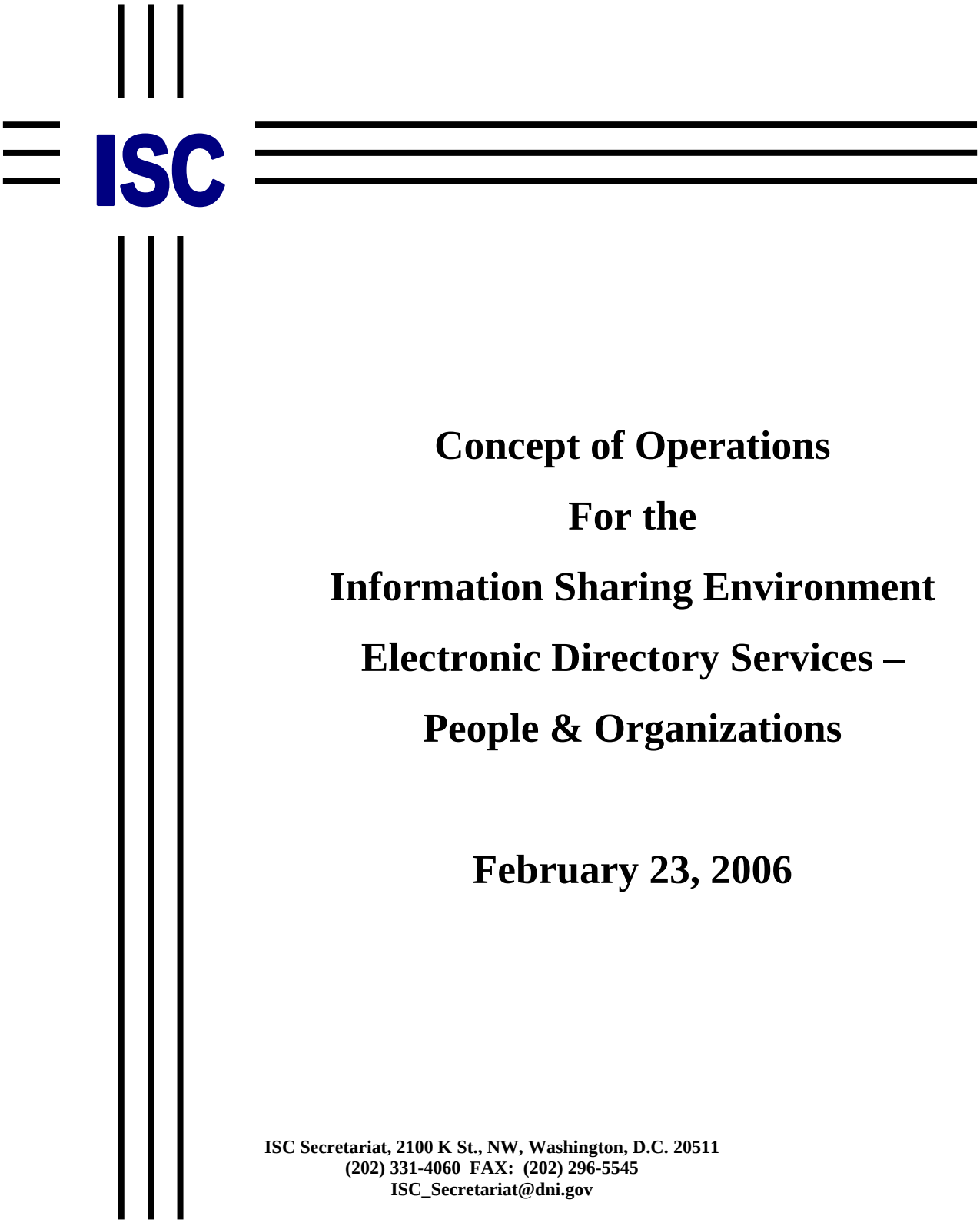
ISC Document
No. 0001



Concept of Operations
For the
Information Sharing Environment
Electronic Directory Services –
People & Organizations

February 23, 2006

ISC Secretariat, 2100 K St., NW, Washington, D.C. 20511
(202) 331-4060 FAX: (202) 296-5545
ISC_Secretariat@dni.gov

ISC Document
No. 0001

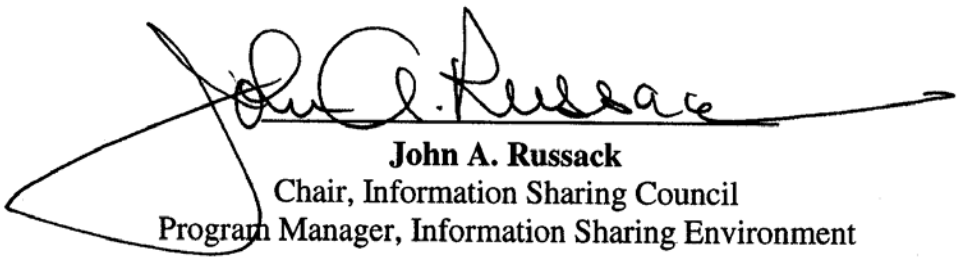
INFORMATION SHARING COUNCIL
WASHINGTON, DC 20511

FOREWORD

1. The Concept of Operations (CONOPS) for the Information Sharing Environment (ISE) Electronic Directory Services – People & Organizations (EDS-PO) identifies the business-driven processes for the initial EDS-PO phases through calendar year 2006. This document serves as a reference for policy and technical directives initiated by the ISE Program Management Office and a top-level strategy for attaining EDS-PO capabilities. The EDS-PO CONOPS, with the February 22, 2006 approval of the ISC, will continue to be revised and updated based on new and emerging user requirements. The primary audiences for the CONOPS are the ISC, the ISE user representatives, the EDS-PO Implementation Team, and executors of the plans to provide the required capabilities.

2. Representatives of the Information Sharing Council may obtain additional copies of this CONOPS at the address listed below.

3. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.



John A. Russack
Chair, Information Sharing Council
Program Manager, Information Sharing Environment

ISC Secretariat, 2100 K St., NW, Washington, D.C. 20511
(202) 331-4060 FAX: (202) 296-5545
ISC_Secretariat@dni.gov

Table of Contents

Figures

Tables

1 Introduction

1.1 Problem Statement

Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) [1] calls for improved sharing of terrorism information to support the country's ability to effectively prosecute the counterterrorism (CT) mission. Improved sharing of information allows users to more efficiently and effectively locate, interact and connect the dots.

Improvements needed to information sharing include:

- Eliminate single points of failure;
- Ensure that information flows not only to senior officials, but also down or laterally to operational entities;
- Improve support to real-time operations;
- Increase connectivity and access between users and critical information; and
- Improve sharing among Federal, State, Local, Tribal (SLT) and private sector (PS) personnel.

Additional observations and principles have been developed by CT practitioners that must be addressed in developing the Information Sharing Environment (ISE) include:

- Integrate systems across Federal, State, Local and Tribal governments;
- Better manage the complexity of the information flood;
- Ensure that information sharing tactics are driven by the needs of the information users; and
- Standardize terminology.

As detailed in the IRTPA, a critical function of an effective Information Sharing Environment is an electronic directory service that facilitates personal contact between CT professionals.[2] To begin the process of overcoming the current shortfalls in our CT capability, IRTPA directs the Program Manager, in consultation with the Information Sharing Council (ISC) to:

> "*(2) Establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information*;"[3]

[1] Pub. L. No. 108-458, 118 Stat. 2638 (Dec. 17, 2004) [hereinafter IRTPA].
[2] See IRTPA §1016 (c)(2)
[3] See IRTPA, §1016 (c)(2)

The goal is to implement directory services that assist in locating *people*, *organizations*, *data* and *services* across multiple security domains and government entities. The initial capability will leverage and expand existing systems to facilitate Federal users in locating people and organizations within the Federal Sensitive Compartmented Information (SCI) and SECRET security domains. This is the focus of this document and is known as Electronic Directory Services – People & Organizations (EDS-PO).

This document also applies to Federal SBU and cross-domain mechanisms. Figure 1 shows the conceptual ISE as three security domains of information. Each of the three security domains contains an EDS capability that supports locating Federal people and organizations and also utilizes cross-domain services inherent in the ISE.

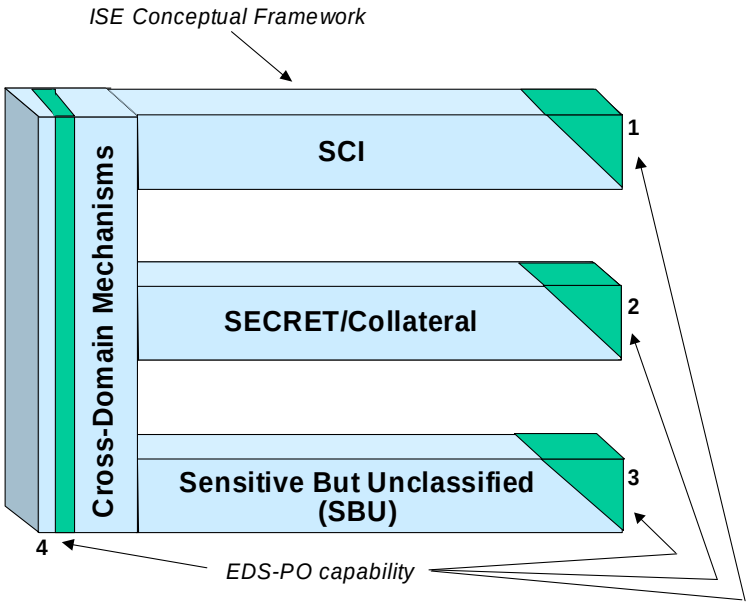


Figure 1: EDS-PO in the ISE Framework.

