

Common Terrorism Information Sharing Standards Working Group (CTISSWG) Meeting

10 April 2006

Agenda

1. Getting Started
 - a. Please sign contact sheet
 - b. Introductions
 - c. Review of Agenda for today's meeting
 - d. Review and approval of Meeting Summary from 04 April 06
2. Presentation from the ODNI/CIO on the Six Proposed Standards
3. Discussion of Categories and Types of CTISS
4. Discussion of baseline CTISS
5. Discussion of the ISE Architecture
6. Review of Ongoing Common Standards Efforts, Interconnections and Alignments
7. Wrap Up and Review of Working Group Tasking

Proposed Common Terrorism Information Sharing Standards

Some Background and Context

10 April 2006

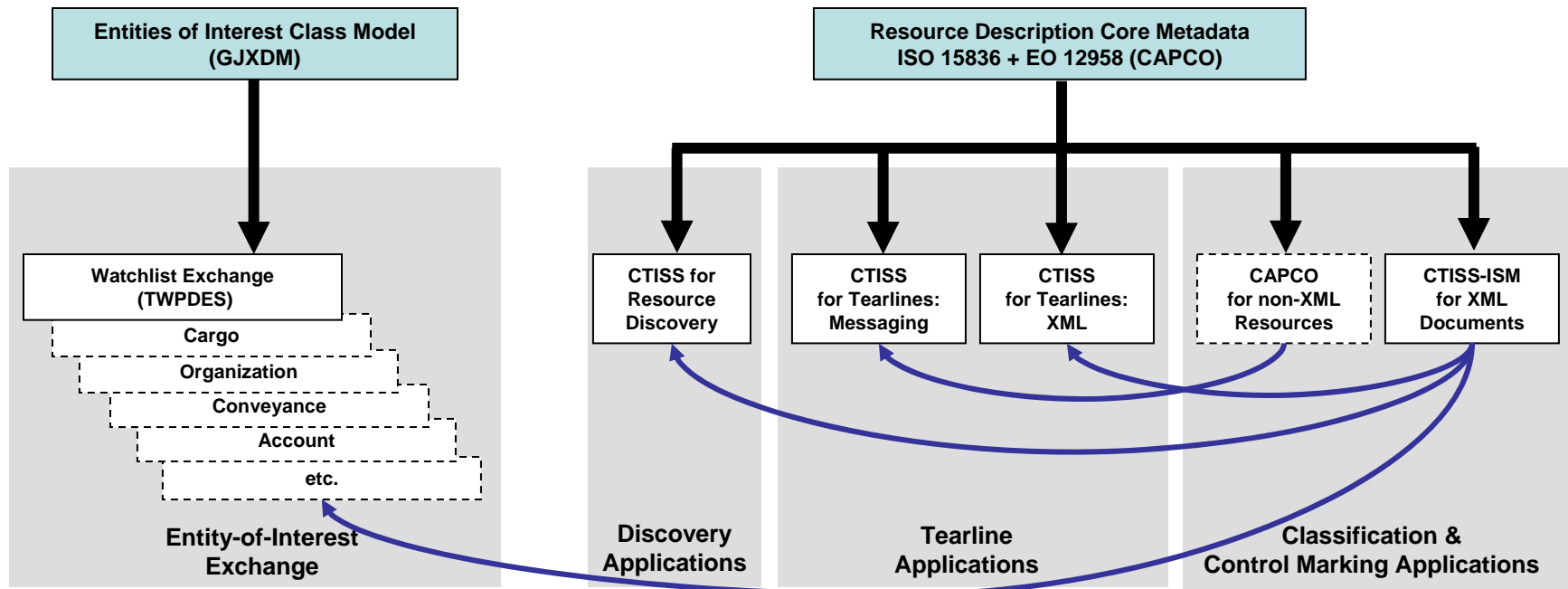
Baseline Standards Proposed

For EO 13356 and Task 2.a(i), (ii) and (iii):




