>82</sup> to assist Federal, and SLT governments in addressing key challenges for terrorism information sharing and standardization of processes and products across the ISE community.

The CTISS baseline issuance document addresses items 1 and 2 above, as shown in Figure 7-2. The CTISS Working Group identified general categories, a set of standards bodies, and a baseline set of core standards.

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;

---

<sup>81</sup> Office of the PM-ISE, *Information Sharing Environment Implementation Plan*, Ibid., Section 6.3.

<sup>82</sup> Office of the PM-ISE, *ISE Common Terrorism Information Sharing Standards (CTISS, Version 2.0)*, Ibid.

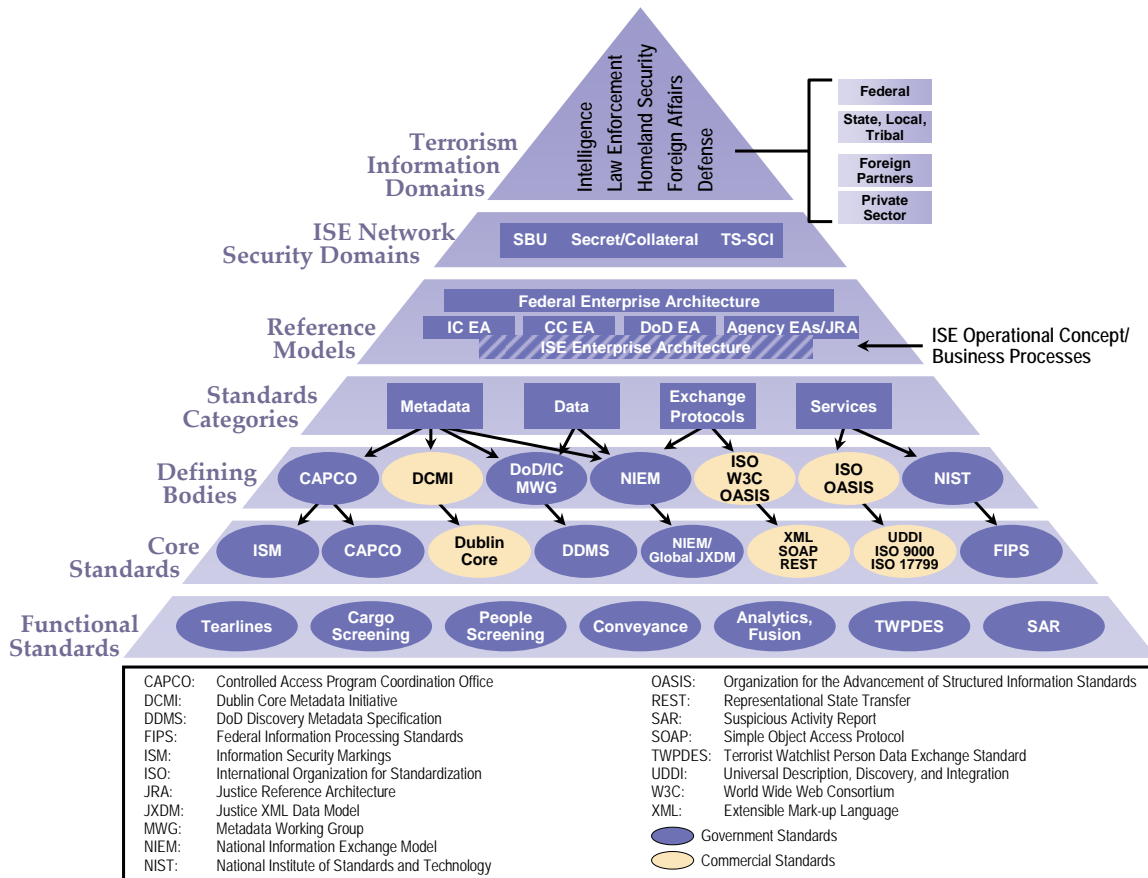


Figure 7-2. CTISS Framework

- 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 standards should provide necessary guidance for access controls;
- Standardizing SBU definitions across the ISE should be included in future standards implementation activity; and
- User training (initial and ongoing) should be provided to support a successful implementation of standards.

The CTISS Working Group introduced a standards governance and management process for use across all levels of government (Federal, SLT), and among all communities of interest (law enforcement, homeland security, intelligence, defense, and foreign affairs). The standards process supports the essential activities of acquiring,

accessing, producing, retaining, and sharing terrorism information. The ISE EAF will adopt all CTISS common standards. For example, in the case of the SAR mission process, a CTISS functional standard will be developed to support the exchange of SAR information across the ISE.

## 7.4 Service-Based Architecture

Information sharing in the ISE should be enabled by implementing a service-based architecture. Participants should develop services that facilitate exposure of terrorism information to other ISE participants. Participants will update business processes and supporting applications to leverage services offered by other ISE participants. The ISE will provide the infrastructure and Core Services required to support service-based architecture.

Service-based architecture is a business-driven approach to software architecture that supports integration of business processes as a set of linked, repeatable activities, or 'services'. It provides the necessary orchestration and exposure of distributed capabilities to service consumers independent of the controlling ownership domains and service providers. A high-level model of service-based architecture is illustrated in Figure 7-3.