While the implementation, as per IRTPA, is initially at the Federal level, SLT and PS representatives reviewed this Concept of Operations (CONOPS) to provide early feedback in support of their eventual inclusion into the EDS-PO.

1.2 Document Scope

Currently, three phases are identified for EDS-PO. Details of each phase are to be developed in the Implementation Plans.

Phase 1	By March 31, 2006, the first priorities in Phase 1 are the implementation of a web-based Blue Pages directory with contact information for CT related organizations within the Federal Government and identification of current capabilities that support the EDS-PO CONOPS. Deliverables include Blue Pages on the SCI and SECRET network domains, user feedback mechanisms, links to existing systems that provide EDS-PO functionality, user outreach plan and Phase 2 Network level Implementation Plans.
Phase 2	Through calendar year 2006. Begin the integration of additional directory sources into selected White Pages. Introduce and incrementally develop a Yellow Pages capability. Enhance the functionality of the Blue Pages to better support the expanding White Pages capabilities.
Future Phases	Integration of the EDS-PO functionality into the Information Sharing Environment (ISE) Services Oriented Architecture (SOA) framework. Continue the enhancement of Phases 1 and 2 capabilities.

This document serves as a business process-driven CONOPS for the EDS-PO Phase 1 and Phase 2 implementations through calendar year 2006. Chapter 3 of this document identifies required and desired data attributes that are needed to provide responses to user searches and lead to a description of the derived EDS-PO functionality. A series of notional scenarios that support identification of the attributes and illustrate the utility of EDS-PO in support of the CT user's business processes is given in Section 3.3. Future phases of EDS-PO will occur within the full ISE implementation, driven primarily by an ISE CONOPS, Implementation Plan and SOA.

This document also serves as a reference for policy and technical directives initiated by the PMISE and a top-level strategy for attaining EDS-PO capabilities. Chapter 4 discusses the governance and management of EDS-PO for Phases 1 and 2.

The EDS-PO CONOPS, with the approval of the ISC, will continue to be revised and updated based on new and emerging user requirements. The EDS-PO CONOPS will evolve to define future EDS-PO Phases that address:

- Any new requirements identified as a result of User experience from EDS-PO operation and the development of the ISE CONOPS;

- Lessons learned as Phase 1 and Phase 2 initiatives are implemented and assessed for effectiveness; and
- Integration with the ISE Architecture.

Potential solutions and development methodologies are not discussed in the EDS-PO CONOPS, as the Implementation Plans for each phase of EDS-PO will address technology, standards, framework, tool and protocol details.

The primary audiences for the EDS-PO CONOPS are the ISC, the user representatives, the EDS-PO Implementation Team and executors of the plans to provide the required capabilities.

1.3 Document Development Approach

The ISC, supported by the ISE Program Manager's Office (PMISE), established and directed two teams populated with appropriate representatives from the ISC member agencies.[4]

1.3.1 Strategy Team

The Strategy Team was responsible for developing the EDS-PO CONOPS and identifying the user requirements that represent the needs of users across the various CT mission areas. The Strategy team was comprised of representatives from the stakeholder organizations with relevant mission experience. The PMISE developed the EDS-PO CONOPS to be approved by the ISC.

1.3.2 Implementation Team

Working concurrently with the Strategy Team, the Implementation Team conducted a baseline study to characterize the stakeholders' existing capabilities, which is included in this document as Appendix C. The Implementation Team is responsible for developing the phased Implementation Plan for the EDS-PO to meet the requirements set forth in the EDS-PO CONOPS. Similar to the EDS-PO CONOPS, the Implementation Plan will be approved by the ISC.

1.4 Current EDS-PO Capabilities

Electronic directory services currently exist in a variety of capabilities and maturity levels within the individual communities associated with the ISE and are used primarily to locate people and not information.[5] There is little interaction or integration between these individual directories. In addition, the data collected, the supporting infrastructure technologies, the user roles and the user access methodologies vary across systems, agencies and security domains.

---

[4] Central Intelligence Agency, Department of Commerce, Department of Homeland Security, Director of National Intelligence, Department of Defense, Department of Energy, Department of Justice, Department of Transportation, Federal Bureau of Investigation, Department of Health and Human Services, National Counterterrorism Center, Office of Management and Budget, Program Manager of the Information Sharing Environment, Department of State and Department of Treasury.

[5] Preliminary Report on the Creation of the Information Sharing Environment, PMISE (15 June 2005).

The PMISE, through the EDS-PO Implementation Team, identified a sampling of existing and planned directory capabilities related to CT across the Federal Government (see Appendix C). This activity provided a sampling of current functionality, features, protocols, standards, status and security domains. As part of this process, directory service solutions that are currently sharing information across agency boundaries, or that are capable of being extended to share information, are also identified (see Appendix D).

The existing capabilities form the EDS-PO baseline, from which any improvements will be assessed. The Implementation Plan, to be generated by the Implementation Team, will identify how the gap between the existing baseline capabilities and the EDS-PO CONOPS-identified requirements will be closed.

2 EDS-PO Purpose

2.1 EDS Vision from IRTPA

EDS, a critical component of the ISE, assists in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information.[6]

The full EDS, populated with attributes relating to people, organizations, data and services will ultimately:

- Be fully integrated into the ISE;
- Provide multiple EDS capabilities working together;
- Support controlled access and sharing of information across security domains, consistent with applicable laws, regulations and policies;
- Include technical framework and standards, business processes and policies enabling integration and collaboration;
- Include federated agreements for governance;
- Include people, organizations, services and data to support mission intelligence and data needs; and
- Maintain security and privacy of information that may be useful to adversaries and competitors of the United States, the owners of the information (corporate, organizational, individual) and individual citizens.

As stated in Section 1.1, the first step in the iterative process to develop the full EDS is to focus on *"Assist[ing] in locating. . . .people with relevant knowledge about intelligence and terrorism information."*

2.2 EDS-PO Definition

> *EDS-PO is a set of registries that share a common, trusted and up-to-date view of people and organization information, which includes identification of necessary attributes, desired attributes and standardized metadata on people and organizations, to assist in locating in the Federal Government people with relevant knowledge about intelligence and terrorism information.*

Locating people means that the EDS-PO returns a list of people and organizational points of contact that are relevant to a user-submitted search; Examples of such searches are given in Section 3.3. The EDS-PO response includes at least one method of contact for each person or organization.

[6] See IRTPA §1016 (c)(2)

The concept of White, Yellow and Blue Pages is useful in understanding the functionality and benefit of an EDS-PO as defined below. Users of the ISE will locate contact information in a manner analogous to the use of paper White, Yellow and Blue page telephone directories.

2.2.1 White Pages Concept

Name, personal attributes and at least one method of contact for named personnel. Additional contact information may include phone numbers, email addresses and postal addresses. For urgent needs, an alternate 24/7 method of contact may be included.[7] *Attributes may include such information as skill set, clearance level and areas of expertise. For certain users, some attributes may not be viewable or searchable.*

2.2.2 Yellow Pages Concept

Organization and contact information, which may include description of roles and responsibilities and organization charts. For urgent needs, an alternate 24/7 method of contact will be included. May include a pointer to the organization directory. For certain users, some organization attributes may not be viewable or searchable.

2.2.3 Blue Pages Concept

Organization listing and associated contact information.. For urgent needs, 24/7 method of contact will be included. May include a pointer to the organization directory. For certain users, some organization attributes may not be viewable or searchable.

For all three directory concepts, users who already know the name of a particular person may search by name to retrieve her contact information. For attribute-based searches, EDS-PO will not provide lists of analysts in other agencies for "cold-calling" or mass solicitation of information but, rather, will provide call center, watch center or organizational contact information.[8]

2.3 Users and Stakeholders

A potential EDS-PO user is anyone who is authorized to access contact information, within a network security domain, for people and organizations related to the CT mission. A user will typically use EDS-PO to locate people and organizations who are outside their home organization and who have a different primary function (i.e., cyber-threat analyst from the FBI using EDS-PO to locate a linguist at CIA.) However, users may also, subject to proper authorization, use EDS-PO to perform searches for people and organizations within their own agency. Authorized users from all levels of the government and private sector will use EDS-PO to search for and locate CT related people and organizations.

[7] 24/7 refers to information that allows contact 24 hours per day, 7 days per week, such as a watch center.
[8] Attribute-based searches use criteria such as role, responsibility or expertise rather than a person's name.

EDS-PO users are defined by their need for information, not by position or title. The same user may use the system while performing different roles in the course of their duties.

The EDS-PO principal stakeholders are those organizations that will provide their directory information to the EDS-PO. At the Federal level, principal stakeholders are defined as the organizational participants in the ISC.[9] For Phases 1 and 2, the stakeholders are charged with providing the appropriate data for the EDS-PO.

2.4 Principles and Overarching Strategies

The December 16, 2005 Presidential Memorandum defined principles relevant to the ISE EDS-PO: [10]

- Leverage existing systems to the maximum extent practicable;
- Use mandated information sharing guidelines; and
- Create a culture of information sharing.

