COMMON TERRORISM INFORMATION SHARING STANDARDS (CTISS) PROGRAM MANUAL, VERSION 1.0

Prepared by the
Program Manager, Information Sharing Environment (PM-ISE)

This page intentionally blank.

TABLE OF CONTENTS

LIST OF FIGURES

This page intentionally blank.

SECTION I – PURPOSE

This reference manual for the CTISS program is a companion document to the PM-ISE issuance Information Sharing Environment (ISE) Administrative Memoranda (ISE-AM) number 300 (*Common Terrorism Information Sharing Standards (CTISS) Program*). It is intended to provide further clarification and guidance on the implementation of the CTISS program in the ISE. This manual identifies the two categories of standards under CTISS, functional standards and technical standards, and presents a relational, hierarchical framework for the CTISS that provides defining structure and interfaces necessary for CTISS development and implementation. This manual also introduces a construct for CTISS implementation, administration, and management practices across the entire ISE.

SECTION II – DEFINITIONS AND ASSUMPTIONS

The December 2005 Presidential Memorandum for the Heads of Executive Departments and Agencies states, "The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information."[1] Federal information resource policy similarly states that agencies will conduct information management planning using "voluntary standards and Federal Information Processing Standards where appropriate or required."[2] Standards affecting national security systems funded through the National Intelligence Program (NIP) will be coordinated through the Office of the Director of National Intelligence (ODNI) and the Committee on National Security Systems (CNSS), and standards affecting systems funded through the Military Intelligence Program (MIP) will be coordinated through the Office of the Secretary of Defense. Standards affecting the National Communications System (NCS) will be coordinated through the NCS Manager and the NCS Committee of Principals (COP).

Responsive to national and executive branch policies, the ISE will be formed using standard interfaces and processes that align major standards defining bodies supporting the Federal, State, local, and tribal governments; the private sector; and foreign partners as appropriate. Standards have an important role for ensuring consistency of business processes, information flows, information exchanges, and infrastructure development, and they are key decision-making factors when considering future information resource architectures and investments. Functional standards and technical standards constitute the two categories of common standards under the CTISS program (Figure 1). ISE *Functional Standards* constitute detailed mission descriptions, data and metadata on focused areas that use ISE business processes and information flows to share information. ISE *Technical Standards* identify specific technical methods and techniques to implement information sharing capability into ISE

[1] White House, *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 2.

[2] Office of Management and Budget, *Circular A-130*, (OMB: Washington, DC, 2005), section 8(a)(1)(h).

affiliated systems. Conceptually, CTISS provides a standards process foundation that can be implemented across all levels of Government (Federal, State, local, and tribal) and among all applicable communities (e.g., law enforcement, homeland security, intelligence, defense, and foreign affairs). CTISS supports the essential activities of acquiring, accessing, producing, retaining, protecting, and sharing terrorism information consistent with Presidential Guideline 1[3].

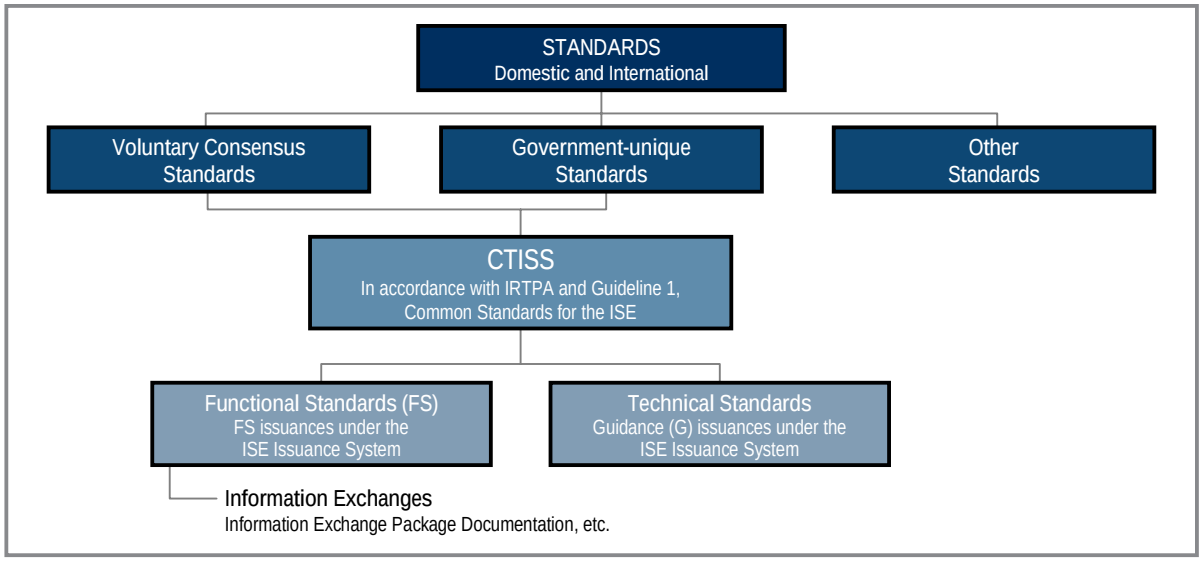


Figure 1. Taxonomy of the CTISS

As developed by the CTISS Working Group in May 2006, the CTISS program is founded on the following assumptions:

- ISE common standards should not be classified national security information;
- ISE common standards must be considered throughout all phases of the intelligence cycle[4];
- The common standards implementation approach should support the development or leveraging of existing standards to enable information sharing consistent with applicable Public Laws, executive orders, and other policies;
- Structured and unstructured information sharing standards apply to data, documentation, related business processes, information flows, and respective production methods;
- The CTISS should not be precluded from supporting the sharing of other information types (i.e., beyond terrorism information such as emergency response);
- Standards improvement should be considered a continuous process;

[3] White House, Ibid., section 2.
[4] The intelligence cycle, defined for the U.S. Intelligence Community, includes five major activities: planning and direction, collection, processing, analysis and production, and dissemination.

- Metadata, essentially data about data, is a key information sharing enabler for ensuring that terrorism information is understandable, searchable, and accessible based on common characteristics across the ISE;
- Metadata tags provide accuracy and relevancy indicators of the information;
- Extensible Mark-up Language (XML) is the chosen markup language to facilitate information sharing within the ISE;
- ISE common standards must provide the necessary guidance for access controls;
- Standardizing Sensitive But Unclassified (SBU) definitions across the ISE will be part of the standards implementation activity consistent with Presidential Guideline 3 implementation; and
- User training (initial and ongoing) is critical to successful implementation of the CTISS.

While Federal law promotes the use of voluntary consensus standards, terrorism information sharing business process requirements present new and unique challenges that may require a combination of both Government-unique standards and voluntary consensus standards. Regardless of whether Government-unique or voluntary consensus standards are used for the ISE, the development, selection, and use will be in accordance with joint and open processes and forums that include representatives from all five ISE communities.