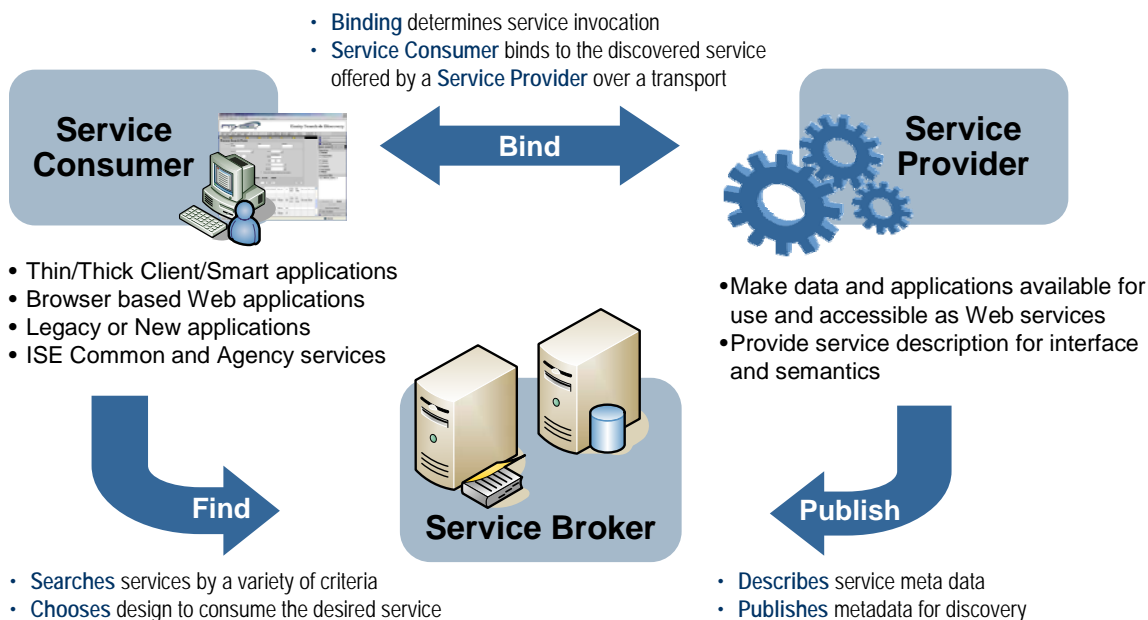


Figure 7-3. Service-Based Architecture

Services are self-contained, reusable software modules with well-defined interfaces. They are independent of applications and the computing platforms on which they run. Service-based architecture enables development of composite applications that integrate functionality from multiple sources to support horizontal business processes.

A service-based architecture allows an organization to decompose its business activities to a level of granularity that each service encapsulates a single activity independent of all others. As illustrated above in Figure 7-3, a service-based architecture includes “Service Providers” and “Service Consumers.” Service Providers publish interfaces to their capabilities via a “Service Broker.” Published services are now available for Service Consumers to search, discover and access using the Service Broker. Although not required, it is preferred that services be packaged as a set of services.

A service-based architecture can be viewed from either a micro or macro perspective. The micro view shows development of granular services on a small scale approaching business processes that are easily encapsulated in a service gradually evolving to more complex services. The macro view defines services as the representation of a unit of work within the enterprise. It is a representation of the processes required to address a business problem. Often it is more practical to implement services at the micro level rather than tackle the task of moving an entire enterprise to a service-based architecture.

Services are based on open standards, which provide interoperability without requiring prior knowledge of the underlying development platform or technology stack. This quality provides the technology-agnostic characteristics required for successful implementation of a service-based architecture.

In the ISE, participants defined as service providers should expose data in legacy databases through publication of information access services. The data should be tagged with metadata making it understandable, searchable, and accessible based on common characteristics across the ISE. Data meta-tags will also include data classification to control access, ensure security, and protect privacy. For SAR, metadata tags will delineate summary (excluding privacy protected information) and detailed (includes all data) SAR records, and required data elements necessary for impacting other ISE business processes.

Due to the many benefits that service-based architectures can provide, the ISE will encourage use to the maximal extent. Primary benefits of service-based architecture include the following:

- **Reusability:** A service-based architecture promotes reuse of capabilities or services reducing redundancy. This enables participants to avoid duplications, creating single services shared across multiple applications. This translates into cost savings for participants.
- **Interoperability:** A service-based architecture is built upon industry recognized “open standards”. This ensures interoperability will be achieved and results in effective sharing of resources and data assets among participants.
- **Loose Coupling:** In a service-based architecture, a service provider defines and publishes its service. This allows a service provider to mask its implementation and

platform details from service consumers. A service provider has great flexibility in terms of choosing platforms and technologies for implementing its services, as well as minimizing the impact of changes to its service implementation, as long as the service interface remains the same. This “loose coupling” between a provider and a consumer offers implementation and platform flexibility.

- **Business Agility:** Organizations can rapidly deploy new or modified business processes to achieve new functionality easily since services are built as reusable, loosely-coupled modules. This ability offers businesses greater agility to rapidly identify new capabilities and leverage them in innovative ways.

## 7.5 Enterprise Application Integration

Enterprise Application Integration (EAI) “is a business computing term for the plans, methods, and tools aimed at modernizing, consolidating, and coordinating the computer applications in an enterprise. Typically, an enterprise has existing legacy applications and databases and wants to continue to use them while adding or migrating to a new set of applications that exploit the Internet, e-commerce, extranet, and other new technologies. EAI may involve developing a new total view of an enterprise’s business and its applications, seeing how existing applications fit into the new view, and then devising ways to efficiently reuse what already exists while adding new applications and data.”<sup>83</sup> With respect to the ISE, EAI refers to the strategy and methodology to leverage legacy agency applications and business models in the ISE and its associated service-based architecture. The ISE EAF uses enterprise integration (EI) patterns based on the Enterprise Integration Patterns Symbology as introduced by Gregor Hohpe and Bobby Woolf to describe EAI.<sup>84</sup> For a more detailed example of this approach refer to Appendix G.

EI patterns represent industry best-practices for describing reusable designs. They are proven methods to encapsulate subject matter expertise where a simple “one size fits all” solution does not exist. Each pattern poses a specific design problem, discusses the considerations surrounding the problem, and presents a solution that balances various drivers. Typically, a pattern represents a solution that has evolved through use over time; therefore providing technical guidance and instruction for addressing similar scenarios.

EI patterns are relatively small design products which address specific problems encountered during systems integration. This approach limits the scope of problems encountered during integration of systems to more manageable units. The use of patterns is well suited to the ISE, which relies on ISE participant organizations to build the application components that implement the architecture. The patterns provide guidance to participants when designing approaches to implement common components, such as a service.