1. **Resource Metadata: Metadata Element Set** (version 1.0, November 2004. (This extends International Standard ISO 15836 by adding a logical element for information security.)
2. **Information Security Markings: XML Implementation** (version 2.0.3, February 2006. (This is a re-titled IC ISM. The current IC ISM version number has been retained in order to avoid confusion among the many IC ISM implementers.)
3. **Resource Discovery Metadata** (version 1.3, June 2005; a.k.a. Defense Discovery Metadata Specification, version 1.3, June 2005)
4. **Tearline Applications: Messaging Implementation** (version 1.1, November 2004)
5. **Tearline Applications: XML Implementation** (version 1.0, November 2004)
6. **TWPDES Person Standard** (version 2.0, July 2005) for watch list exchange
7. **Global Justice XML Data Model (GJXDM)** (version 3.0.3)

Url for the IC Metadata Working Group Six Baseline CTISS Standards Proposed:
<https://www.icmwg.org/ciss/introduction.asp>

CTISS Implementations for Various Applications



GJXDM— Global Justice XML Data Model
CAPCO— Controlled Access Program Coordination Office Implementation Manual
TWPDES— Terrorist Watchlist Person Data Exchange Standard

Applications 
Implementations 
Used by 

Standard 1: Common Information Sharing Standard for Resource Metadata: Metadata Element Set, version 1.0, November 2004.

A superset of International Standard ISO 15836, the Dublin Core Metadata Element Set.

Augmented by adding a logical element for information security.

Definition:

The standard prescribes 16 logical elements of information about digital or non-digital assets that have been made available as shared resources within the national security community, The purpose of the resource metadata standard is to provide a framework for enhancing discovery and exchange. The elements are to be used when applicable.

Identifier	Format
Title	Language
Creator	Type
Publisher	Rights
Contributor	Source
Date	Relation
Description	Security
Subject	
Coverage	

Standard 2: Common Terrorism Information Sharing Standard for Information Security Markings: XML Implementation, version 2.0.3, February 2006.

A module for XML documents to hold the classification and controls marking abbreviations prescribed by E.O. 12958, ISOO Directive 1, the CAPCO Register, and DoD 5200.1-R.

Definition:

Eighteen XML global attributes for use in binding classification, controls, and declassification information to individual XML elements, including a document level element.

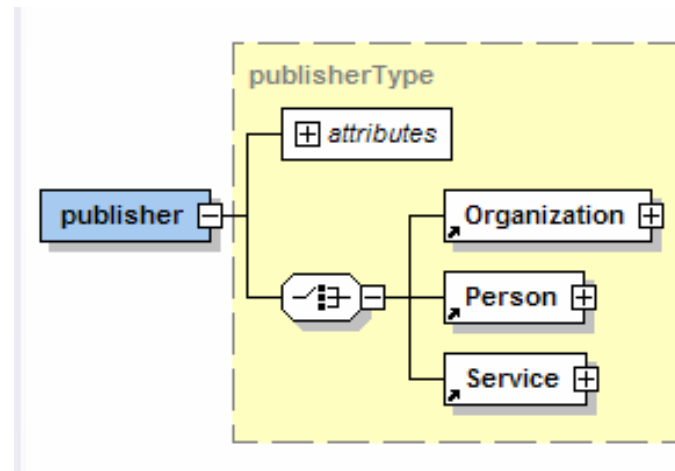
→	ownerProducer	classifiedBy
→	classification	classificationReason
	SCIcontrols	derivedFrom
	SARIdentifier	declassDate
	FGIsorceOpen	declassEvent
	FGIsorceProtected	declassException
→	disseminationControls	typeOfExemptedSource
	releasableTo	dateOfExemptedSource
→	nonICmarkings	declassManualReview

Standard 3: Common Information Sharing Standard for Resource Discovery Metadata, version 1.3, June 2005.

An implementation in XML of standard #1 for purposes of enabling discovery and exchanging resource metadata.

Definition:

A packaging and decomposition of the “CTISS for Resource Metadata: Metadata Element Set” as an XML schema that can be used for discovery in a net-centric environment. This standard provides a more granular implementation so that the contents of the individual Dublin Core logical elements can be better controlled. The schema can be imported into other XML applications in order to associate resource metadata with those applications.



Standard 4: Common Information Sharing Standard for Tearline Applications: Messaging Implementation, version 1.0, November 2004.

Included in response to tearline provision in E.O. 13356.