SECTION III – CTISS AND ISE ARCHITECTURE

Standards are key decision-making factors when aligning and modifying architectures, investments, and information sharing processes. Five strategic goals guide the CTISS program:

1. Establish a self-governing, institutionalized standards adoption process across Federal, State, local, and tribal governments with common standards that guide counterterrorism information exchange related business processes and investments

2. Engage foreign and private sector partners to promote the ISE

3. Leverage published, voluntary consensus technical standards when appropriate and available

4. Select and implement performance-driven standards

5. Ensure standards are compliant with public law, Executive Orders, and other policies

Figure 2 depicts the conceptual ISE implementation approach for addressing disparate Enterprise Architecture (EA) interfaces among different ISE participants in the community. The ISE promotes common services and a core transport to interface with EAs using the CTISS and the ISE Enterprise Architecture Framework (ISE EAF). Initially with legacy systems, interfaces may require translation devices to interconnect disparate systems using mediation services that enable interconnectivity. However, to effectively share information across organization boundaries for the long-term, common semantic understandings of the data and the business processes or services used by participants in the ISE must be established. Additional necessary requirements are common understanding and semantic consistency in the structure of the data that is to be successfully shared and a measure of consistency in the manner in which the information is captured, stored, and exchanged. This process must also include measurable performance indicators on the effective outcomes of information sharing using the CTISS. A common standards framework, the *CTISS Framework*, provides a common lexicon for defining, structuring, and guiding existing and future information resource planning and investment acquisition processes to meet these requirements.

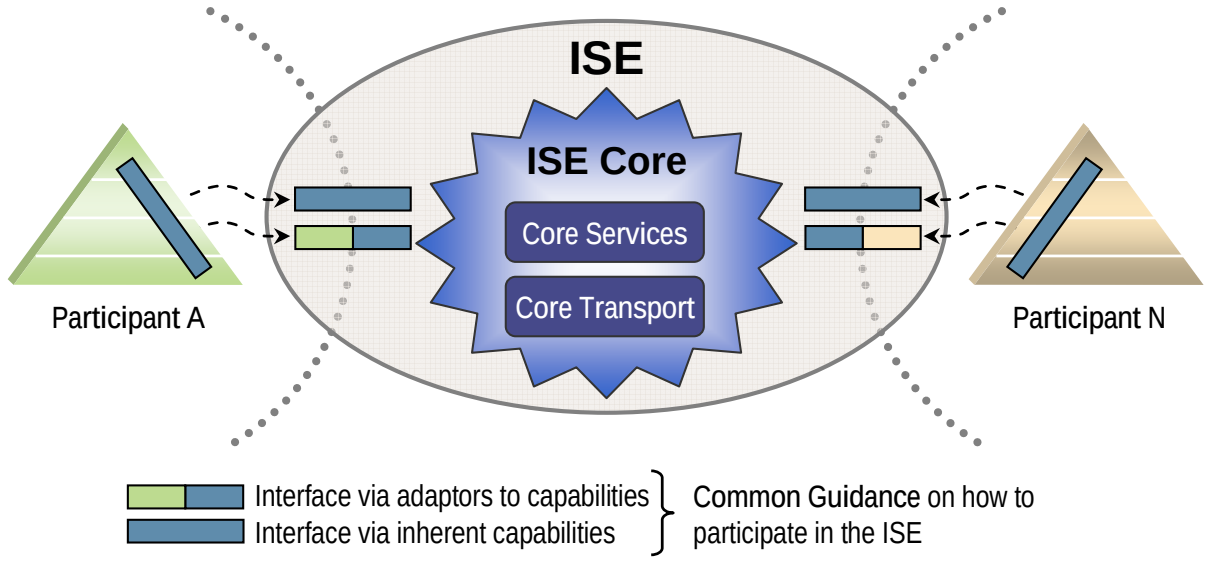


Figure 2. ISE Implementation Approach

SECTION IV – THE CTISS FRAMEWORK

The CTISS Framework provides a relational, hierarchical mapping and programmatic structure that identifies standards types, standards defining bodies and core standards for leveraged use across the ISE community. As depicted in Figure 3, the highest level of the Framework identifies the terrorism information domains, or affected interest areas, influenced by standards for information sharing: intelligence, law enforcement, homeland security, foreign affairs, and defense.[5]

[5] The five annotated terrorism information domains depicted in Figure 3 correspond to the five ISE communities.