2.4.1 Leverage Existing Systems

To develop a successful EDS-PO for Phases 1 and 2, the existing directories and infrastructure of the ISE participants will be leveraged to develop an interim EDS capability as detailed in Section 2.4.4. To accomplish this, the EDS Strategy and Implementation teams will evaluate existing systems and technology using specified criteria to identify the candidate systems that provide initial EDS-PO capabilities. These may be a limited number of systems that can be integrated, with a minimum level of effort and resources, to provide a near-term ISE capability for EDS-PO.

When candidate systems are selected, an Implementation Agent (IA) will be identified and will work with data providers, system owners and stakeholders to allocate the necessary resources to enable data sharing. The primary Phase 1 deliverables are:

- Web-based Blue Pages on the SCI and SECRET network security domains to provide immediate contact information;
- Processes for regularly updating the Blue Pages content;
- User feedback mechanisms;
- Links to existing systems that provide EDS-PO functionality;
- User outreach plan; and
- Phase 2 Network Security Domain Implementation Plans.

[9] Central Intelligence Agency, Department of Commerce, Department of Homeland Security, Director of National Intelligence, Department of Defense, Department of Energy, Department of Justice, Department of Transportation, Federal Bureau of Investigation, Department of Health and Human Services, National Counterterrorism Center, Office of Management and Budget, Program Manager of the Information Sharing Environment, Department of State and Department of Treasury.

[10] Memorandum to the Heads of Executive Departments and Agencies, Subject: *Guidelines and Requirements in Support of the Information Sharing Environment*, (December 16, 2005).

Concurrent with Phase 1, the EDS Implementation Team will work towards designing and implementing new capabilities and services that build upon and harmonize the existing systems and begin to migrate to the goal of a seamless, common view for all ISE users for Phase 2 and into future phases.

2.4.2 Information Sharing Guidelines

The President's Memorandum defines five guidelines in developing processes and systems to share information within the ISE.[11] The guidelines are:

- Develop a common framework;
- Develop common standards;
- Standardize procedures for Sensitive but Unclassified information (SBU);
- Facilitate information sharing with foreign parties; and
- Protect the information privacy rights and other legal rights of Americans.

As the DNI, in coordination with the Secretaries of State, Defense, Homeland Security, the Attorney General, the ISC and others as directed by the President, issues frameworks, standards, procedures and additional guidance designed to "maximize the acquisition, access, retention, production, use, management and sharing of terrorism information within the ISE", EDS functionality will be adjusted to implement the emerging best practices, technologies and standards.[12] The EDS-PO will be integrated, using a Service Oriented Architecture (SOA) framework, within the larger ISE to be both a consumer and provider of services. Additional standards and services may include data representation languages, technologies for directory updates and retrieval and access control policies.

2.4.3 Create a culture of information sharing

The goal of the Information Sharing Environment is to break across institutional barriers and processes in order to facilitate communication and collaboration for users working on CT missions. In support of that goal, characteristics of a successful ISE-based EDS-PO include:

- Operates within a "need to share" (rather than a "need-to-know") culture;
- Implements security and access control by adequate identity management, authentication and authorization mechanisms;
- Data is accessible by users in an SOA-based framework rather than through centralized information control; and
- Provides contact information for CT related people and organizations in the Federal Government (State, Local, Tribal Governments and the Private Sector are to be included in future phases.)

[11] Memorandum to the Heads of Executive Departments and Agencies, Subject: *Guidelines and Requirements in Support of the Information Sharing Environment*, (December 16, 2005).
[12] Memorandum to the Heads of Executive Departments and Agencies, Subject: *Guidelines and Requirements in Support of the Information Sharing Environment*, (December 16, 2005).

This EDS-PO CONOPS has been developed, in accordance with these characteristics, to reflect the users' business-processes, recognizing that much information sharing occurs today after personal contact by phone, email or face-to-face. In order for users to effectively use the functions described here for locating people and organizations, attribute information that may have been optional in existing systems will become mandatory. Furthermore, in order for the full EDS (i.e. people, organizations, data and services) to function as required by law, policy changes may mandate information sharing between the disparate directory repositories of the Federal Government, SLT and PS. This will be accompanied by governance agreements and performance measures.

2.4.4 The EDS Roadmap

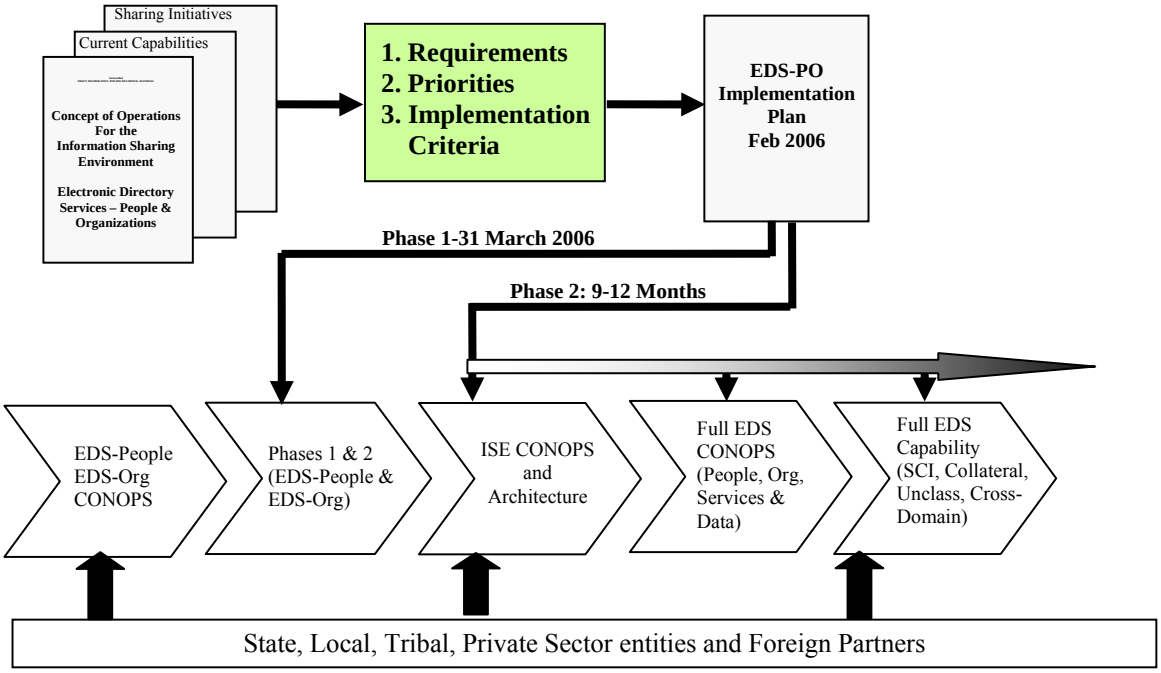


Figure 2: EDS Short-Term and Long-Term Roadmap

The relationship between the EDS-PO CONOPS and the full EDS capabilities to be developed for the ISE is shown in Figure 2. The path to full EDS capabilities includes the following steps:

1. The Current Capabilities (see Appendix C) and Sharing Initiatives (see Appendix D) Matrices define the baseline, or starting point. The Implementation Team will establish evaluation criteria to identify implementation candidates from amongst the current capabilities and sharing initiatives.
2. Selected implementation candidates will be:
   - Included in the March 31, 2006 EDS-PO Phase 1. Any enhancements to current capabilities or sharing will be incorporated as time and resources permit.

- Included in the EDS-PO Phase 2 Implementation Plan. Additional parts of the solution satisfying the EDS-PO CONOPS-identified requirements could span policy, process, technology, promulgation or other initiatives.

3. The Implementation Plan will identify how the gaps between the EDS-PO CONOPS-specified requirements and the current systems will be closed.
4. The EDS will provide a service within the Information Sharing Environment and, as such, will eventually be fully integrated within the ISE services framework.

2.5 Assumptions, Constraints and Risks

2.5.1 Assumptions

These are circumstances, conditions or actions that are believed to be true for the purposes of implementing EDS-PO:

- Changes in Law, Regulation, or Policy – If the need for a change in an executive order, regulation, or administration policy is identified, the existing governance structure for the ISE will institute the change in order to remove obstacles to the EDS-PO implementation.[13]
- Cultural Impediments to Change – The perceived value of an implemented EDS-PO can overcome cultural impediments to change existing sharing arrangements and philosophies.
- Quality in Transition - Users are aware of and will accept data quality limitations as the system develops. For Phases 1 and 2, the EDS-PO will use “best available” data in terms of accuracy, authority and timeliness (see Section 3.1.4.)
- Phases 1 and 2 User Access – Information within EDS-PO Phases 1 and 2 will be accessible only by US citizens.
- Need to Share – For Phases 1 and 2, users of EDS-PO in a security domain have a "need-to-share" the contact information for people and organizations.

2.5.2 Constraints and Risks

These are element that may restrict, limit or place control over the implementation of EDS-PO. The following constraints and risks have been identified:

- Time – IOC for the initial phase of EDS-PO functionality is March 31, 2006. The compressed timeline includes the risk that most of the desired early functionality will be implemented during Phase 2 or subsequent phases.
- Security – The users of EDS-PO will have varied clearance levels and information requirements and will obtain access via multiple, separate network security domains. This may restrict certain contact information from being provided by the EDS-PO participants for Phases 1 and 2.
- Domain Level Access Control: Phases 1 and 2 will rely on network access control and logging mechanisms. Subsequent phases will use the ISE access control services.