Definition:

A format that all national level organizations can use for plain text applications (such as cable traffic) to create tearline-delimited reports that will be automatically validated, extracted, and distributed without additional human review for cross-domain dissemination. The standard prescribes a set of markings, prosigns and metadata elements to be used in a specific sequence.

See next slide for an illustration.

:::: BEGIN TEARLINE ::::

Security Marking

WARNING: NONE

ID: 271000 Apr 2004

SUBJ: (S) This is the subject of the SIPRNet version of the document.

DATE: 20040427

TOPIC: TERR


COUNTRY: AFG

SOURCE EVAL: NONE

POC: NONE

TEXT:

(U) This is the body of the SIPRNet variant.

 A local weatherman says that it will rain next month. Send raincoats.

Security Marking

John Hancock

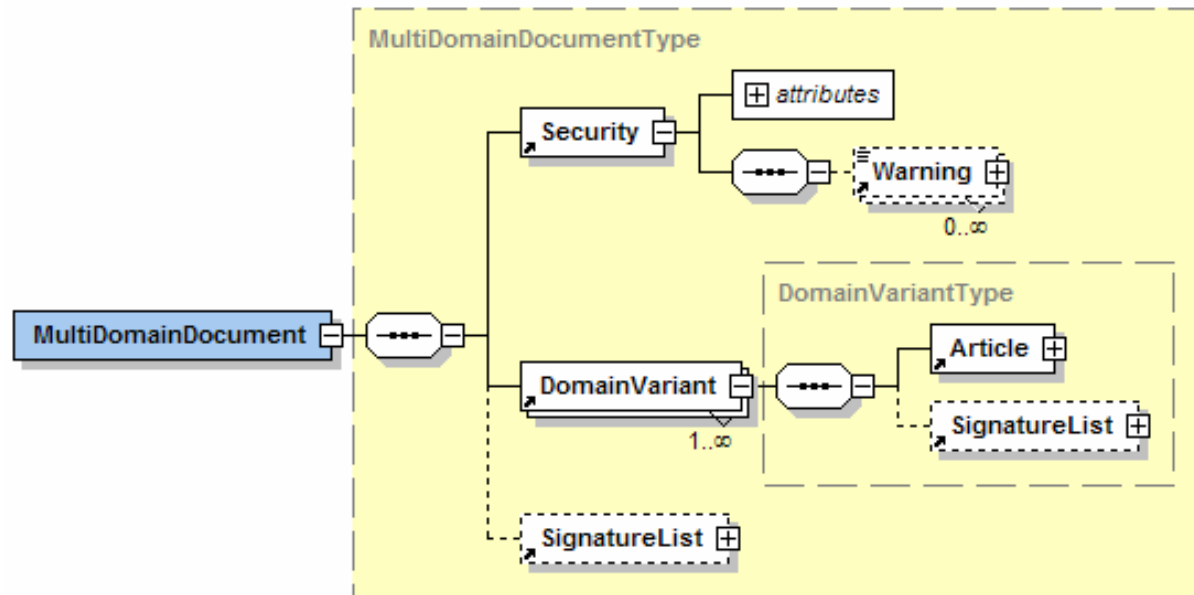
:::: END TEARLINE ::::

Standard 5: Common Information Sharing Standard for Tearline Applications: XML Implementation, version 1.0, November 2004.

Included in response to tearline provision in E.O. 13356.

Definition:

An implementation in XML to support tearline applications and dissemination of document variants to multiple domains. Applies the rigor of well-defined structured markup to specify classification and control markings and metadata in an unambiguous manner that can be used by cross-domain solutions. Facilitates rapid dissemination without unnecessary further human review. Includes provisions for digitally signing all and/or parts of the document.



Standard 6: Terrorism Watchlist Person Data Exchange Standard (TWPDES), version 2.0, July 2005.