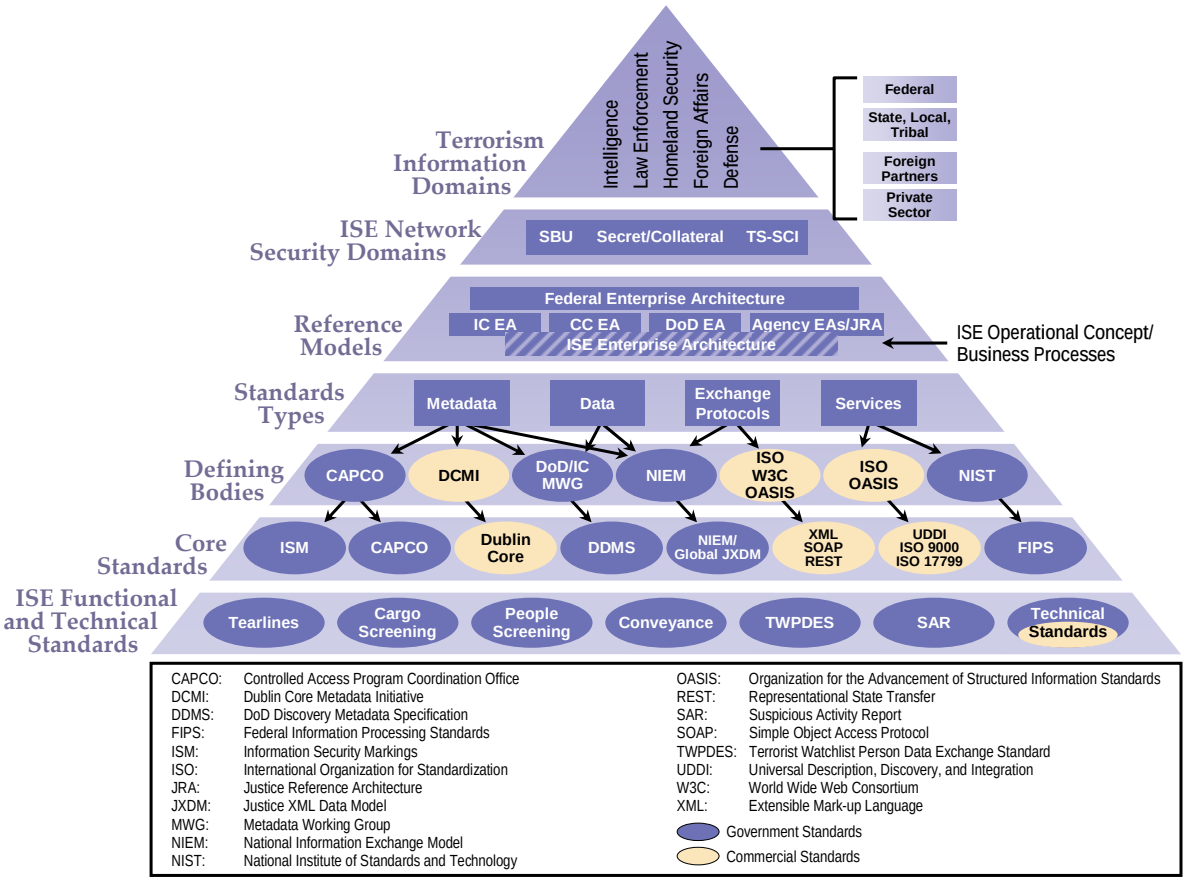


Figure 3. CTISS Framework

Each information domain spans all levels of the Government including Federal, State, local, and tribal governments as well as foreign partners and the private sector. Consistent with the ISE Implementation Plan[6], security domains affecting ISE supporting networks also span the Framework with three broad domains addressed for information sharing (Sensitive but Unclassified {SBU}, Secret, and Top Secret/Sensitive Compartmented Information {SCI})[7]. From an information resource architecture perspective, the Federal Enterprise Architecture (FEA) and the ISE EAF, an architectural subset of the FEA, serve as universal reference models spanning the entire Framework, integrating information sharing capability in the Intelligence Community EA (ICEA), the Department of Defense EA (DODEA), the Continuity

[6] The ISE Implementation Plan may be found at www.ise.gov.

[7] For the purposes of this document, consistent with 50 U.S.C. Sec. 435a, SCI is defined as the "classification for information in such material concerning or derived from intelligence sources, methods, or analytical processes that requires such information to be handled within formal access control systems." TOP SECRET, defined in Executive Order 13292 (Classified National Security Information) is "information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe." SECRET, defined in Executive Order 13292 is "information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe." SBU is described in detail in the current Presidential Guideline 3 Report currently under White House review.

Communications EA (CCEA), and other agency EAs[8]. The ISE operating concept provides the ISE business process definitions, information flows, and requirements inputs into the ISE EAF development.

With the context established for standards usage, the standards types (*Metadata, Data, Exchange Protocols, and Services*), the next level in Figure 3, provide key differentiations for existing or newly developed standards in the ISE. Metadata describes those standards providing the searchable *characteristics* of terrorism information (data descriptors about actual data). A library card catalog is a familiar example of a metadata resource used for searching and locating a single book within a vast collection of books. The Data standards type focuses on the actual information *content* to be shared. For example, this content may include standards describing units of measurement or observation, the particular data medium (e.g., electromagnetic signals versus photographic, data elements in a SAR report, or data character encoding formats [e.g., American Standard Code for Information Interchange {ASCII}, plain text, etc.]).

The Exchange Protocols standards type addresses *the way* the information is to be shared across systems and networks. For example, this sharing may include network protocol standards (such as those supporting Internet communications in the Open Systems Interconnection {OSI} model), network security, or computer database standards. Finally, the Services standards type describes the uniform *business processes, information exchanges, common services, and activities* supporting information sharing. Examples of the processes described by Services standards may include quality management, records management, accreditation activities, information security, privacy, and data search service routines.

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

[8] These EAs also include the Justice Reference Architecture, considered a potential model for developing those enterprise architectures at State and major urban-area fusion centers.

SECTION V – STANDARDS TYPES

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

- ***Metadata Standards[9]:*** Metadata is structured, encoded data that provide *nomenclature and characteristics* of information-bearing elements aiding in the identification, discovery, sorting, understanding, and management of described information— essentially data about data. Search engines use metadata to find and describe matching information sources. With respect to the ISE handling of terrorism information, both machine and records management functions are necessary, and as such, metadata standards will address information applicable to both functions. An example of a CTISS Metadata type is the *tearline standard* used for differentiating and distributing intelligence information with varying levels of security classifications. A tearline report is an area in an ISE-shared intelligence report in which a sanitized version of a more highly classified or controlled report is located, allowing wider dissemination of information. Tearlines of lower classification contain the substance of the more detailed information without identifying the actual producer of the product or revealing sensitive sources and methods. Metadata provides differentiating labels, or tags, that help manage, sort, and distribute this information and are particularly useful for protection of Personally Identifiable Information (PII). Metadata provide the primary information exchange standardization content for Functional Standards under CTISS.
- ***Data Standards:*** Data standards help identify the fundamental building blocks for *defining, formatting, and exchanging* actual terrorism information. Data standards are applicable to a wide range of elements to include raw collected data, messages, and published documents and records. In general, CTISS data standards for Federal Government agencies and departments must map to components of the Federal Enterprise Architecture (FEA), such as the Data Reference Model and the ISE EAF. An example of a broad data standard is the Global Justice XML Data Model (GJXDM), the precursor to the National Information Exchange Model (NIEM), and a common language used to describe, structure, and share criminal justice and homeland security data. Another example is the DOD/IC U-CORE with data application support for the defense and intelligence communities. Data standards provide the primary information exchange standardization content for Functional Standards under CTISS.
- ***Exchange Protocols Standards:*** Exchange Protocols standards, predominantly technical in nature, address the rules that influence *system-to-system communications;* these may include syntax, sequencing, and formatting guidelines for the systems affected. A core Exchange Protocol standard for the CTISS is the Extensible Markup Language (XML)[10]. XML is a general-purpose markup computer language used for creating special purpose markup languages capable

[9] Metadata is described at the DCMI website: http://dublincore.org.
[10] XML is described at http://www.w3.org/XML/.

of describing many different kinds of data. Markup languages are formal annotation approaches to documents or collections of digital data that aid in identifying structure and content of representative data elements. This annotation may also aid computers with processing and displaying information. The primary purpose of XML is to facilitate the sharing of data across different systems, particularly systems connected via Internet Protocol (IP) networks. Exchange protocols provide the primary technical standardization content for Technical Standards under CTISS.

- ***Services Standards:*** Services standards describe the *business processes and system servicing routines* supporting those common activities used for discovering, identifying, distributing, protecting, and managing terrorism information. These standards may also describe new information sharing services for incorporation into agency service-based architectures and integrate with other organizational business processes. Universal Description, Discovery, and Integration (UDDI) is an example of a Services standard that supports information search capability on the Internet using distributed operator sites as servicing entities.[11] Another example is the International Organization for Standardization (ISO) standards series 9000 used for outlining quality management business processes in organizations. These service standards provide the primary information exchange standardization content for Functional Standards, but they may describe technology-related services that support the ISE and are published as Technical Standards under CTISS.

SECTION VI – STANDARDS DEFINING BODIES

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

The following listing of standards defining bodies is merely representative for leveraging in the CTISS program and does not encompass all standards bodies existing across the public and private sectors.

A Standards Defining Bodies for Metadata

1 Controlled Access Program Coordination Office (CAPCO)

Director of Central Intelligence Directive (DCID) 3/29, now DCID 6/11, originally established the CAPCO. Currently CAPCO is part of the DNI Special Security Center. The Controlled Access Program Oversight Committee (CAPOC) is responsible for

[11] The UDDI website is at http://uddi.org.

policy, oversight, and reporting for all compartmented intelligence programs, and the CAPCO functions as the staff element for the CAPOC. CAPCO primary areas of responsibility include coordinating the controlled access program and releasing community security classification markings standards. The CAPCO leads the Community Markings Implementation Working Group and maintains the Markings Implementation Manual and the IC Register of Authorized Markings, more commonly referred to as the CAPCO Register.