[13] Information Sharing Environment Interim Implementation Plan (January 2006)

- Resources – EDS-PO operates within existing resources and will identify opportunities to eliminate unnecessary duplication and redirect resources to accomplish overall ISE goals. As a result, EDS-PO participants may be required to reallocate limited funds and resources in order to implement EDS-PO.
- Use of Existing Systems – While EDS-PO will leverage existing systems to the maximum extent practicable, selected systems may provide significant challenges for interoperability due to security features, proprietary designs or other system characteristics.

3 Mission Objectives

The EDS-PO will allow users to find contact information about people and organizations that are relevant to exchanging mission-related information. Such cross-mission contact among experts will significantly enhance our Nation's execution of the CT mission.

The remainder of this section lays out the related user requirements, data elements and functional characteristics. It is understood that the fielded capabilities will evolve over multiple phases and that initial capabilities will be those that are part of existing legacy programs of record and systems.

3.1 User Requirements

3.1.1 User Interface

- User access to EDS-PO functionality will be included in each of the three network security domains identified in Figure 1, with access to domain-appropriate people and organizational information.
- As functionality becomes available in the phased implementation approach, the EDS-PO will support both text searches and structured searches for names, organizations and terrorism-related attributes for Blue, Yellow and White pages. (See sections 2.2.1, 2.2.2 and 2.2.3 for specific definitions).
- User access will include Graphical User Interfaces that support both free-text and structured search and consist of standard form elements such as drop-down menus, checkboxes and radio buttons.
- EDS-PO will include a service that aligns attribute names into a common taxonomy in order to address the lack of standardized metadata terminology across the multiple agencies and departments that have a role in the CT mission.
- EDS-PO will provide a thesaurus service ("fuzzy" search) that identifies key words or metadata attributes that are similar to terms in a user search.

3.1.2 Accessibility

- The EDS-PO will be available via standard web browser for all Federal users in the SCI and SECRET network security domains.
- Participating departments and agencies will provide varying levels of people and organization contact information to the EDS-PO depending on the network security domain. For Phases 1 and 2, EDS-PO will not provide an access control service, but rather rely on network access control and logging mechanisms. Subsequent phases will use the ISE access control services.

3.1.3 Accuracy and Timeliness of Data

- The participating agencies are responsible for the accuracy and timeliness of submitted data.

- A process will be available to users, through their parent organization, to submit updates and corrections to their own EDS-PO information. The process and execution of such updates and corrections will be determined by participating departments and agencies, in accordance with applicable laws. The system will track when data is updated and reviewed and display that information when available.

3.1.4 User Searchable Attributes

The attributes that a user can search are defined below. Section 3.2 contains a list of required and desired attributes and data elements necessary for the EDS-PO to achieve full user functionality. Section 3.3 contains notional views of the searches and results.

3.1.4.1 Blue Pages

Searchable attributes for the EDS-PO Blue Pages will be:

- Department/Agency/Service; and
- Organization.

3.1.4.2 Yellow Pages

Searchable attributes for the EDS-PO Yellow Pages will be:

- Department/Agency/Service;
- Watch/Call Center Name;
- Intelligence Topic (relevant NIPF topic); [14]
- Country/Region (refined NIPF element);
- Language (expertise); and
- Jurisdiction (locality or region of responsibility – State, US region, etc.).

3.1.4.3 White Pages

For White Pages searches on attributes other than the person's name, EDS-PO will provide call center, watch center or organizational contact information. Searchable attributes for the EDS-PO White Pages will be:

- Name (surname, given name);
- Department/Agency/Service;
- Organization;
- Intelligence Topic (NIPF);
- Country/Region (NIPF);
- Language;

[14] National Intelligence Priorities Framework – a framework for the President to prioritize the intelligence needs of the United States. Intelligence Topics (IT) are high level intelligence related topic areas (e.g., Terrorism, Military Capabilities) that are prioritized and broken down into detailed intelligence needs.

- Jurisdiction (locality or region of responsibility – State, US region, etc.)

3.1.5 User Search Results

In addition to views of information specific to the type of search (Blue, Yellow or White) performed, several general guidelines will be followed for search results:

- The applicable Watch Center contact information should be returned for all attribute-based search responses. Watch Center and other organizational contact information should be displayed at the top of the results list.
- Search results will always include at least one method of contacting a relevant person or organization. Users searching for a person (White Pages) may be returned contact information for an organization (Yellow Pages or Blue Pages) based upon security and resource management considerations.
- Contact information returned on a search will reflect the best available information from the data provider and will include "date last updated" and "date last reviewed" information when available.

3.1.5.1 Blue Pages

A Blue Pages type search result will provide the user the following contact information, when available:

- Department;
- Watch Center or Call Center Name;
- Unclassified Phone;
- Unclassified Email;
- Secure Phone;
- Secure Email; and
- Continuity of Operations (COOP) contact information.

3.1.5.2 Yellow Pages

A Yellow Pages type search result will provide the user the following contact information, when available:

- Department;
- Watch Center or Call Center Name;
- Unclassified Phone;
- Unclassified Email;
- Secure Phone;
- Secure Email;
- Mission areas of expertise (including NIPF topics); and
- COOP contact information.

3.1.5.3 White Pages

A White Pages type search result will provide the user the following contact information, when available:

- Name (surname, given name, MI);
- Department;
- Unclassified Phone;
- Unclassified Email;
- Secure Phone;
- Secure Email;
- Watch Center Phone (or 24/7 Contact phone); and
- COOP contact information.

3.2 Data Attributes

The following table contains a list of required and desired attributes and data elements necessary for the EDS-PO to achieve full user functionality. The table also illustrates which of these attributes, when available, should be searchable from the search screen and viewable in the response screen.

For Blue Pages EDS-PO entries:

Attribute	Description	Mandatory	Populate if available	Searchable	Viewable
Department/Agency/Service	e.g., FBI, NJ State Police	X		X	X
Organization	e.g., JIATF-CT, WINPAC	X		X	X
Phone	Unclassified, Secure	X			X
Email	Unclassified, Secure	X			X
24/7 Phone	Alternate contact phone number for 24/7 contact		X		X
Watch Center	Watch Center affiliated with people and organizations in search results		X		X

Table 1: Data Attributes for Blue Pages

For Yellow Pages EDS-PO entries:

Attribute	Description	Mandatory	Populate if available	Searchable	Viewable
Department/Agency/Service	e.g., FBI, NJ State Police	X		X	X
Watch/Call Center Name	e.g., NSOC, NMCC Alert Center	X		X	X
Phone	Unclassified, Secure	X			X
Email	Unclassified, Secure	X			X
Intelligence Topic	Relevant NIPF IT	X		X	X
Country/Region	More refined element of NIPF IT	X		X	X
Language	Expertise		X	X	X
Jurisdiction	Locality or region of responsibility (e.g., State, US Region)		X	X	X
Alternate Site (COOP) Phone	Phone number in the event that the primary site cannot be contacted	X			X

Table 2: Data Attributes for Yellow Pages

For White Pages EDS-PO entries:

Attribute	Description	Mandatory	Populate if available	Searchable	Viewable
Name	Surname, Given, MI	X		X	X
Department/Agency/Service	e.g., FBI, NJ State Police	X		X	X
Organization	e.g., JIATF-CT, WINPAC	X		X	X
Phone	Unclassified, Secure	X			X
Email	Unclassified, Secure	X			X
24/7 Phone	Alternate contact phone number for 24/7 contact		X		X
Watch Center	Watch Center affiliated with people and organizations in search results		X		X
Intelligence Topic	Relevant NIPF IT		X	X	X
Country/Region	More refined element of NIPF IT		X	X	X
Language	Expertise		X	X	X
Jurisdiction	Locality of people and organizations are responsible for (State, US Region)		X	X	X
Alternate Site (COOP) Phone	Phone number in the event that the COOP site must be contacted		X		X

Table 3: Data Attributes for White Pages

3.3 Notional Search and Result Views

The following figures represent how a user will interact with EDS-PO for searching, the display of the search results and the additional information available if a specific result link is selected. These figures are not meant to represent exact build specifications and are not necessarily complete.

3.3.1 Blue Pages Search

In the following figure, a user specifies a search by one or more attributes. If a specific value is not selected, it defaults to "All".

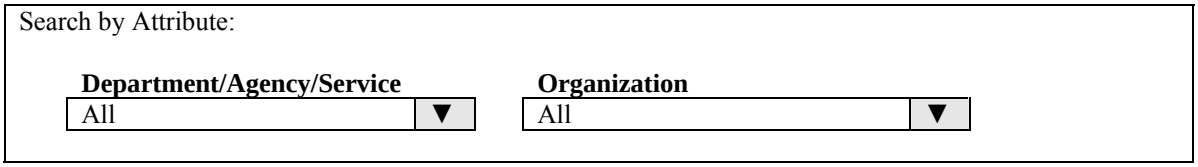


Figure 3: Blue Pages Search Example

3.3.2 Blue Pages Result View

The following figure shows the constant banner of key contacts and, below, the search results.