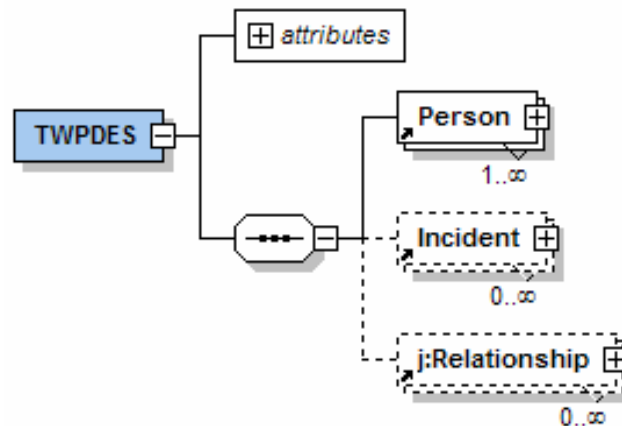
An Implementation of the person class of the Global Justice XML Data Model (GJXDM), version 3.0.3, harmonized with the original TWPDES model.

Created in response to GAO recommendation to standardize watch list formats.

Definition:

TWPDES is an XML implementation of a data exchange format for watch lists. The original TWPDES is in use by organizations feeding data to the NCTC, and by the NCTC to provide data to TSC. TSC uses variants to provide data to its customers. The intent is for these organizations to move to the CTISS version.

Pursuant to the strategic roadmap for responding to E.O. 13356, the CIA, NCTC, TSC, FBI, and OJP harmonized the original TWPDES with the GJXDM person and other classes to produce the CTISS version.



Global Justice XML Data Model (GJXDM), version 3.0.3.

A data model and associated process managed by the XML Structure Task Force, which includes representation of federal, state and local constituencies.

Proposed as the starting point for exchange models for other entities of interest called out by HSPD 6, HSPD 11 and other directives.

Definition:

GJXDM is a comprehensive product that includes a data model, a data dictionary, and an XML schema. It is a class model that defines over 3,000 data elements and the relationships between them. It is also a set of procedures and tools that can be used to create specific interchange formats from the class model. The tools allow implementers to constrain the classes and extend them with application-specific data elements. TWPDES is the result of applying the watch list-related constraints and extensions to the GJXDM person and other classes.

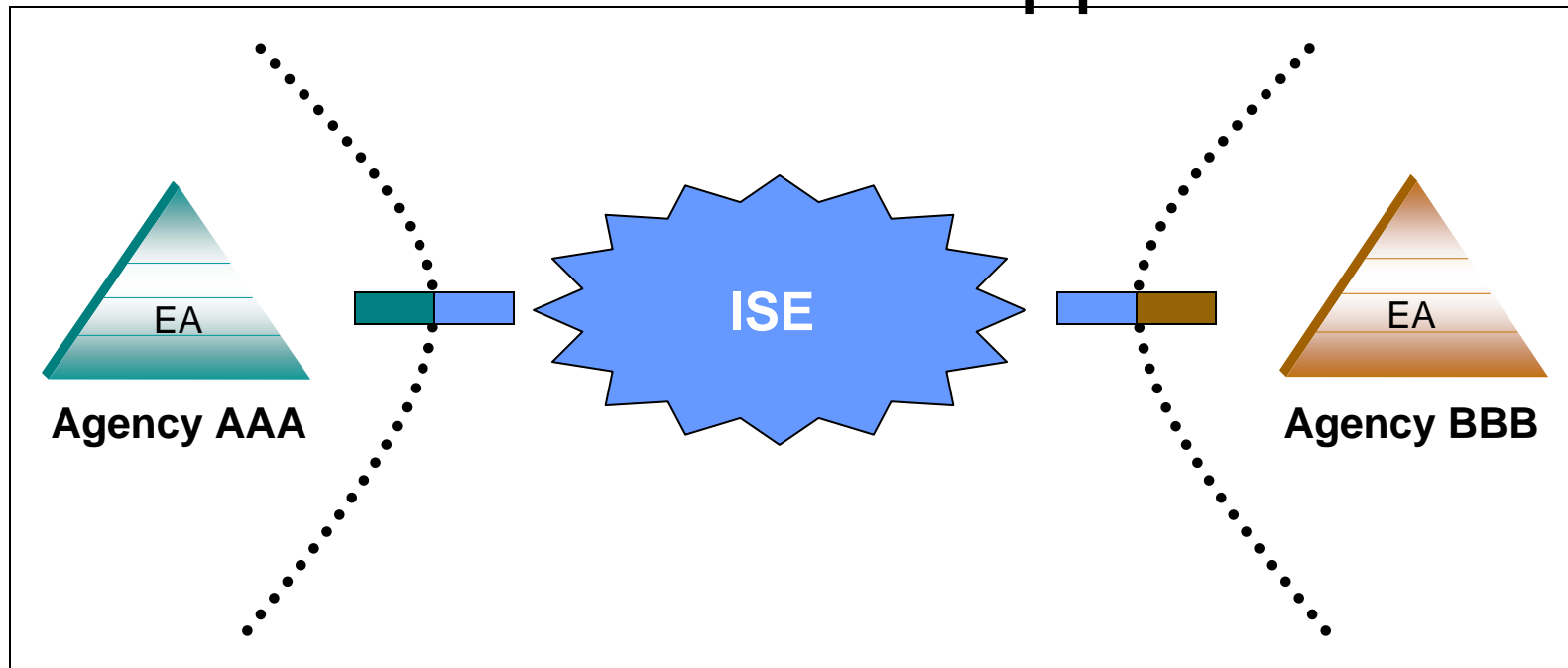
GJXDM is designed specifically for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to create application-specific data exchanges in a timely manner.