2 Dublin Core Metadata Initiative (DCMI)[12]

The DCMI is an international organization dedicated to promoting the widespread adoption of interoperable metadata standards and developing specialized metadata vocabularies for describing resources that enable more intelligent *information discovery* systems. DCMI promotes an open forum engaged in the development of interoperable online metadata standards that support a broad range of purposes and business models. The DCMI provides simple standards to facilitate the finding, sharing, and management of information.

The DCMI is independent, not controlled by special interests, and is not biased toward specific domains or technical solutions. DCMI encourages participation from organizations anywhere in the world and promotes consensus building among participating organizations. DCMI outreach activities include consensus-driven working groups, global conferences, and workshops. The U.S. is represented in the DCMI by organizations such as the U.S. Library of Congress and the National Science Foundation. The National Science Foundation is an independent U.S. agency responsible for promoting science to benefit national prosperity, welfare, and national defense.[13]

3 DOD/IC Metadata Working Group

The DOD/IC Metadata Working Group (MWG) includes representation from Department of Defense (DOD) and Intelligence Community (IC) components as well as other organizations to which it has ties. MWG products include policy recommendations, specifications related to information sharing, coordinated metadata engineering actions, and specific metadata artifacts that are published and managed collectively. The MWG is a parent organization to numerous focus groups that act on and provide guidance with respect to DOD and IC data/metadata management needs. The base technology for data standardization under the MWG, to include the Metadata Registry (MDR), is XML.

[12] The DCMI website is at http://dublincore.org.
[13] The National Science Foundation website is at http://www.nsf.gov.

4 National Information Exchange Model (NIEM)[14]

To identify and facilitate information exchanges between agencies, the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) launched NIEM through a partnership agreement between their Chief Information Officers (CIOs) on February 28, 2005. NIEM is designed to develop, disseminate, and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in both emergency and routine situations. NIEM provides a set of common standards to facilitate timely, secure information sharing across the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprises. NIEM includes a governance structure of committees and councils working with logical entities, attributes, and relationships to develop standards describing data shared across multiple business domains of Federal, State, and local agencies.

B Standards Defining Bodies for Data

1 NIEM

The base technology for data standardization used in the NIEM is an XML-based framework and support infrastructure. NIEM representatives provide technical assistance and training to local, State, tribal, and Federal organizations seeking to implement NIEM information exchanges (identified as Information Exchange Package Documents).

2 DOD/IC Metadata Working Group (MWG)

The base technology used for data standardization under the MWG includes XML and Universal Core (U-CORE) elements, part of a joint standards program consisting of information on the nature, the location, and the timeframe of information exchanges that support the defense and intelligence communities.

C Standards Defining Bodies for Exchange Protocols

1 NIEM

As with data standards, the base technology for exchange protocols standardization used in the NIEM is XML. NIEM provides a set of services and products needed to effectively build and implement information exchanges. NIEM tailors products consistent with open exchange protocols standards to ensure interconnectivity and information sharing across multiple communities of interest (COIs).

[14] The NIEM website is http://www.niem.gov.

2 International Organization for Standardization (ISO)[15]

The ISO is a non-governmental organization of national standards institutes from 156 countries on the basis of one member per country. The Central Secretariat, which has overall responsibility for coordinating the international standards system, is located in Geneva, Switzerland. The ISO acts as a bridging organization for consensus on solutions that meet both the requirements of business and the broader needs of the international society, such as the needs of worldwide stakeholder groups, consumers, and users.

ISO standards describe state-of-the-art products, services, materials, and systems. The ISO identifies the international standards required for business, government, and society; develops them in partnership with the sectors that will implement them; and adopts these standards by transparent procedures based on national input. The official U.S. representative to the ISO is the American National Standards Institute (ANSI), a private, non-profit organization.

3 World Wide Web Consortium (W3C)[16]

The W3C is an international consortium in which member organizations, a full-time staff, and the general public work together to develop standards for the Web. The W3C develops interoperable specifications, guidelines, software, and tools to lead the Web to its full communications potential. The W3C primarily pursues its mission through the creation of Web standards and guidelines, engages in education and outreach, develops software, and serves as an open forum for discussion about the Web. By publishing open, non-proprietary standards for Web languages and protocols, W3C seeks to avoid market fragmentation and Web fragmentation. Major U.S. corporations, universities, and the National Institute of Standards and Technology (NIST) are members of the W3C. NIST is a non-regulatory Federal agency within the U.S. Commerce Department that works with industry to develop and apply technology, measurements, and standards.[17]

4 Organization for the Advancement of Structured Information Standards (OASIS)[18]

OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. OASIS, which produces more Web services standards than any other organization, generates standards for security, e-business, and public sector application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organizations and 100 countries. OASIS is distinguished by its transparent governance and operating procedures.

[15] The ISO website is at http://www.iso.org.
[16] The W3C website is at http://www.w3.org.
[17] The NIST website is at http://www.nist.gov.
[18] The OASIS website is at http://www.oasis-open.org/home/index.php.

Members set the OASIS technical agenda using a collaborative process expressly designed to promote industry consensus and unite disparate efforts. Completed work is ratified by open ballot, and governance is accountable and unrestricted. Major U.S. corporations, NIST, and the Department of Defense are members of OASIS.

D Standards Defining Bodies for Services

1 ISO

ISO promotes the widespread adoption of international standards in support of products and services development. Services that apply compatible technology based on common standards enhance interoperability and facilitate information sharing. Examples of widely used standards that may be applied to services standards include identification card management, information security, language code identification, and other associated management systems.

2 OASIS

OASIS develops standards through technical committees. Committees that are working on applicable services standards include computing management, e-Commerce, law and government, security, Service Oriented Architecture (SOA), Web services, and XML processing.

3 NIST

NIST is a non-regulatory Federal agency within the U.S. Commerce Department that works with industry to develop and apply technology, measurements, and standards.[19]

SECTION VII – CORE STANDARDS

Core standards serve as broad standardization resources for developing the CTISS. The actual development of business process-driven functional standards and technical standards in the CTISS will leverage attributes of these various core standards from the associated standards defining bodies. While not addressing all detailed operational aspects of information sharing products, information flows, and processes, the following core standards address those broad process and technical areas that must be addressed across the ISE. These core standards represent those necessary for leveraging in the CTISS and are not representative of all core standards used across the international, public, and private sectors.

[19] The NIST website is at http://www.nist.gov.

A Metadata Standards

1 Information Security Markings (ISM)

The ISM consists of a set of descriptors that may be used to associate security-related metadata with XML elements in documents, Web-service transactions, or data streams. The primary focus of the ISM is providing an implementation-independent definition of the data elements used for XML implementations with information of various security classifications. The ISM consists of a vocabulary of agreed-upon data elements that were developed to support use of the CAPCO guidelines for security markings and are intended to provide a standard set of data elements for incorporating classification and controls metadata into data sets. Users of the ISM may develop specific (but separate) programming interfaces to implement their required business process rules around this model. The ISM Data Element Dictionary (DED) provides the name, semantics, data type, data representation, domain value set, and permissible values for each of the ISM data elements. The DED provides definitions for the data elements that specify the information needed to generate security markings such as portion marks, banners, classification authority, and declassification information.