---

<sup>83</sup> Found at SearchWebServices.com, Definitions: EAI.  
([http://searchwebservices.techtarget.com/sDefinition/0,,sid26\\_gci213523,00.html](http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci213523,00.html), 10 October 2006).

<sup>84</sup> Hohpe, Gregor and Bobby Woolf, *Enterprise Integration Patterns* (Addison-Wesley, ISBN: 0321200683, 2004).

EI patterns do not replace standards; they supplement them. They provide guidance to applying selected standards, which are in compliance with the ISE common standards, when building capability within the ISE. For example, a service pattern may provide detailed guidance to apply relevant IA standards when invoked.

The following references were used to help identify patterns relevant to the ISE:

- Integration Patterns and Practices;<sup>85</sup>
- Enterprise Integration Patterns;<sup>86</sup> and
- The technology patterns developed by the Homeland Security (HLS) Enterprise Architecture<sup>87</sup> team.

EAI patterns can be broadly classified into two categories:

1.	Data Integration Patterns	<ul style="list-style-type: none"> <li>• Shared Database</li> <li>• Data Replication</li> <li>• Data Warehousing<sup>88</sup></li> </ul>		
2.	Function Integration Patterns	<table style="width: 100%; border: none;"> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li>• Service-Oriented Integration</li> <li>• Message Broker</li> <li>• Message Bus</li> <li>• Collaboration</li> <li>• Federated Search— ISE Participant Perspective</li> </ul> </td> <td style="vertical-align: top; padding-left: 20px;"> <ul style="list-style-type: none"> <li>• Federated Search— ISE Agency Perspective</li> <li>• Workflow/Process Integration</li> <li>• ISE Portal Integration</li> <li>• Publish/Subscribe Events to ISE</li> </ul> </td> </tr> </table>	<ul style="list-style-type: none"> <li>• Service-Oriented Integration</li> <li>• Message Broker</li> <li>• Message Bus</li> <li>• Collaboration</li> <li>• Federated Search— ISE Participant Perspective</li> </ul>	<ul style="list-style-type: none"> <li>• Federated Search— ISE Agency Perspective</li> <li>• Workflow/Process Integration</li> <li>• ISE Portal Integration</li> <li>• Publish/Subscribe Events to ISE</li> </ul>
<ul style="list-style-type: none"> <li>• Service-Oriented Integration</li> <li>• Message Broker</li> <li>• Message Bus</li> <li>• Collaboration</li> <li>• Federated Search— ISE Participant Perspective</li> </ul>	<ul style="list-style-type: none"> <li>• Federated Search— ISE Agency Perspective</li> <li>• Workflow/Process Integration</li> <li>• ISE Portal Integration</li> <li>• Publish/Subscribe Events to ISE</li> </ul>			

### 7.5.1 Data Integration Patterns

Data integration patterns are used to connect applications on a logical level by establishing an accessible single source of data available to multiple integrating applications. The ISE will be built using a service-based architecture approach to share terrorism information. However, individual ISE participants may have existing enterprise architectures that do not adhere to service-based architecture principles. The data assets of these organizations should be integrated in the data layer using Data Integration Patterns as described in Table 7-3.

<sup>85</sup> Microsoft, *Integration Patterns (Patterns and Practices)* (Microsoft Press, ISBN: 073561850X, 6 October 2004).

<sup>86</sup> Hohpe, Gregor and Bobby Woolf, *Enterprise Integration Patterns* (Addison-Wesley, ISBN: 0321200683, 2004).

<sup>87</sup> Department of Homeland Security, *DHS Enterprise Architecture Technical Reference Model, Appendix O* (DTCGHS-03-A-FLC035-001-0009A, 29 August 2003).

<sup>88</sup> Data Warehousing is used for predetermined information sharing functionality in the ISE only.

**Table 7-3. Data Integration Patterns**

Pattern	Description
<b>Shared Database</b>	A mission-critical information system can be integrated with the ISE by sharing the database. The Shared Database Pattern offers a mechanism for multiple applications to share information stored in one physical database. There are a variety of issues to consider with this pattern, such as maintaining data integrity and application. Knowing those issues prior to designing a shared database is a great improvement to overall information system acquisition.
<b>Data Replication</b>	A Data Replication Pattern is an alternate approach to achieve Data Integration in scenarios where sharing the database may not be a viable option. Original data can be replicated for integration using standard data replication techniques or by employing a Data Warehouse Pattern.
<b>Data Warehousing</b>	A Data Warehouse is a repository approach for an ISE participant's data where information assets are stored and managed. A participant can share its data assets to the ISE via its Data Warehouse. This pattern addresses how a Data Warehouse can be used for integration within ISE.

ISE participants should expose data via services to the ISE allowing participating organizations database access. The ISE will maintain databases and associated storage devices to support directory services and other ISE Core Services. However, shared data assets should be supported by database and stored on devices owned and operated by the participating organizations.

## 7.5.2 Function Integration Patterns

Service-based integration patterns consist of two low-level patterns, Message Broker and Message Bus, as well as numerous high-level function patterns specifically associated with the ISE. A description of the initial set of patterns is presented in Table 7-4. Additional patterns will be identified as the ISE evolves.

**Table 7-4. Function Integration Patterns**

Pattern	Description
<b>Service-Oriented Integration</b>	Since the ISE will be a service-based architecture, patterns based on a service-based integration are a primary focus. Service-based integration enables systems to consume and provide services.
<b>Message Broker</b>	A message broker pattern is derived from the broker pattern which is commonly used in application and integration design. Conceptually, a broker pattern decouples source systems from target systems such that source systems do not require routing information related to the location of target systems. The message broker pattern performs these communications between source and target systems via messages. This pattern can be employed for the ISE Services Registry, where the Registry acts as a broker between a consumer and provider.