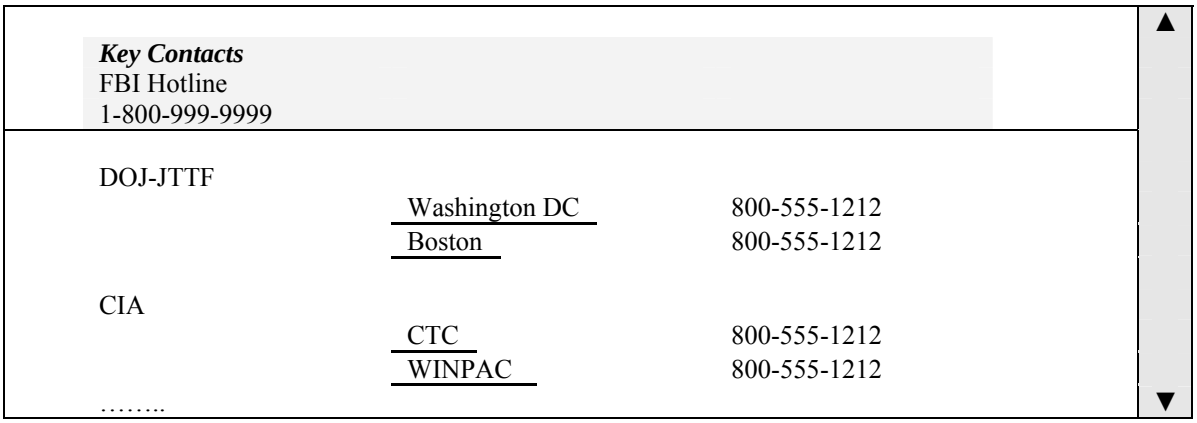


Figure 4: Results from Blue Pages search example

3.3.3 Blue Pages Detail View

The following figure displays all the viewable attributes of a single Blue Pages search result and is displayed by clicking on the location link of the result view.

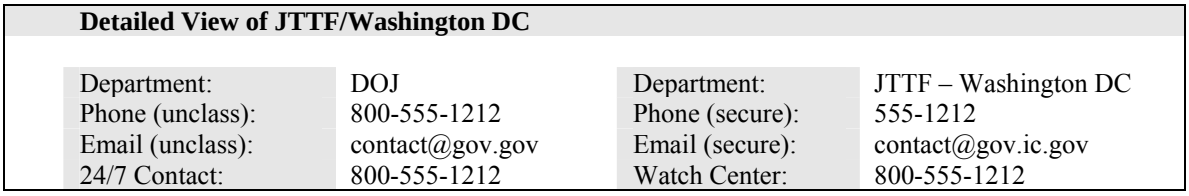


Figure 5: Detail View of a Blue Pages result

3.3.4 Yellow Pages Search

In the following figure, a user specifies a search by one or more attributes. If a specific value is not selected, it defaults to "All".

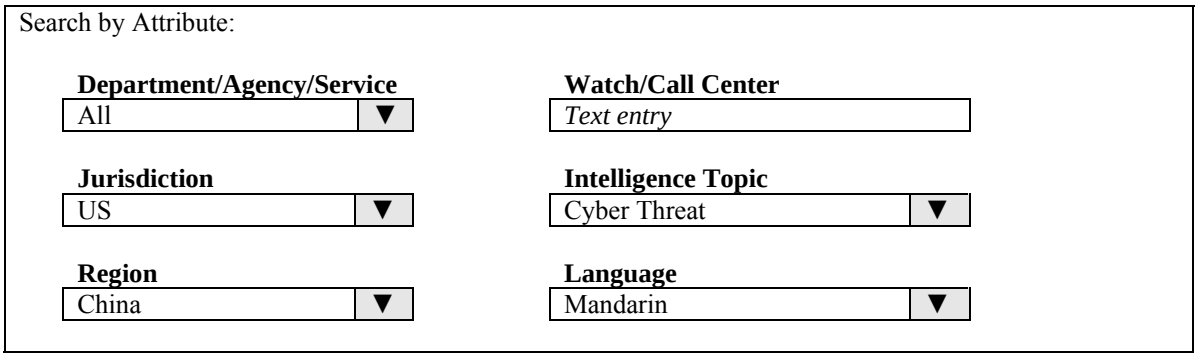


Figure 6: Yellow Pages Search Example

3.3.5 Yellow Pages Result View

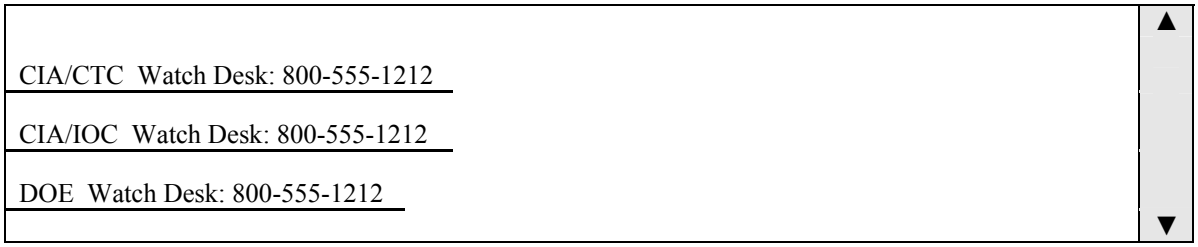


Figure 7: Results from Yellow Pages search example

3.3.6 Yellow Pages Detail View

The following figure displays all the viewable attributes of a single Yellow Pages search result and is displayed by clicking on the location link of the result view.

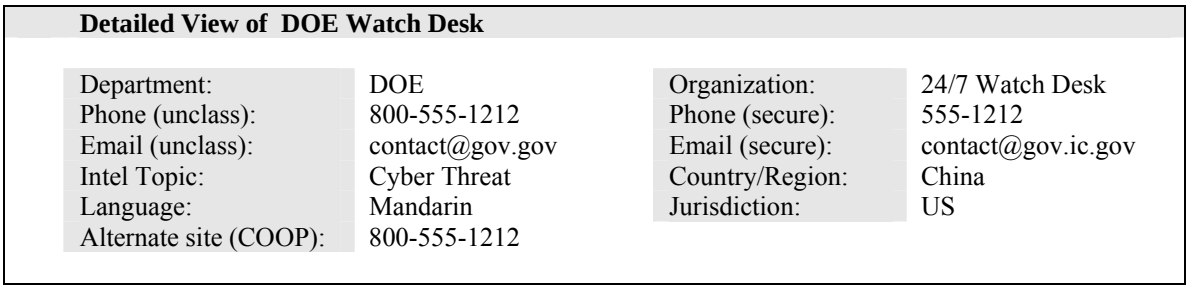


Figure 8: Detail view of a single Yellow Page result

3.3.7 White Pages Search

In the following figure, a user specifies a search by entering a person's name and/or by selecting one or more attributes. If a specific value is not selected, it defaults to "All".

Search by Name and Attribute:

First Name J

Last Name Smith

Department/Agency/Service CIA ▼

Organization All ▼

Intelligence Topic Cyber Threat ▼

Region China ▼

Language All ▼

Figure 9: White Pages search example

3.3.8 White Pages Result View

Smith, John CIA/IOC 800-555-1212 contact@gov.gov

Smith, John CIA/WINPAC 800-555-1212 contact@gov.gov

Smith, J CIA/Syria Watch Desk: 800-555-1212

Figure 10: Results from White Pages search example

3.3.9 White Pages Detail View

The following figure displays all the viewable attributes of a single Yellow Pages search result and is displayed by clicking on the location link of the result view.

Detailed View of Smith, John at CIA

Name:	Smith, John		
Department:	CIA	Organization:	IOC
Phone (unclass):	800-555-1212	Phone (secure):	555-1212
Email (unclass):	contact@gov.gov	Email (secure):	contact@gov.ic.gov
NIPF Intel Topics:	Cyber Threat	Country/Region:	China
Languages:	None	24/7 Phone:	800-555-1212
Watch Center	800-555-1212	Alt site (COOP):	800-555-1212
Jurisdiction:	US		

Figure 11: Detail view of a single White Pages result

3.4 Functional Capabilities

Phases 1 and 2 will expand on existing capability and this section details functional objectives for future phases. To ensure both short-term and long-term success, EDS-PO development subsequent to Phase 2 will emphasize several baseline characteristics:

- Information exchange across network security domains;
- Add new/correct data sources;
- Handle data and user growth;
- Disaster recovery capability;
- Low cost of operations;
- High availability; and
- Responsiveness.

These baseline characteristics translate to functional capabilities:

- Information Assurance;
- Infrastructure Independence and Interoperability;
- Scalability;
- Modularity;
- Redundancy;
- Maintainability; and
- Understandability.

3.4.1 Information Assurance

The EDS-PO capability must be supported by the capability to protect and defend its information, information systems and information infrastructure against a variety of cyber threats. This encompasses mechanisms and measures to defend, restore and recover, as well as to maintain situational awareness.

3.4.2 Infrastructure Independence & Interoperability

The incremental approach used to develop the initial EDS-PO capability requires connectivity among multiple systems across many legacy systems operated by multiple agencies and organization. In many cases, the systems today serve single organizations (segment of an agency) with little or no interaction with external systems. The successful development of EDS-PO requires that defined interfaces for exchange of EDS-PO information be established. As the implementation of a cross-community, cross-domain EDS-PO proceeds, a standards-based implementation, such as SOA, is required to ensure future, successful integration of new systems into the ISE.