2 Extended Dublin Core

The Extended Dublin Core Metadata Element Set is a standard for cross-domain information resource descriptions and consists of logical elements of information about digital or non-digital assets that have been made available as shared resources. The purpose of the resource metadata standard is to provide a framework for enhancing discovery and exchange of information.

Owners of information domains with defined standards map the corresponding data elements to the metadata elements. In some cases the elements will align one-to-one with defined physical data elements in structured data sets, image libraries, or textual publications. In other cases, the standard logical elements will be manifested by complex information structures. By requiring all domains to map to the resource metadata elements, the potential for interoperable systems will be enhanced substantially.

3 Department of Defense Metadata Specification (DDMS)[20]

The DoD Discovery Metadata Specification (DDMS) defines discovery metadata elements for resources posted to the ISE. The DDMS specifies a set of information fields that are to be used to describe any data or service asset that is made known to the enterprise, and it serves as a reference for developers, architects, and engineers by laying a foundation for discovery services. The DDMS will be employed consistently across disciplines, domains, and data formats.

[20] DDMS documentation may be found at https://metadata.dod.mil/mdrPortal/apmanager/mdr/mdr.

DDMS elements provide the basis for organizations to begin planning, transitioning, and implementing metadata tagging initiatives that support the goal of increased data visibility and discovery. The DDMS defines a core set of elements that must be used to describe data assets made visible to the enterprise. Users (human and systems) that search the enterprise will discover data assets that have been tagged and entered into catalogs or repositories that respond to search queries specified in terms of DDMS entries. The DDMS elements are designed to be platform, language, and implementation independent. Accordingly, system designers and engineers can decide on ways to generate and store the discovery metadata information elements, providing flexibility for system developers to generate and retain discovery metadata using any approach, including COTS products.

4 NIEM

NIEM provides XML-based standards that include a data dictionary and XML schema. NIEM was originally designed for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to effectively share data and information; however, its functionality has expanded to homeland security applications. Through the use of a common vocabulary that is understood, system-to-system, NIEM enables information sharing access from multiple sources for use in multiple applications.

B Data Standards

1 NIEM

A NIEM Information Exchange Package (IEP) represents a set of standardized data that is transmitted for a specific business process purpose. The IEP is an instance of an XML document that delivers the payload or information. NIEM Information Exchange Package Documentation (IEPD) is a collection of artifacts that describe the structure and content of an IEP. It does not specify other interface layers (such as Web services). For the CTISS, the IEP format is readily used for developing business process-driven functional standards in the CTISS and is harmonized and aligned with data elements from the DOD/IC U-Core. The IEPDs will also provide XML schema and examples of machine understandable semantics.

2 DOD/IC U-CORE

The DOD/IC U-CORE was developed jointly by the DoD and the 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.

C Exchange Protocols Standards

Exchange protocols standards address those necessary standards for supporting the Application and Service and Technical Partition of the ISE EAF.[21] These technical standards include those necessary to enable such services as transport, collaboration, reporting, enterprise management, storage, messaging, and information assurance.

1 Extensible Markup Language (XML)[22]

The XML is a W3C-recommended general-purpose markup language for creating special purpose markup languages capable of describing many different kinds of data. The primary purpose of XML is to facilitate the sharing of data across disparate systems, particularly systems connected via the Internet. Languages based on XML are defined in a formal way, allowing programs to modify and validate documents in these languages without prior knowledge of their form.

2 SOAP[23]

SOAP is an XML-based protocol standard used between messaging systems. It provides a framework for particular message content, ways to process messages, encoding rules, and conventions for remote procedure message calls and responses. SOAP is well suited for decentralized, distributed applications in which systems exchange structured information. Specifically, SOAP messages include certain components: an envelope defining the content of the message, intended recipients, and processing guidelines; and encoding rules for defining data-types.

3 Representational State Transfer (REST)[24]

REST is a style of software architecture. It prescribes the use of standards for resource representation and for resource types; it has applicability to systems on the World Wide Web and networks, and is also associated with capability for accessing website information using XML-based files that describe the site content.

D Services Standards Protocols

1 Universal Description, Discovery, and Integration (UDDI)[25]

The UDDI, approved by OASIS in 2005, provides the protocols necessary for implementing an information search capability on the Internet using distributed operator

[21] This ISE EAF may be located at the PM-ISE website, www.ise.gov.
[22] XML is described at http://www.w3.org/XML/.
[23] SOAP is described at http://www.w3.org/TR/.
[24] Roy Thomas Fielding, "Architectural Styles and the Design of Network-based Software Architectures," found at http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm
[25] UDDI is described at http://www.uddi.org/.

sites as servicing entities. UDDI provides a standardized capability for locating, identifying, and transposing network-based software into services applicable for agency service-based architectures. The capability of UDDI aids software developers and network architects to work collaboratively in realizing search service capability across agency architectures. UDDI is a background capability that allows software to find other software. Major uses of UDDI result in hard coding of service information.

2 ISO 9000 Series[26]

ISO 9000 Series standards are widely known international business process standards used as references for business-to-business quality management activities. These standards address quality requirements for deliveries to customers, applications of pertinent regulatory requirements, and continued process improvement actions for quality management. Quality management business processes are critical aspects of information sharing activities to help ensure the integrity, accuracy, and relevancy of terrorism information shared across ISE organizations.

ISO 17799

ISO 17799 (Information technology—security techniques—code of practice for information security management) is an international standard from the ISO used in the CTISS for information security and assurance.

3 Federal Information Processing Standards (FIPS)

The E-Government Act of 2002 (Public Law 107-347), passed by the 107th Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), tasked the NIST with developing information security standards and guidelines to be used by Federal agencies for the protection of Federal information systems and the information processed, stored, and transmitted by those systems.

CTISS standards for information security and assurance, consistent with FISMA requirements, include NIST security standards and guidelines. These standards and guidelines, designated as Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs), include FIPS Publication 199 (*Standards for Security Categorization of Federal Information and Information Systems*) and FIPS Publication 200 (*Minimum Security Requirements for Federal Information and Information Systems*) and Special Publication 800-53 (*Recommended Security Controls for Federal Information Systems*). A Risk Management Framework (RMF), developed by NIST as part of the FISMA Implementation Project, integrates the FIPS and supports Special Publications into the System Development Life Cycle (SDLC), which promotes cost-

[26] ISO 9000 is described at http://www.iso.org.

effective, risk-based enterprise information security programs for Federal agencies and Federal contractors.