Pattern	Description
<b>Message Bus</b>	A message bus pattern provides a framework for a common communication mechanism which integrates multiple systems via messages. It also enables separate applications to work together in a decoupled fashion such that new applications can be added or removed without affecting others. The message bus pattern is typically associated with a publish/subscribe pattern.
<b>Collaboration</b>	There is a need to facilitate information sharing between multiple geographically disparate ISE participants. The collaboration pattern addresses the issues related to bringing distributed users together by facilitating interaction and communication. The capabilities offered by the collaboration pattern include instant messaging, on-line chat sessions, white boarding, etc.
<b>Federated Search – ISE Agency Perspective</b>	The federated search pattern from an ISE participant’s perspective involves all the interactions that occur when a federated query is issued by a participant, including issuing queries to all relevant agency data sources, applying data filters, gathering filtered data, and finally presenting result sets to the user.
<b>Federated Search – ISE Participant Perspective</b>	The federated search pattern from the ISE participant perspective addresses how an organization can participate in a federated search capability by allowing its data sources to be queried and indexed.
<b>Workflow/ Process Integration</b>	The workflow/process integration pattern focuses on the orchestration of interactions between multiple systems. To coordinate the execution of long running business processes that may span multiple applications, this pattern employs a process manager that tracks the state of each individual step and provides a mechanism for centralized reporting and management of activities.
<b>ISE Portal Integration</b>	The ISE consists of a variety of users with specific roles and privileges to a variety of applications and services. To improve productivity and eliminate user training every time a new system is deployed, the ISE portal integration pattern offers a way to provide a unified and consistent view by integrating applications and services and offering a “one-stop-shop” concept for ISE participants.
<b>Publishing a Service to the ISE</b>	This pattern builds on the service-based integration pattern and addresses how a service can be published to the ISE.
<b>Publish or Subscribe Events to ISE</b>	As an example, the publish/subscribe pattern addresses how an ISE participant can broadcast an event to all interested receivers. This pattern can be adopted for alert and notification services.

### 7.5.3 Example Pattern: Publishing a Service to ISE

An illustrative example of the notation used to graphically represent an EI pattern is shown in Figure 7-4. The figure depicts the Publishing of a service to the ISE Pattern.

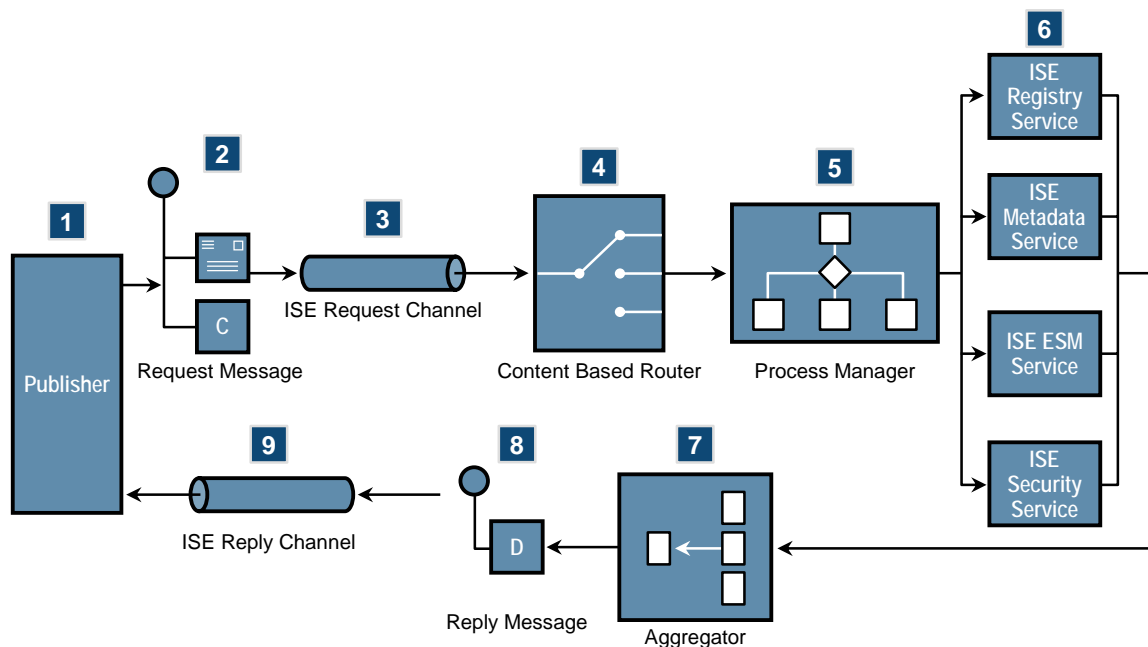


Figure 7-4. Example Pattern: Publishing a Service to the ISE<sup>89</sup>

The following steps briefly describe the sequence of steps illustrated in the figure above. A detailed explanation of this example pattern can be found in Appendix G.

A *publisher* packages all relevant information required to publish a service to the ISE.

A *Request Message* is formed invoking a method.

The request message is routed to a *Process Manager*, which handles all logic associated with publishing the service. The intermediate processing steps can be spread across different systems. In this scenario, the process manager handles all interactions with registry services such as *ISE Service Registry* interface, *ISE Metadata Service* interface, *ISE ESM Service* interface, and *ISE Security Service* interface.

Based on the results of these intermediate processing steps, a *Reply Message* is formed and sent back to the publisher to notify the status of the original request.

## 7.6 Transport

The ISE Core component of the ISE EAF includes the physical and logical connection of ISE participants and centers, referred to as the ISE Transport, so that electronic communications, including data, video, graphics, and voice, can be used to share and collaborate with investigators, analysts, responders, operators, and decision makers. It also includes the software/hardware/network infrastructure required to implement a

<sup>89</sup> Derived from Hohpe, Gregor and Bobby Woolf, *Enterprise Integration Patterns* (Addison-Wesley, ISBN: 0321200683, 2004).

service-based architecture. The connection should use existing networks and systems that are Internet Protocol (IP) compatible while providing the degree of information security and privacy required for the information being shared.

Requirements that (1) direct the NCTC to be a focal point for aggregating terrorism information and (2) direct the sharing of information among Federal agencies, State, local, and tribal entities, the private sector, and with foreign partners require a means of connectivity among all these entities. Requirements that indicate a net-centric, distributed model require an approach that leaves no single point of failure among transport nodes on the network.