3.4.3 Scalability

As EDS-PO matures from its limited, initial capability, growth will occur in two areas: the number of interconnected systems/directories and the number of users. EDS-PO will be implemented such that the growth in data and usage can be handled by the scaling of hardware, software and network infrastructure. Part of this strategy is that these inter-connections are not point-to-point but are to a common services cloud in order to provide scaling, efficiency and manageability benefits.

3.4.4 Modularity

Over time, significant capabilities will be added to the baseline EDS-PO. In order to enhance functional flexibility for the system while isolating functional details within well-defined elements, the system will adhere to a modular architecture. This approach means that additional services and capabilities will be developed such that they operate independently from the operations of the other components, or interact with each other only through well-defined interfaces.

3.4.5 Redundancy

To support high availability, data security and disaster recovery, the EDS-PO will address the need for redundant data stores in distributed geographical locations. Geographically dispersed redundancy ensures data survivability and, if properly implemented, also provides redundant networks paths.

3.4.6 Maintainability

EDS-PO maintainability encompasses two segments – systems and data. Although systems operations and maintenance (O&M) cost is a factor in the implementation of EDS-PO, the maintainability of data is critical. Distributed and remote management will support effective systems O&M. Efficient data maintenance, to include both accuracy and currency, is ensured by instituting policies that push the maintenance responsibility to the data providers.

3.5 Business Processes Supported By EDS-PO

Scenarios in this section are used to illustrate the interaction of the users with the EDS-PO during the course of their various business processes.[15] For the purpose of providing common definitions across the user base, the EDS-PO Strategy Team developed four general business processes that are supported by the EDS-PO. The business processes themselves are beyond the scope of the EDS-PO. However, the EDS-PO is a facilitator of the business processes by enabling the location of people and organizations. This facilitation promotes information sharing, which in turn contributes to improved business process outputs.

Two user-oriented Use Cases have been generated to characterize the user interaction with EDS-PO; they are called "*conduct a keyword search*" and "*conduct a structured*

[15] Specific Scenarios and Use Cases, based upon this Chapter, may be developed in the EDS-PO Implementation Plan as necessary to convey functionality status throughout the phases of implementation.

search" where the actor is the user and EDS-PO is the system. After providing a description of the business process drivers and a general scenario, the Use Cases are presented. Each Use Case is accompanied by a notional Usage Narrative that uses an example to illustrate how a user will interact with the EDS-PO in a typical situation.

The business process outcomes are enhanced by the use of the EDS-PO by connecting relevant people and organizations. The EDS-PO does not replace normal reporting, coordination and operational chains of command inherent in the business processes.

3.5.1 Business Process Descriptions

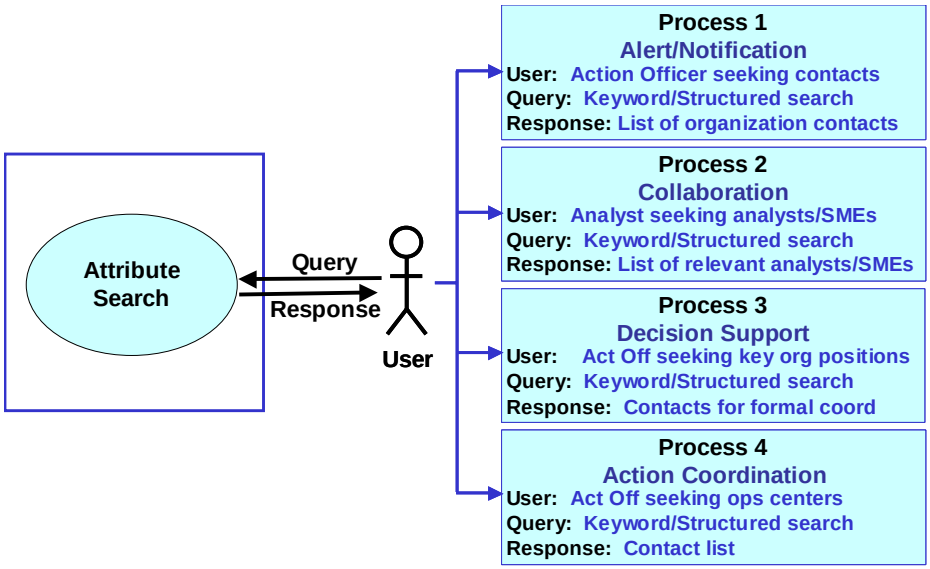


Figure 12: Business Processes Supported by EDS-PO

1. Alert/Notification – The Alert process refers to a user attempting to answer the question, "Who needs to know about an event or information item and how do I contact them?" The intent is the rapid dissemination of information to interested parties that are not part of the user's normal reporting procedures, i.e. cables, product reports or even the CRITIC[16] system. The user is supplementing normal reporting channels when the situation warrants doing so.
2. Collaboration – Collaboration occurs when a user attempts to answer the question, "Who is an expert on this topic and how do I contact them?" Collaboration includes information fusion and analysis for law enforcement purposes. This process may also include a feedback and follow-up mechanism to assess the value of the collaboration and/or generate after-action analyses.
3. Decision Support – Decision Support occurs when a user attempts to locate and contact interested parties that can coordinate on the development of courses of action, estimates of supportability and other decision support activities.

[16] CRITIC – Handling system for messages containing national security information that must be delivered to the highest levels of the government as fast as possible.

4. Action Coordination – The Action Coordination process occurs where decisions have been taken and relevant people and organizations must be identified and contacted to coordinate and implement specific activities.

3.5.2 Generic Scenario – Target of interest

Below are three scenarios given to show EDS-PO supporting these business processes on a generic Target of Interest, Production of Intelligence and Notification of a Target of Interest.

The user can be performing the role of intelligence analyst, law enforcement officer or any other role supported by the business processes. To illustrate the functionality of the EDS-PO, the scenario is considered first in an emergency situation representing an immediate threat that requires Alert and Notification activities and then in a less time sensitive situation requiring deliberate Collaboration activities.

The general scenario is defined as:

> *A user is cued to a target of interest (TOI) that could pose a threat to the United States or US interests.*

3.5.2.1 Use for Alert/Notification

The EDS-PO will support emergency activities, such as finding people and/or organizations to alert or notify them of time sensitive activities. A generic emergency situation using the Alert/Notification business process is:

Alert/Notification - The user determines that the TOI is an emergency situation. The user requires contact information for relevant people and organizations that must be alerted or notified of the impending threat. The user conducts a structured search on selected search terms relevant to the TOI and the threat. The search result displays organizational contact information relevant to the TOI and the threat, including watch centers and continuity of operations (COOP) contact information. The results would also display contact information for people with expertise on the TOI and threat. In the case of the emergency situation, the organizational contact information is most relevant to the user. If the user does not have appropriate credentials, based on security level of the system and user, the search results may only contain organizational contact information with at least one method of contact. With the contact information in hand, the user can now execute the Alert/Notification business process.

3.5.2.2 Use for Collaboration

The EDS-PO will support deliberate efforts such as analysis, information fusion and investigation. A deliberate scenario using the Collaboration business process is:

Collaboration - The user determines that the TOI does not require emergency actions and decides to collaborate with people having relevant expertise. The user conducts a search for a known expert. A keyword search on terms relevant to the TOI and threat returns contact information for people and organizations in that community of interest. The

search results would also contain COOP contact information, as well as watch centers. The user in the deliberate scenario would find the contact information for a named person most relevant. If the user does not have appropriate credentials, based on security level of the system and user, the search results may only contain organizational contact information with at least one method of contact. With the contact information in hand, the user can now execute the Collaboration business process.

3.5.2.3 Use for Decision Support and Action Coordination

The EDS-PO will support decision support with subsequent coordination activities. A scenario using the Decision Support and Action Coordination business processes is:

Decision Support – A user in a leadership role or someone acting on their behalf may wish to contact relevant people and organizations to develop courses of action and recommendations for action. The user needs to contact regional authorities that may have a role in any action taken on the TOI. This may include Regional Fusion Centers, State and Local law enforcement, Customs and other regional authorities. The user conducts a structured search on relevant criteria. The search result displays organizational contact information for those regional authorities, as well as COOP contact information if any. The search results would also contain information on people relevant to the search criteria used, but the organizational information would be most relevant to the user.

3.5.3 Specific Scenarios

3.5.3.1 Production

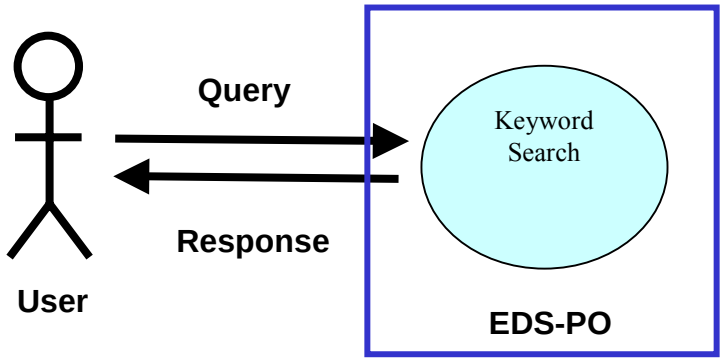


Figure 13: Use Case - Keyword Search

Usage Narrative: Conduct a Keyword Search
Fred, a staff member of a State Department of Homeland Security, is collecting information for a report on the potential impact of specific biological and chemical threats to the state's cattle population. He's particularly interested in learning more about the mortality rate of a highly contagious virus that is known to infect cattle. Fred brings up the EDS search page and selects the NIPF topic "Agriculture and Food Security" and hits the Submit button. Several hits appear – one being a scientist at an Army research lab in Maryland with listed expertise for "food animal pathogens." Fred clicks on the link and a window appears with a telephone number and an email address. Fred writes an email to the scientist explaining his reason in contacting him. In addition, Fred attaches a copy of his report abstract to the email. The scientist replies via email and indicates that he was only a minor participant during a series of tests three years ago, but that he knows two people at a Federal lab in New Mexico who are actively engaged in research. Fred types one of the names into EDS and three responses appear. He sees that one of the responses works at the lab in New Mexico and calls that person.