NIST standards and guidelines provide a common framework and understanding for expressing security that promotes effective management and oversight of information security programs, including the coordination of information security efforts through the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

SECTION VIII – CTISS IMPLEMENTATION, ADMINISTRATION, AND MANAGEMENT

The ISE is envisioned to create a powerful national capability to share, search, and analyze terrorism information across jurisdictional boundaries and provide a distributed, protected, and trusted environment for transforming data into actionable information. The resulting environment will also recognize and leverage the vital roles played by State and major urban area fusion centers, which represent crucial investments toward improving the Nation's counterterrorism capacity.[27] The ISE must be multipurpose and flexible and provide the fundamental information sharing functionality and services needed for counterterrorism missions while protecting privacy and civil liberties.

Federal departments and agencies, using their respective lines of authority, have initiated information sharing segment architectures, standards, and governance mechanisms that can be directly leveraged as support structures to begin implementing attributes of the CTISS program. The CTISS provides major components to the ISE EAF and, more specifically, in the Data, Application and Service, and Technical Partitions of the EAF. The CTISS focus, driven by business processes derived from ISE operating concepts, is to further expand the sharing capability of terrorism information across the Federal Government into functional and integrated support areas. The CTISS also expands the information sharing capability among Federal, State, local, and tribal governments and private sector entities and foreign partners.

As depicted in Figure 4, introduction of the CTISS into Federal agencies and their processes will follow two implementation paths. The *investment-driven path* will target new system investments (i.e., systems whose design is not finalized) or any system undergoing development, modernization, and enhancement (DME). Applicable standards will be published at the time of system design, or CTISS implementations that meet the mission and functional needs of these affected systems will be scheduled. Timelines for implementation will be synchronized to fiscal year programming and budgeting cycles. The CTISS process will introduce functional standards and technical standards that are compatible for integration between both civil and national security

[27] PM-ISE, *ISE Implementation Plan*, (Washington, DC: 2006), xiv.

system architectures. In general, standards affecting architectures *not* designated as national security systems will be coordinated through existing OMB processes. Standards affecting national security systems funded through the National Intelligence Program will be coordinated through the Office of the DNI/CIO, and standards affecting systems funded through the Military Intelligence Program will be coordinated through the Office of the Secretary of Defense/CIO.

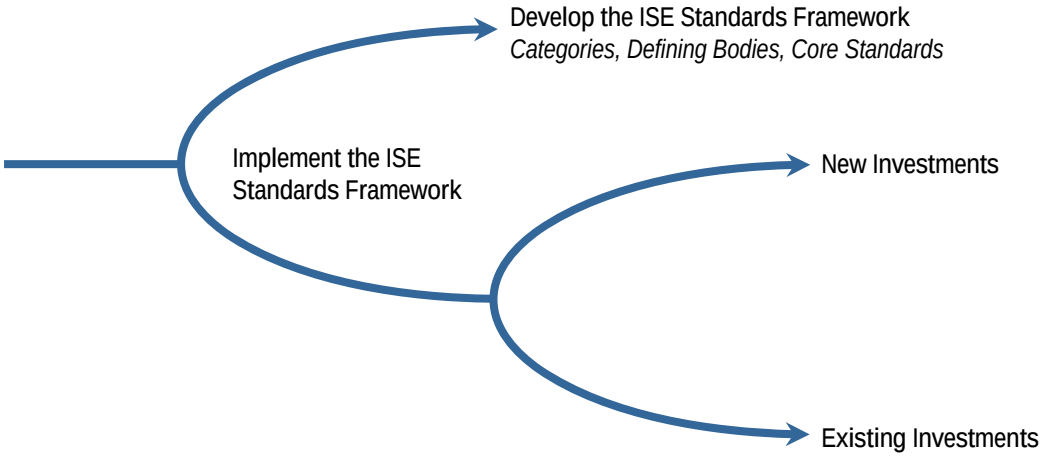


Figure 4. Standards Implementation

The second implementation path, *priority-driven*, targets standards affecting existing investments for those critical business processes and information flows along functional areas requiring adoption within a near-term, fixed time period, potentially without immediate identified funding. For these standards, the PM-ISE and the ISC will set identified priorities and work with agencies to review cost impacts on existing and planned investments, documenting these potential impacts during standards selection and/or development. Participants should review functional standards and technical standards that are priority driven for implementation, assessing operational and programmatic impacts weighed with the overall benefits for improving national information sharing. Participants should also identify impacts as early as possible to determine feasible implementation strategies that will help minimize those impacts yet promote the necessary incorporation of new standards needed in these critical areas.

Information sharing standards for non-Federal government participants will be published as recommendations from the PM-ISE, through the Offices of the Secretary of Homeland Security and the Attorney General, for use by State, local, and tribal (SLT) governments, law enforcement agencies, and the private sector. As the ISE continues to evolve, organizations not in standards compliance may find it increasingly difficult to connect to the ISE and exchange information. However, since these standards are being developed in collaboration with the National Information Exchange Model (NIEM), a joint Federal, State, local, tribal, and private sector standards group co-sponsored by the DHS and the DOJ, standards consideration and adoption actions will reach a wide distribution of SLT and private sector organizations. State and major urban area fusion centers will be central to implementation at the State and local levels, and these fusion

centers will be advised to follow the CTISS recommendations and provide necessary translations to external systems, such as at local levels, not yet compliant with the CTISS.

The CTISS development and implementation process will be conducted by agencies consistent with the OMB-mandated universal framework for modeling the Federal IT Enterprise, the Federal Enterprise Architecture (FEA)[28]. New standards supporting information sharing will be incorporated into the Technical and Data Reference Models with standards compliance verified through the *Federal Transition Framework Catalog* and the *FEA Program: Enterprise Architecture Assessment Framework*. The PM-ISE expects that the CTISS will begin to be incorporated into fiscal year 2009 investment planning, with full standards incorporation into investments beginning in fiscal year 2010. The PM-ISE will work with the ODNI, the DOD, the National Command and Coordination Capability (NCCC), the National Communications System (NCS), the Committee on National Security Systems (CNSS), and the DHS overall on implementing CTISS into those terrorism information sharing investments affecting national security systems. The CTISS managed through the FEA and national security system architectures will broaden agency capabilities to operate more efficiently and effectively in sharing terrorism information across the communities of the ISE.

A sound administrative structure is essential to ensure that CTISS activities are carried out and that appropriate mid-course corrections can be made. The existing ISE administrative structure, shown in Figure 5, is based on the principle that ISE issues should be resolved at the lowest organizational level wherever possible, but that, when necessary, an organized process is in place to elevate these issues for resolution, up to and including the Cabinet level and the President.

As detailed in Chapter 4 of the ISE Implementation Plan, in consultation with the ISC, the PM-ISE is responsible for planning for, overseeing the implementation of, and managing the ISE, including monitoring and assessing progress with the CTISS. The ISC is integral to the success of the ISE—assisting and advising the President and the PM-ISE on establishing, implementing, and maintaining the environment and ensuring coordination among Federal departments and agencies participating in the ISE. Through this interaction, the PM-ISE attempts to secure agreement and establish common understanding among ISE participants, referring any unresolved issues to the ISC for collaborative resolution. If necessary, matters may be further elevated to senior executive branch offices for consideration and resolution.[29]

[28] The FEA website is at http://www.whitehouse.gov/omb/egov/a-1-fea.html.
[29] PM-ISE, *ISE Implementation Plan*, Ibid., 36-37.