The business activities of the transport capability are to connect the users and ensure the quality, delivery, and security of the information is maintained. Although quality and security are overlapping activities, quality must address the network performance required by the application while security must address the prevention/mitigation of attacks to the underlying network and content of the transmitted information.

Figure 7-5 illustrates 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 “Agency ISE Shared Space”. The external ISE includes the ISE Core and the ISE Shared Spaces of all other participating organizations. For SAR, shared spaces are defined as where SAR data records would be deposited for access by ISE participants.

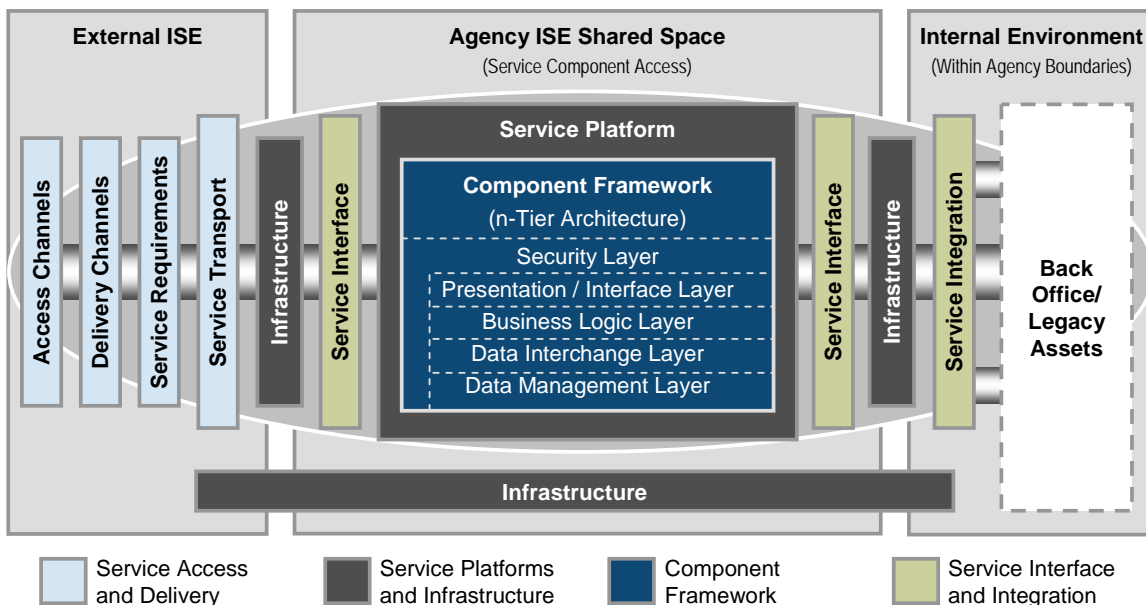


Figure 7-5. Typical Agency Connection to the ISE

An organization/center could have up to three instances of this model: one for each security domain (TS/SCI, Secret/Collateral, and SBU) signifying that even organizations with multiple internal networks will only have a single connection to the ISE transport carrying data from all three security domains. ISE participants leverage three internal networks representing the TS/SCI, Secret/Collateral, and SBU security domains. Each network is attached to an ISE Shared Space for external filtered communication to expose terrorism information for sharing from information related to other missions. The “external” area is represented by an existing, external WAN operating at the appropriate classification level. Both the internal networks and their associated ISE Shared Spaces are protected commensurate with the level of information transported, stored, and processed on that network and are approved for operation through the appropriate certification and accreditation process. Each ISE Shared Space contains a switch that manages LAN connections within the shared space that connects to the participant’s/center’s internal network through another firewall.

## **7.7 Information Assurance**

### **7.7.1 Information Assurance Overview**

Information Assurance (IA) for the ISE relies on overarching governance and risk management processes based on an IA model encompassing six IA Categories, the four partitions of the ISE Architect’s view, and IA controls and countermeasures.

#### **7.7.1.1 Governance and Risk Management**

The governance and risk management processes for the ISE are critical to establishing and maintaining effective IA for the ISE. The artifacts of governance arrangements and activities are policies, rules, guidelines, recommendations for changing laws, and decision making that impact all aspects of the ISE, including establishing and maintaining a known and acceptable level of risk for the ISE. IA is a key capability in the ISE to support business process-driven exchanges, such as SAR, where data elements may include those of a sensitive nature (such as privacy protected information) 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); and
- Determining whether residual risk is acceptable or additional protective measures are required.

By progressing through this process, a risk decision should be made by the appropriate governance bodies and accrediting authorities for the ISE to ensure a known and acceptable level of risk (not risk avoidance) is considered 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.

A more detailed discussion of governance and risk management is outside the scope of this chapter but is included here due to its crucial impact on the IA approach for the ISE.

### 7.7.1.2 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 7-6<sup>90</sup>. Descriptions of the elements of the IA dimensions follow.

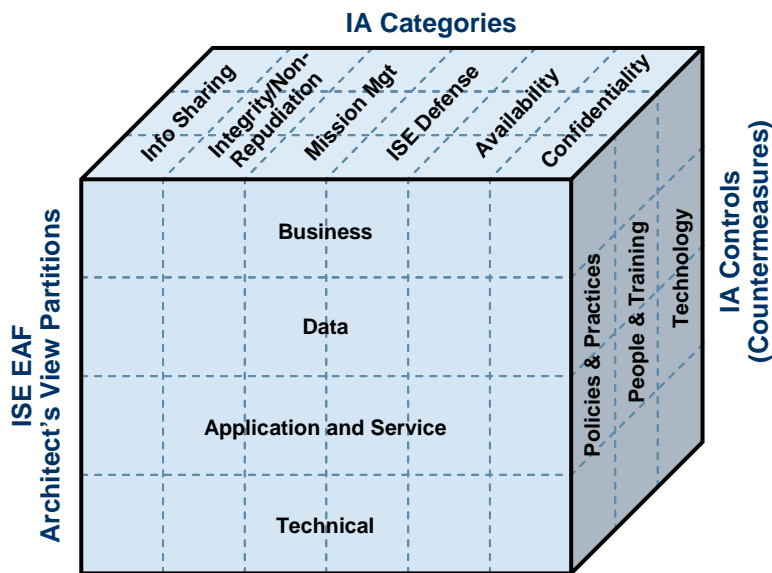


Figure 7-6. IA Model<sup>91</sup>

<sup>90</sup> Office of the PM-ISE, *ISE Information Assurance Model and Common IT Security Framework*, Draft Version 0.6 (August 2007).