GJXDM removes the burden from agencies to independently create exchange standards, and because of its extensibility, there is more flexibility to deal with unique agency requirements and changes. Through the use of a common vocabulary that is understood system to system, GJXDM enables access from multiple sources and reuse in multiple applications.

ISE Architecture

- ISE Architecture Approach
- Terrorism Information Defined

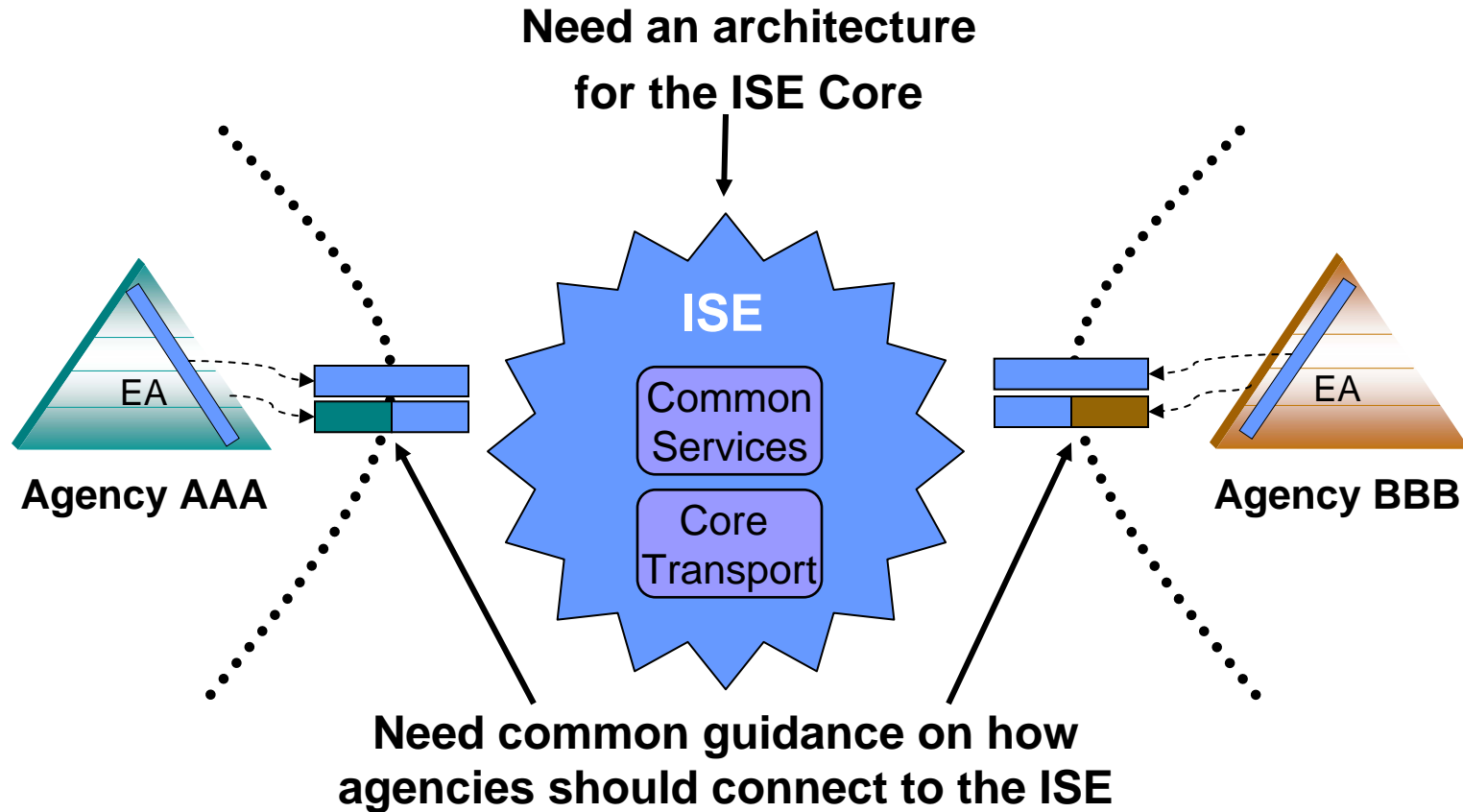
ISE Architecture Approach



Considerations :

- Need to leverage the FEA and associated processes