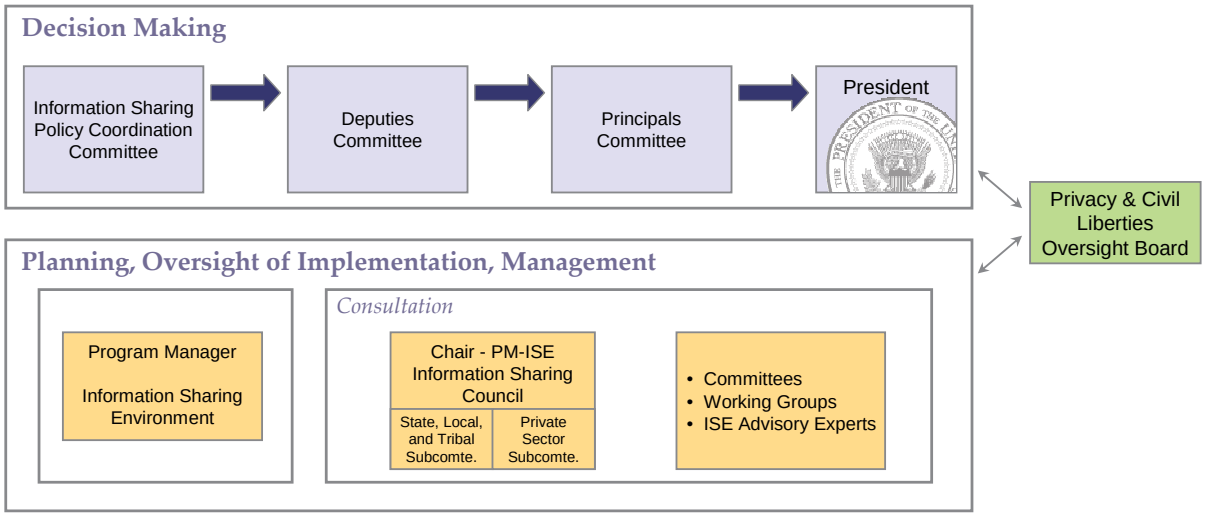


Figure 5. ISE Implementation Governance Roles and Responsibilities

During the CTISS program implementation phase and with overall CTISS administration, the CTISS Committee, chaired by the Office of the PM-ISE with membership from all ISC departments and agencies, NIST, NCS, CNSS, and State and local representatives, will identify and recommend functional standards and technical standards for issuance by the PM-ISE to all ISE participants. Functional Standards will be issued under the "FS" (Functional Standard) issuance designation, and Technical Standards will be issued under the "G" (Guidance) issuance designation. The CTISS Committee will effect harmonization with other Federal agencies and their standards programs. Alignment of NIEM and the DOD/IC U-CORE data elements and standards will be addressed through the activities of the newly formed, inter-agency Executive Steering Committee that interfaces with existing executive forums on standards (Figure 6). Unresolved issues regarding data harmonization may be elevated up to the ISC-level as necessary. Periodic monitoring of CTISS implementation activity will be conducted by the CTISS Committee, under the authority of the ISC, with reports sent to ISE agencies and OMB as appropriate.

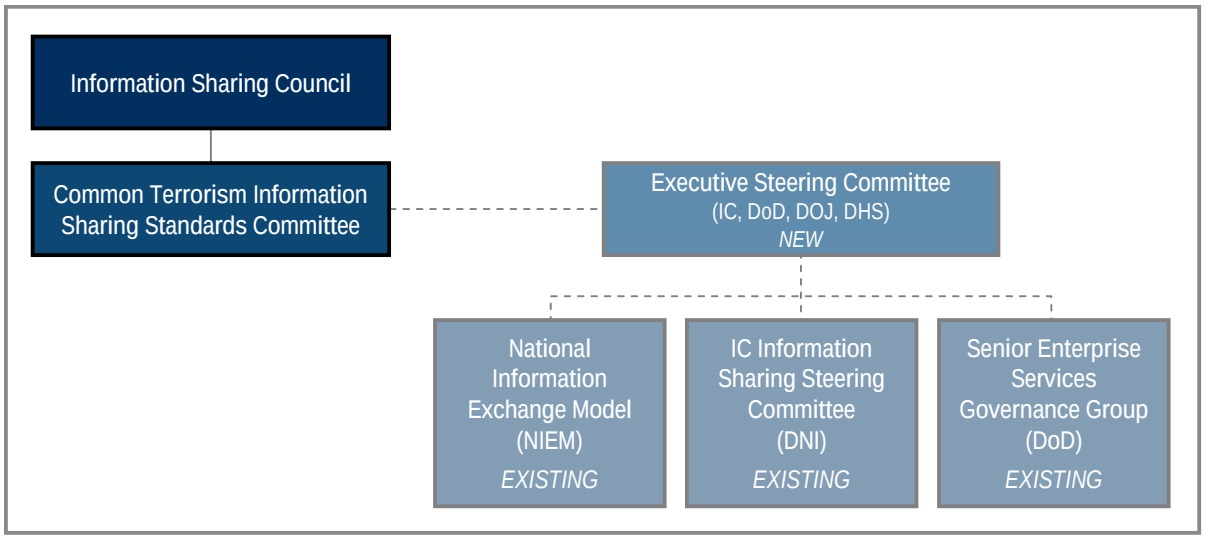


Figure 6. CTISS Administrative Structure

Figure 7 depicts the way NIEM and the DoD/IC U-Core will be leveraged to support the development of the CTISS Universal Core under this administrative structure. 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 developed for Functional Standards in CTISS. Other data elements particular to information sharing business processes will also be integrated with CTISS Universal Core elements to define and standardize the overall information exchanges.