<sup>91</sup> This IA Model represents an initial approach to align information assurance concepts and capabilities with the ISE EAF partitions. This model may continue to evolve during the development of the FEA-ISE Profile and will be presented in greater detail, including its application, in the Profile and future versions of the ISE EAF.

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, Defend the ISE, Assured Availability, and Assured Confidentiality;
- Demonstrates relationships to the four partitions of the ISE EAF Architect's View; and
- Includes categories of IA Controls that address policies and practices, people and training, technology, and standards.

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

### 7.7.2 Information Assurance Categories<sup>92</sup>

Table 7-5 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 ISE issuances.

**Table 7-5. IA Categories**

IA Category	Description
<b>Assured Information Sharing</b>	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.
<b>Assured Integrity/Non-Repudiation</b>	The ISE must assure the integrity/non-repudiation of data, at rest, during processing, in transit, and across systems during normal, degraded, and disconnected operating modes, and in low bandwidth environments. This requirement refers primarily to measures that ensure data is not inadvertently or maliciously modified.
<b>Assured Mission Management</b>	The ISE must provide the ability to assign, prioritize, modify, and revoke user and system roles, access rights, and COI membership.
<b>Defend the ISE</b>	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).

<sup>92</sup> 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).

IA Category	Description
<b>Assured Availability</b>	The ISE must assure a level of availability consistent with stated requirements.
<b>Assured Confidentiality</b>	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, he or she cannot leverage that access to view ISE information.

Security mechanisms, tools, practices, policies, management processes, ISE Core Services, and features of service-based architecture combine to provide information assurance in each of these categories. The following sections describe several security approaches used in each IA category.

### 7.7.2.1 Assured Information Sharing

**Security Domains:** The ISE has three security domains:

- 1) Top Secret/Sensitive Compartmented Information;
- 2) Secret/Collateral; and
- 3) 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 SBU domains. The three security domains should provide assured information sharing within a security domain.

**Cross-Domain Solutions:** The ISE vision to make terrorism information available, accessible, and useable by all ISE participants and centers is complicated due to 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 between 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 participants.** Information exchanged from one security domain to another should occur internally therefore placing responsibility on the 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 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 do not currently exist.

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

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

**Authentication and Authorization:** Robust authentication and authorization, in addition to supporting the “Assured Integrity and Non-Repudiation” and “Defend the ISE” IA Categories below, are key capabilities required to support assured information sharing.

#### 7.7.2.2 Assured Integrity and Non-Repudiation

**Authentication:** The ISE must take measures to ensure only authorized users can access ISE resources. These measures include assuring that a prospective user is who he or she says he or she is, and assuring that the user is authorized for access to the ISE. Exclusively allowing authorized users to access the data on the ISE will help to assure that data is not subject to unauthorized modification. Authentication should be accomplished using certificates and digital signatures through a PKI.



**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 taken 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:** The ISE should employ one or more PKIs. It is desirable that there be one PKI across all three ISE 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.

### 7.7.2.3 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.

### 7.7.2.4 Defend the ISE

**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 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 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 only perform those functions permitted by their identity and role. Not only must a user be authenticated to the ISE, but 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 to defend the ISE.

**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.

#### 7.7.2.5 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, providing and maintaining accessibility to required information in any environment (stable to austere), and providing 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 patch management; monitoring the status of ISE assets; and detecting, diagnosing, responding, and correcting problems.

#### 7.7.2.6 Assured Confidentiality and Privacy

**Encrypted Communications:** All communications leaving an enclave at any security domain level should be encrypted. This 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.<sup>93</sup>

---

<sup>93</sup> 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>.

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

### 7.7.3 Four Partitions of the ISE Architect's View

The IA model for the ISE identifies IA implications for the overall ISE as well as within each of the four partitions of the ISE Architect's view. Figure 7-7 provides a graphical representation of the method used to analyze IA implications and needs in each of these partition areas.