- Need an architecture to guide the establishment of the ISE
- Need guidance for agencies to include information sharing capabilities in their agency EAs

The ISE Architecture Must Provide Guidance to Each Agency & to Establish an ISE Core



 Short Term: Interface via an adapter to legacy systems

 Long Term: Interface via an inherent capability of the agency systems

Terrorism Information Defined

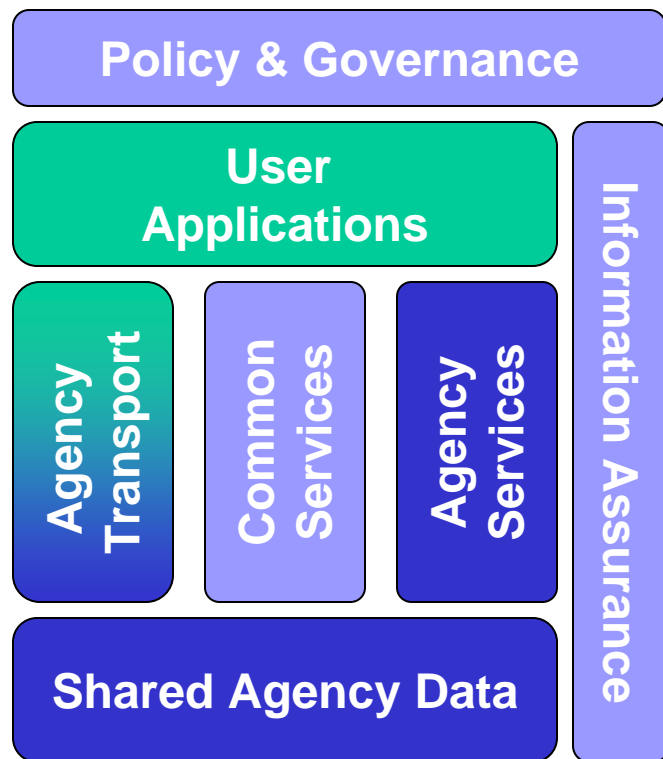
IRTPA at §1016 (a) and (b):

"Terrorism information" is defined 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."