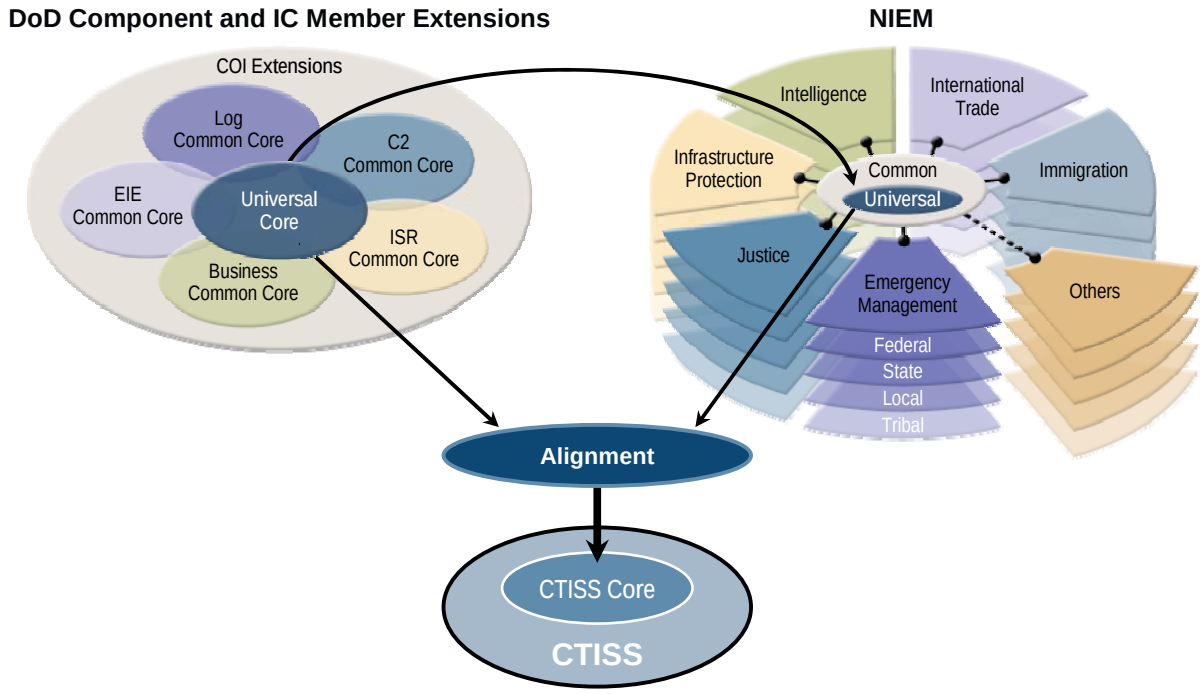


Figure 7. CTISS Universal Core Development

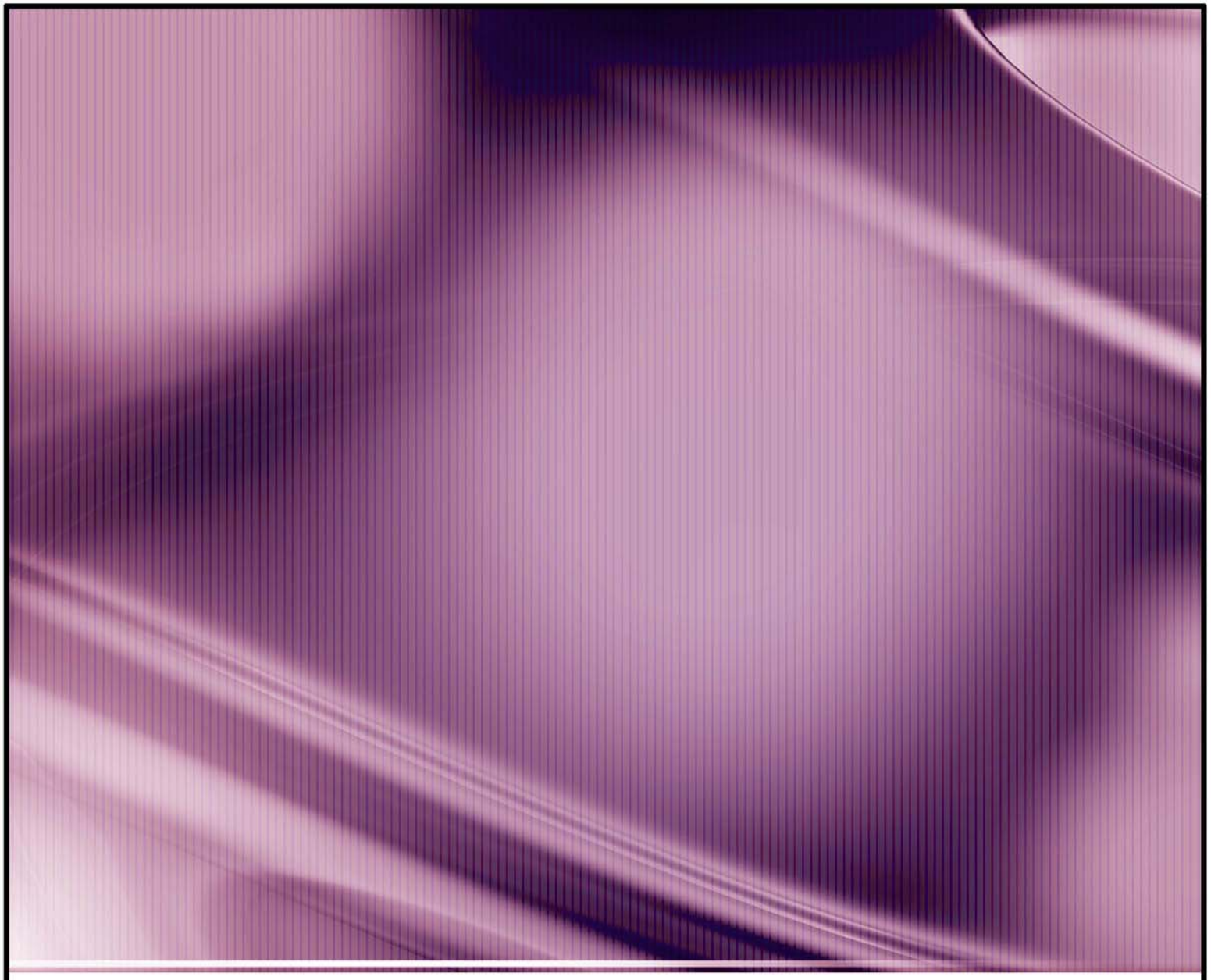
SECTION IX – ACRONYMS

AM	Administrative Memoranda
ANCII	American Standard Code for Information Interchange
ANSI	American National Standards Institute
CAPCO	Controlled Access Program Coordination Office
CCEA	Continuity Communications Enterprise Architecture
CNSS	Committee on National Security Systems
COI	Community of Interest
COP	Committee of Principals
COTS	Commercial Off-the-Shelf
CTISS	Common Terrorism Information Sharing Standards
DCMI	Dublin Core Metadata Initiative
DDMS	Department of Defense Discovery Metadata Specification
DED	Data Element Dictionary
DME	Development, modernization, and enhancement
DoD	Department of Defense
DODEA	Department of Defense Enterprise Architecture
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standards
FS	Functional Standards
G	Guidance
GJXDM	Global Justice XML Data Model
IC	Intelligence Community
ICEA	Intelligence Community Enterprise Architecture
IEP	Information Exchange Package
IEPD	Information Exchange Package Document
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISC	Information Sharing Council

ISE	Information Sharing Environment
ISM	Information Security Markings
ISO	International Organization for Standardization
JRA	Justice Reference Architecture
JXDM	Justice XML Data Model
MIP	Military Intelligence Program
MWG	Metadata Working Group
NCCC	National Command and Control Capability
NCS	National Communications System
NIEM	National Information Exchange Mode
NIP	National Intelligence Program
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
PM-ISE	Program Manager, Information Sharing Environment
REST	Representational State Transfer
RMF	Risk Management Framework
SAR	Suspicious Activity Report
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SDLC	System Development Life Cycle
SLT	State, local, and tribal
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
TS	Top Secret
TWPDES	Terrorist Watchlist Person Data Exchange Standard

U-CORE	Universal Core
UDDI	Universal Description, Discovery, and Integration
W3C	World Wide Web Consortium
XML	Extensible Mark-up Language

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