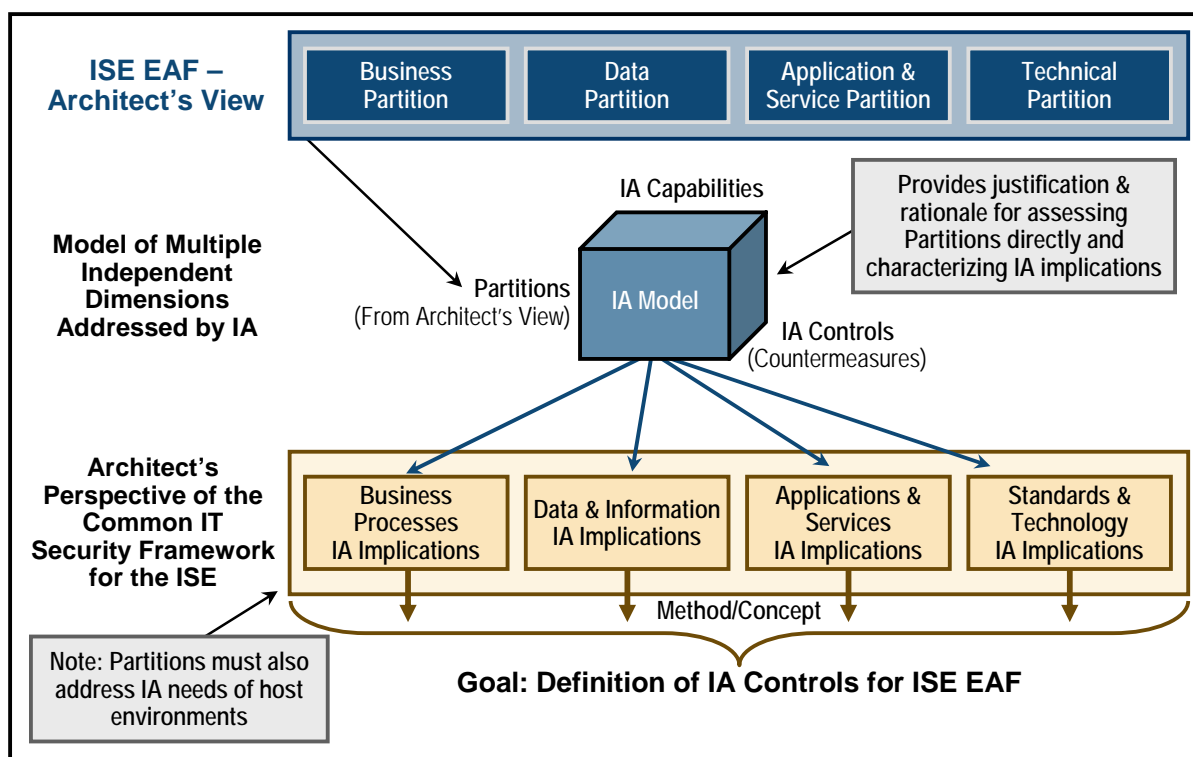


Figure 7-7. IA Relative to Four Partitions of the ISE Architect's View

### 7.7.4 IA Controls and Countermeasures

The selection and integration of IA controls for the ISE are based on IA controls in NIST standards and guidelines, specifically NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* and FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. Use of FIPS 199 and NIST Special Publication 800-53 is mandated for all Federal non-National Security Systems. DoD, DNI, CDMO and other organizations are transforming the certification and accreditation (C&A) process for National Security Systems (NSS) by creating a common catalog of security controls using NIST 800-53 as a starting point and incorporating unique controls required from DoDI 8500.2 and DCID 6/3. The benefit of using the FIPS 199 and NIST 800-53 approach is the security categorization of systems

can be determined and compared based on an applied set of common security controls. The ability to compare the security controls applied to different systems will significantly facilitate establishing a model for trust that enables information sharing.

The *IA Controls and Countermeasures* dimension of the IA Model is commonly grouped into three focus areas:

- People and Training;
- Policy and Practices (or Operations); *and*
- Technology.

The People and Training focus area includes education and training, experience, professional development and certification, recruiting and retention, personnel security, and leadership. The Policy and Practices (or Operations) focus area includes policies (program, issue-specific, and system-specific), management, monitoring and administration, governance, intelligence/threat analysis, incident handling and response, certification and accreditation, and all other policies and processes that support assuring the ISE. Technology focus area includes tools, products, and technical approaches (such as identification and authentication mechanisms, access controls, cryptography, etc., as well as non-IT measures, such as physical locks and barriers). Controls within each must reinforce the others to provide a comprehensive set of controls to enforce information assurance and minimize risks to the ISE.

## 7.8 Standards

The ISE EAF begins with the CTISS framework (Figure 7-2) categories of Metadata, Data, Exchange Protocols, and Services. It further breaks these into subcategories as shown in Table 7-6. Table 7-6 below lists the standards subcategories with example technical standards in each section under consideration. Definition and formal selection of technical and functional standards will be through the governance processes identified in the CTISS baseline program issuance.

**Table 7-6. ISE Technical Standards Under Consideration**

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 Markings (IC ISM), ISO 11179
		Information Exchange	NIEM, GJXDM, TWPDES, OMG Standards
Data		Encoding and Formats	ASCII, audio/video/data storage standards, NIEM IEPD, DoD/IC U-Core, Unicode
Exchange Protocols		Application	SNMP, FTP, DNS
		Presentation	SSL, XDR, XHTML
		Session	ISCSI, RPC, SQL
		Transport	TCP, UDP
		Network	IPv6, ARP, BGP, ICMP
		Data Link	Ethernet, PPP, SLIP
		Physical	SONET, ISDN, CAT-5
Services	IA Services	Confidentiality	FIPS 140, FIPS 197
		Integrity/Non-Repudiation	FIPS 180-2, FIPS 186-2
		Assured Information Sharing	XACML, SAML
		Highly Available Enterprise	DODI 8500.2, NCID T400
		Network Defense	DCID 6/3, DODI 5299.40
		Management and Infrastructure	PKI v1.5, X.509, XKMS
	Service Based Architecture Foundation Services	Core XML	XML, XSD, XSLT, XPath
		Invocation	SOAP, 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	HTML, JSR-168, WSRP, AJAX

The **Metadata** section of the standards categories addresses various standards required to share terrorism information such as:

- **Controlled Vocabulary** – a consistent way to represent a collection of terms. It addresses standards for representing metadata such as DDMS, Dublin Core, and includes standards for representing common data such as FIPS codes for zip codes, country names, etc.
- **Information Exchange** – represents standard formats for exchanging information across the ISE. It includes various information exchange standards such as NIEM, DoD/IC U-Core, etc.

The **Data** section of the standards categories addresses various data standards required to share terrorism information such as:

- **Encoding and Formats** – represents various data format, storage, document standards.
- The **Exchange Protocols** section of the standards categories addresses standards and protocols to provide ISE transport infrastructure and standard protocols for use among the agencies, State and major urban area fusion centers, and the NCTC for interoperability. It is derived from the Internet Protocol suite that was developed to support the Internet. The categories most relevant to ISE transport are:
  - **Transport** – this category manages connections and provides reliable packet delivery. It operates in units of messages.
  - **Network** – this category addresses and routes datagrams. It performs fragmentation and reassembly. It operates in units of packets.
  - **Link** – provides hardware addressing and error detection/correction. It operates in units of frames.
  - **Physical** – this category addresses connection through electrical and wiring specifications. It operates in units of bits.

The **IA Services** standards subcategory addresses numerous existing and new standards in the areas of information system security. Most of these standards are intended to address security issues via encryption and policies. The IA subcategories align directly with the IA categories described in Section 7.7.2.