3.5.3.2 Notification

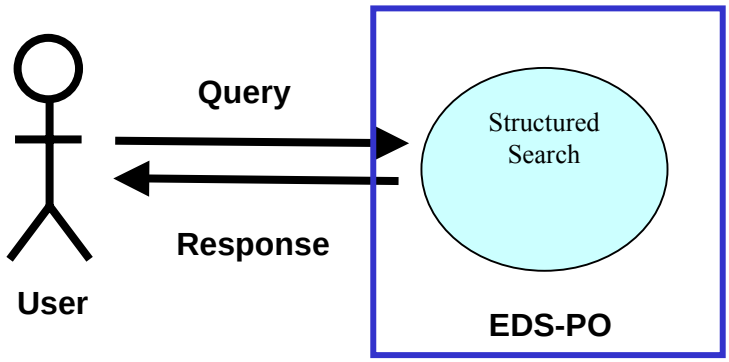


Figure 14: Use Case - Structured Search

Usage Narrative: Conduct a Structured Search
Bill, an analyst at a Federal agency, receives an alert regarding a target of interest about to dock in a foreign country. In order to coordinate a response to the target's arrival, Bill wants to alert US officials located in the country before the ship arrives in the capital city's port. Bill brings up the EDS search page and selects the "Structured Search" checkbox. This causes multiple attribute selection options to appear. Bill moves his mouse to the drop-down menu titled "Area of Expertise" and selects the NIPF topic "Illicit Drugs." Bill then moves to the menu titled "Current Duty Station" and selects the foreign country from the menu list. He clicks on the Submit button and three hits appear. Two are named personnel and one is an office of a US intelligence agency. Bill reviews the information summary for each hit and clicks on the link for the Lower Slobbovian FBI Legal Attaché. A contact window appears with an unclassified phone number, email address and a secure telephone number for the 24/7 watch officer at the U.S. embassy. Bill calls the unclassified phone number and the FBI agent answers.

4 Governance and Management

4.1 Roles and Responsibilities

The following roles and responsibilities for key stakeholders provide guidance for the next 9-12 months. These roles and responsibilities may change as the EDS-PO is integrated into the ISE.

4.1.1 Information Sharing Council (ISC)

- Understand and agree on the impacts of the EDS-PO CONOPS on existing directory services of record;
- Understand and agree on the components and services described by the EDS-PO CONOPS that will be provided by the EDS-PO;
- Select an Implementation Agent (IA) for each EDS-PO phase, where the IA ensures that ISC standards, policy and guidance are followed;
- Recommend policy directives to the Information Sharing Policy Coordination Committee (ISPCC) that must be implemented to facilitate the EDS-PO;[17]
- Approve this Concept of Operations for the EDS-PO;
- Approve the Implementation Plan for the EDS-PO; and
- Approve the Development, Modification and Enhancement (DME) roadmap recommended by the PMISE.

4.1.2 Information Sharing Environment Program Management Office

- Develop the EDS-PO CONOPS with input from participating department and agency representatives on the Strategy and Implementation Teams;
- Submit EDS-PO CONOPS and Implementation Plan to the ISC for approval;
- Maintain the DME roadmap to ensure interoperability across network security domains;
- Identify impediments to implementation and generate issue papers for ISC consideration;
- Chair EDS-PO Strategy Team and Implementation Team;
- Make policy recommendations to ISC for consideration;
- Oversee the implementation of the components and services described by the EDS-PO CONOPS that will be provided by the EDS-PO; and
- Periodically report EDS-PO metrics to the ISC.

4.1.3 ISE Participating Departments and Agencies

- Implement and execute the standards, policy and guidance set forth by the IA for each EDS-PO phase;

[17] See Memorandum to the Heads of Executive Departments and Agencies, Subject: *Guidelines and Requirements in Support of the Information Sharing Environment*. (December 16, 2005).

- Representatives on the PMISE Implementation Team will identify and nominate systems that in the short term meet some or all of the Mission Objectives in the Mission Objectives detailed in Chapter 3;
- Representatives on the Implementation Team will assist in the development of the Implementation Plan for Phase 1, Phase 2 and future EDS-PO implementation;
- Allocate resources to execute the Implementation Plan as determined by each agency, in conjunction with recommendations from the ISC and the Implementation Agent;
- Provide the best and most current contact and attribute information available;
- Maintain a process to update information shared in the EDS-PO in accordance with applicable laws; and
- Develop and publish internal business rules that determine what information can and cannot be shared in each security domain of the EDS-PO.

4.2 Performance Measures

Performance measures for Phases 1 and 2 focus primarily on quantifiable statistics that provide general information on usage and searches. User feedback mechanisms will provide data used to refine and enhance system capabilities. This is a preliminary list of possible measures. Measurement points, tools and roles have not yet been defined.

4.2.1 Technical Measures

- Number of user searches/time to recover trends in usage;
- Availability;
- Search response time; and
- Percentage of instances where responses contained cross-mission contacts.

4.2.2 Quality Measures

- Percentage of successful searches (responses to search elements);
- Percentage of time user search terms did not provide a positive response; and
- Percentage of instances when each structured search term is used and causes a positive response.

4.2.3 User Feedback Process

The PMISE will solicit feedback in order to develop iterative improvements for subsequent phases. Feedback methods include:

- PMISE will establish temporary, ad hoc “Mission Teams” to evaluate the deployed system and provide comments and suggestions;
- PMISE will develop online mechanisms, accessible from the EDS-PO search and result pages, to allow users to submit comments and suggestions; and
- PMISE will periodically survey various group of selected users. Sample questions might include the following:

- I use the system (daily, weekly, monthly, less than monthly);
- The amount of information provided is (too little, too much, just right);
- The information I receive is (never, sometimes, usually, always) accurate;
- The system is easy to understand and use? (yes, no); and
- If I could change one thing, it would be: (free-form entry).

4.3 EDS-PO Implementation

4.3.1 Community Outreach

PMISE will reach out to the CT user community to ensure that EDS-PO is adapted to meet new and changing mission requirements. PMISE user outreach will include performance measures and solicitation of user requirements. PMISE anticipates an implementation plan for the entire ISE will include an outreach program to meet the mission needs of the growing user base.

4.3.2 Training

PMISE recognizes that user training will be an important part of EDS-PO implementation. As the implementation details for each phase are defined, PMISE will develop training plans based on the needs of the user community. Training will be formalized and focused on learning objectives that test critical details of system use and user skills. Wherever possible, EDS-PO training will link into existing training programs.

4.3.3 Verification

To ensure that the various phases and versions of EDS-PO satisfy the stated requirements, the PMISE, in conjunction with stakeholders, will create ad hoc user groups to evaluate and verify each version of the system as it deployed. The user group will be disbanded after the verification and comment process is complete.

5 Conclusion

The EDS-PO CONOPS is a key step towards implementing an EDS directed by IRTPA. In focusing first on people and organizations within the Federal sector, it sets targets and establishes the basis for implementing immediate solutions. EDS-PO will be deployed in phases: Phase 1 by March 31, 2006 and Phase 2 to be implemented over the next 9 to 12 months. The EDS-PO CONOPS provides direction for implementing Phases 1 and 2 by identifying a definition of EDS-PO, including the concepts of Blue, Yellow and White pages, user requirements, data attributes, functional capabilities, and governance and management. The EDS-PO Implementation Plan builds on the EDS-PO CONOPS by specifying operational and functional details for the EDS-PO development and deployment. Future phases will be integrated with the ISE CONOPS. Experience gained from operating the EDS-PO will aid in efforts to further expand capabilities and the ISE as a whole.

Appendix A – Glossary and Acronyms

Attributes: Specific data entries associated with people and organizations. Such data entries will perform one or more of the following functions:

- Identify people or organizations
- Provide search characteristics
- Enable management of the EDS-PO

Counterterrorism (CT): The practices, tactics and strategies that governments, militaries and other groups adopt in order to neutralize terrorist operatives in the U.S. and to dismantle terrorist networks worldwide.

Current Capabilities Matrix: Spreadsheet of directory systems currently in operation, development, or planned within the Federal sector.

Electronic Directory Services – People & Organizations (EDS-PO): A set of registries that share a common, trusted and up-to-date view of people and organization information, which includes identification of necessary attributes, desired attributes and standardized metadata on people and organizations, to assist in locating in the Federal Government people with relevant knowledge about intelligence and terrorism information.

Information Sharing Council (ISC): The ISC is an interagency forum established by Section 1016 of IRTPA and Executive Order 13388 and operating under a Charter approved by the ISPCC. It is an advisory body to the President and PM in the development of policies, procedures and guidelines necessary to implement the ISE. Additionally, it provides participants an avenue to actively engage in implementation planning and decision-making for the establishment of an effective ISE. The Council also acts as a mechanism to ensure coordination among Federal departments and agencies and is a means for the PM to assess progress among ISE communities. The ISC was recently directed to establish two sub-committees to address State, Local and Tribal as well as private sector issues. These subcommittees will be co-chaired by DHS and DOJ.