Notional Information Sharing Architecture

ISE

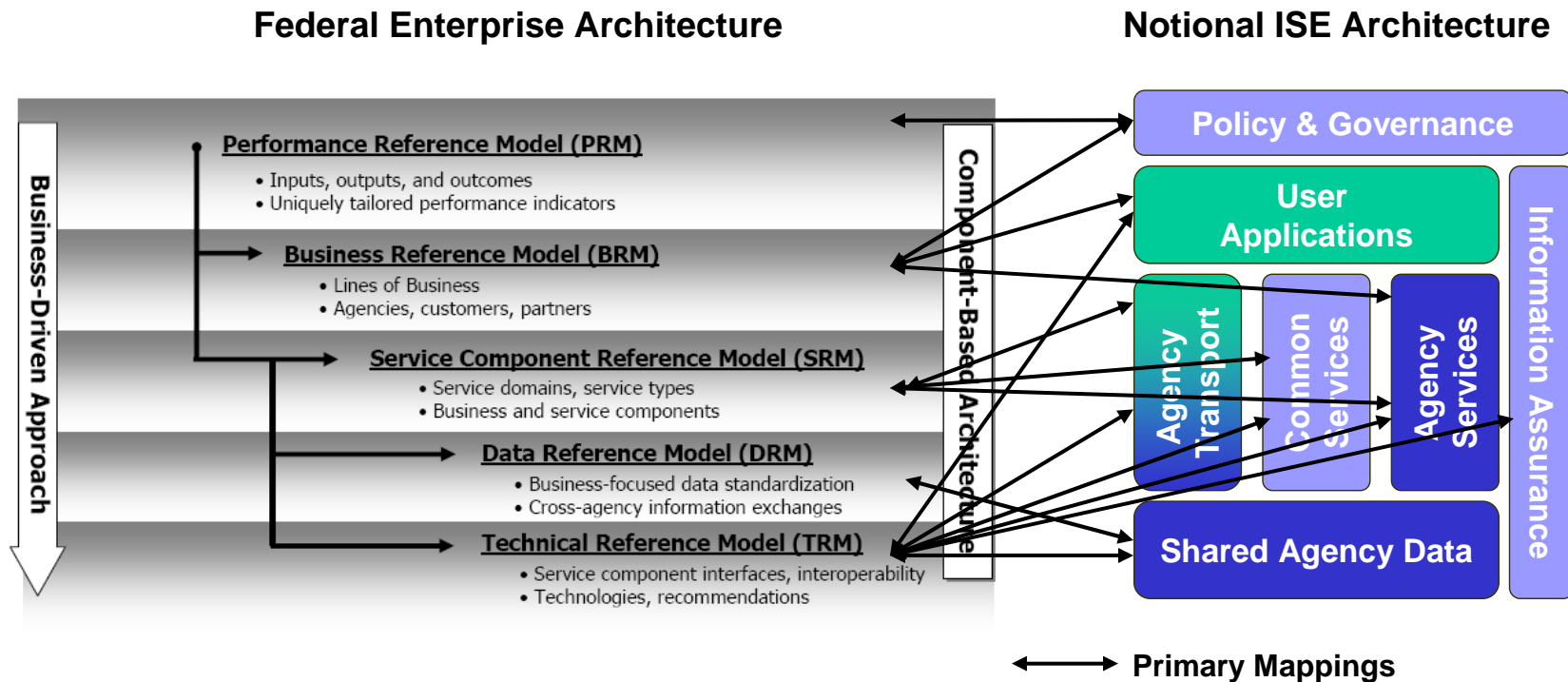


Information Sharing Environment

The notional ISE Architecture consists of 7 elements:

- The Policy & Governance element provides the management and administrative environment to develop and maintain the ISE
- User Applications in a data-consuming agency will access shared information via Web services
- Agency Services will be provide access to data by adding Web services to existing or emerging applications
- The Agency Transport and Common Services elements provide the communications infrastructure
- The Shared Data element provides a vocabulary and data models for the information to shared
- The Information Assurance element provides standards to ensure security & privacy

The Information Sharing Environment Architecture can be Mapped to the FEA



Review of Existing Efforts

- Ongoing Common Standards Efforts – See Handout
- Possible Interconnections and Alignments with CTISSWG

Next Steps

1. By COB, April 14th provide to micheds@dni.gov and mshorter@scitor.com
 - a. Review of Draft Report Detailing Categories and Types of CTISS and Suggested baseline (Tasks 1 and 2)
 - b. Review of Draft Report Detailing Ongoing Efforts and Possible Interconnections (Tasks 3 and 4)
2. Review and provide commentary on draft reports and plan for implementation discussions prior to next meeting
3. Next Meeting: April 18, 2006, 1030-1230
 - a. Discussion on Implementation and Continued Development of CTISS (Task 5)
 - b. Final Review of Draft Report Detailing Categories and Types of CTISS and Suggested baseline (Tasks 1 and 2)
 - c. Final Review of Draft Report Detailing Ongoing Efforts and Possible Interconnections (Tasks 3 and 4)