The **Service-Based Architecture Foundation Services** section of the standards categories addresses standards needed to provide the service-based architecture framework. The services taxonomy of ISE is derived by leveraging the services categories published in the DoD Web Services Profile Issue Paper of the NCIDS Services Segment S100 Document and the standard service Protocol Stack. Each layer addresses specific aspects of the services architecture. It should be noted that the technologies, concepts, and specifications are relatively more mature in the areas of Core XML and certain lower layers of the stack, such as those related to Description,

than other standards at the top. The following taxonomy of Service-Based Architecture Foundation Services standards is adopted by the ISE:

- **Core XML** – this includes all the standards such as XML, XML InfoSet, XML Namespaces, XML Schema, etc., which provide a foundation upon which service-based architecture is built.
- **Invocation** – this includes standards such as REST and SOAP, which are mechanisms to invoke a delivered capability.
- **Metadata Management** – includes all the standards related to Description (such as WSDL), Discovery (such as UDDI, ebXML, etc.), Addressing (WS-Addressing), Policy (WS-Policy), and Metadata Exchange (WS-MetadataExchange) of services.
- **Messaging** – includes standards related to Notifications, Eventing, Alerting, with standards such as WS-Eventing, WS-Notification, etc.
- **Composable Service Elements** – handles Security, Reliable Messaging, and Transactionality of Services. This includes standards such as WS-Security, XACML, WS-Reliability, WS-Transactions, etc.
- **Process Orchestration** – handles the dynamic flow of business logic between agencies. It includes standards such as BPEL4WS.
- **Management** – addresses service management via standards such as WS-Manageability and WS-Provisioning.
- **Presentation** – handles the user interface standards of services and includes standards such as WSRP and JSR 168 for developing interoperable, reusable portlets.

## 7.9 Technical Partition Transition Strategy

The Technical Partition transition from the baseline (AS-IS) to the target (TO-BE) takes place as the ISE Core and ISE agency capabilities are implemented. As components are developed, they leverage the technologies and standards identified in the Technical Partition. This should occur as an inherent part of the capability implementation, requiring no special planning or projects. In some cases, a specific effort must be made solely to implement the required technology or standard. A non-ISE example of this is the current cross-agency initiative to move all Federal agencies from the IPv4 network protocol standard to IPv6.

The Technical Partition is an open-ended framework that will be extended incrementally over time. Additional standards will be added as a result of the work of the CTISS Working Group. Additional patterns will be added as necessary and useful to guide agencies in participating in the ISE.

This page intentionally blank.



## Chapter 8 – Implementer’s View

The Implementer’s View consists of the components shown in Figure 8-1. This view takes the results of the ISE Architect’s View and organizes them into a model to guide organizations participating in the ISE.

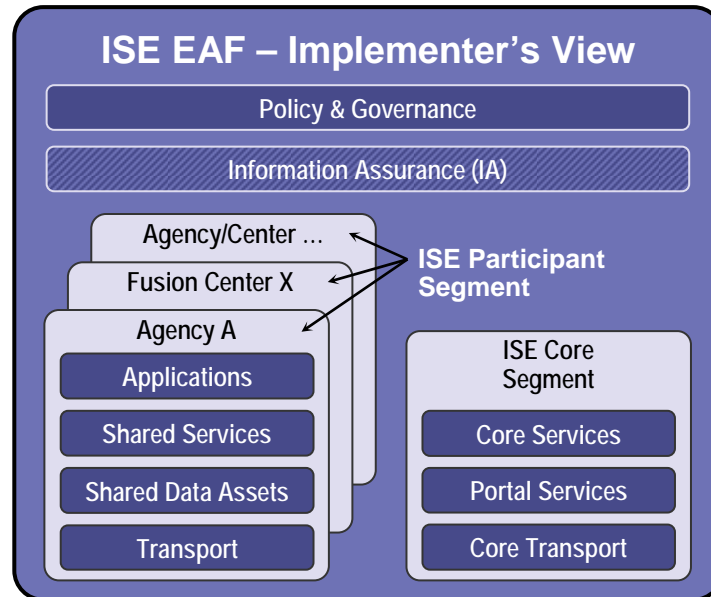


Figure 8-1. ISE Enterprise Architecture Framework: Implementer’s View

There are two main segments shown in this view: ISE Core Segment and ISE Participant Segment.

The **ISE Core** Segment provides Core Services, Portal Services, and Core Transport functions to all agencies that participate in the ISE.

- Core Services are those services required to provide a service-based architecture and are used by nearly all ISE participants.
- Portal Services support the ISE Portal and ISE Management Portal functions and provide additional services (e.g., publish/subscribe, collaboration, etc.) through a user interface.
- Core Transport includes the hardware, software, and transport media that support transmission and reception of message traffic within and across the ISE.

As explained earlier, 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 IT Implementation Agents to provide these capabilities to all the ISE participants.

The **ISE Participant** Segment shown on the left in Figure 8-1 (Agency A, Fusion Center X, Agency/Center...) represents the components managed by a participant or fusion center that use or provide information via the ISE.

- Within an organization, Applications developed provide capabilities to address the counterterrorism mission. These applications may incorporate information and services provided by other participants through the ISE.
- Shared Services are those provided by a specific participant. These services typically provide other participants with access to data or capabilities “owned” by that organization.
- Shared Data Assets are those information assets shared by participants via the ISE. In the case of SAR this is where data is deposited.
- Agency Transport includes the hardware, software, and transport media that support transmission and reception of message traffic from participant systems to the ISE Core Transport Component.

These components, taken together, provide the building blocks for each organization to participate in the ISE.

**Policy and Governance** and **Information Assurance** span both the ISE Participant 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. **Information Assurance** manages accessibility while safeguarding information. IA also protects sources and methods of collection from unauthorized use or disclosure.

The *FEA-ISE Profile* document provides guidance for organizations participating in the ISE, and discusses the components of the Implementer’s View in more detail.

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>