Information Sharing Environment (ISE): an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section.

Information Sharing Policy Coordination Committee (ISPCC): Established by the President in June, 2005, the ISPCC is chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC). It has the responsibilities set forth in Section D of Homeland Security Presidential Directive-1 and other relevant presidential guidance with respect to information sharing. The ISPCC was established to address major information sharing policy issues, including the resolution of issues raised by the PM and provide policy analysis and recommendations for consideration by the more senior committees of the HSC and NSC systems.

Private Sector (PS): Non governmental organizations such as commercial and academic entities.

Program Management Office (PMO): Staff supporting the Program Manager. The PM's Office is supported by an experienced staff from across the U.S. Government. Supporting personnel include several advisors with expertise in specific information sharing issues, e.g., State and Local information sharing and technology standards.

Program Manager: The PM will build upon current information sharing efforts across the U.S. Government and facilitate change toward tomorrow's ISE, engaging the ISC in the implementation process through continuous communication, interaction and inclusion in decision-making processes. The PM will act as the catalyst to improve terrorism information sharing among ISE communities by working with them to remove barriers and facilitate change to improve information access.

Sharing Initiatives Matrix: Spreadsheet of directory systems currently in operation within the Federal sector which provide information across organizational lines

Stakeholder: The EDS-PO principal stakeholders are those organizations that will provide their directory information to the EDS-PO.

State, Local and Tribal (SLT): Non-Federal public sector, including government, police, justice and health and human services, that are involved in or could be impacted by CT.

Appendix B – National Intelligence Priorities Framework

The National Intelligence Priorities Framework (NIPF) is used by the President to prioritize the intelligence needs of the United States. The following table contains the NIPF Intelligence Topics (IT). These are high level intelligence related topic areas that are prioritized and broken down into detailed intelligence needs.

Advanced Conventional Weapons Development and Proliferation
Agriculture and Food Security
Arms Control and Treaty Monitoring
Baseline
Counterintelligence
Cyber Threats to US Infrastructure
Democratization and Political Stability
Demographics, Migration and Population Movements
Economic and Financial Stability
Emerging and Disruptive Technologies
Energy Security
Environment and Natural Resources
Foreign Denial and Deception
Foreign Military Combat Capabilities, Operations and Intentions
Foreign Policy Objectives and Relations to the US
Foreign Space Threats and Operations
Homeland Security
Hostile Foreign Military Combat Capabilities, Operations and Intentions
Human Rights and War Crimes
Humanitarian Disaster and Relief Operations
Illicit Drugs
Infectious Disease and Health
International Organized Crime
Military and Civilian Infrastructure
Money Laundering
POWs and MIAs
Regional Conflicts and Crises
Terrorism
WMD Development and Proliferation • Biological Weapons • Chemical Weapons • Missiles • Nuclear

Appendix C – Current Capabilities Matrix

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
1	ADEX Phase I - Active Directory/ Exchange	DHS CIO	Dave Jones David.L.Jones@uscg.dhs.gov (703) 313-5526	No (in progress)	-Component of DSES system above -Global Address List (GAL) for all of DHS -Metadirectory -Capable of sharing data with Active Directory and other Enterprise databases	X	Limited			LDAP, SSH, Lotus Notes Connectors		O	Program	None	SBU	Microsoft Identity Integration Server (MIIS), Microsoft SQL Server		
2	DSES - Directory Services and Email System	DHS CIO	Dave Jones David.L.Jones@uscg.dhs.gov (703) 313-5526	Yes	Provides: -Directory services -White Pages via http://directory.dhs.gov/ -Assigns uniform “@dhs.gov” to all employees -Routes email to, from, and between all DHS Components and the Internet -Anti-virus and Anti-SPAM protection	X	Limited			LDAP, SMTP, ESMTP, HTTP, FTP, SSH, X.500, DNS	RFC822, RFC2822	O	Program	None	SBU	Syntegra email and directory, Sophos Anti-Virus and Anti-Spam		
4	Terrorist Identities Datamart Environment (TIDE)	NCTC	Robert Cranston (571)280-5616	Yes, CIA IPC	TIDE is the official USG repository of international terrorist identities. TIDE provides comprehensive identity information and real-time information on terrorists to NCTC analysts and other key customers. TIDE is a key component of the terrorist watchlist process. TIDE is made up of a full access system (TIDE Prime) and a web-access system with reduced functionality	X	X			TWPDES, XML	TWPDES	O	SOR		ADN and JWICS	Officiall USG Repository of Terrrorist Identities. Official Identity and Alias relationship Official Identity and alias spelling	APP - Web app server MWARE - BEA WebLogic Data - Oracle with SAN	
5	CLASSNET	State Dept	IRM/IA	State CIO (?)	State Department's Classified Network (CLASNET) is a global Secret-high system for use by the Foreign Affairs Community. 20000+ employes world wide (rough estimate). State Dept and Foreign Affairs Agencies. Office Work Suites, Email, Web Intranet Browsing, SIPRNET connectivity	X	X			SMTP, HTML, HTTP, XML, Active X	CNSS issuances	O	Base Program Funded	Need-to-know.			MicroSoft Office, Oracle, and OS (e.g., XP)	

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
6	HR Connect	Treasury	Carl Wylie	C&A completed	Personnel listing of all Treasury employees. Ties to LDAP with contact info as well as e-mail addresses.	X	X			PeopleSoft, Oracle, LDAP	LDAP	O	Funded Program	Excellent for name listings and some attributes. Would have a problem listing degrees of proficiency (high, medium, low skill) and would not have capability to list databases or other useful systems.	Unclass	swern.gov. Southwestern critical response network. Possible expansion to national.		
7	Active Directory	DoS	Dion Herbert (202) 203-7400	Y	Global Address List and authentication directory. Utilizes MicroSoft AD	X	X			LDAP,	Windows 2003	O	Program		SBU/Classified			
8	DoS Web Phone Directory	DoS	Aaron Jackson (202) 647-8662		Searchable Web site with orgainizations and people http://www.state.gov/business/	X	X	X		HTTP		O	Program	(ISE PM) Limited phone list to division chiefs.	Internet/SIPRNET			
9	Intelink	DNI CIO	Intelink Management Office	Yes	Organizational Pages/ Points of Contact (POCs) – a directory of organizations that have information spaces registered with the Intelink Management Office (IMO). The listing is updated every twenty minutes with the last known operational status of each server. POC information is provided for non-operational servers	X	X	X				O	Funded Program		TS S			

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
10	Intelink	DNI CIO	Intelink Management Office	Yes	OSIS Point of Contacts listed alphabetically noting their organization, OSIS responsibilities, unclassified email and unclassified phone number	X	X					O	Funded Program		SBU			
11	Intelink	DNI CIO	Intelink Management Office	Yes	OSIS Account Management Interface - web site where users maintain their own point of contact information.	X	X					O	Funded Program		SBU			
12	Intelink	DNI CIO	Intelink Management Office	Yes	Find a registered home page – an application which supports searches for servers and home pages registered with the IMO	X	X					O	Funded Program		TS S			
13	Intelink	DNI CIO	Intelink Management Office	Yes	Find a person link for searching the IC common White Pages of contact information for people within the Intelligence Community.	X	X	X				O	Funded Program		TS			

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
14		DNI CIO	Intelink Management Office	Yes	Find a person - link to ISMC 411 which contains in excess of 105,000 entries about people and organizations easily accessible via LDAP. Intelink-S Specific Intelink-S links to directory information on persons and organizations: 66th Military Intelligence Group (persons; phones and email) Counter Drug Intelligence Systems (CDIS) (organizations; phones) DEA MERLIN Address Book (persons;e-mail and phones) DEA Intelligence Division (persons,organizations;phones) El Paso Intelligence Center (EPIC) (persons;e-mail and phones) FBI Contacts List (persons;e-mail and phones) Houston JDIG Contacts (persons;phones) NDIC Contacts (persons,e-mail and phones) DIA Office for CounterDrug	X	X	X	X			O	Funded Program		S			
15	Intelink	DNI CIO	Intelink Management Office	Yes	Specific Intelink-SBU links to directory information on persons and organizations: Department of State and USAID oPAL	X	X	X				O	Funded Program		SBU			
16	Intelink	DNI CIO	Intelink Management Office	Yes	Google Search – the same search technology that has made Google.com the most popular search engine on the Internet is available on Intelink. “Pull” capability based on key word input. Intelink-TS, Intelink-S, Intelink –SBU (2006)	X	X	X	X			O	Funded Program		TS S SBU	DNI Best Practice		

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
17	Intelink	DNI CIO	Intelink Management Office	Yes	Dispatcher - makes the realtime nature of ICDS possible. It allows producers to notify Intelink search engines of new, modified, or deleted products automatically, supporting . Dispatcher gets the updates into the Intelink search engines immediately, as opposed to the time it takes Google to crawl Intelink. It is a convenient method for producers to ensure their new and changed content is available to search engine users immediately.	X	X	X	X			O	Funded Program		TS S			
18	Intelink	DNI CIO	Intelink Management Office	Yes	Intelligence Community Collaborative Presence features the use of InfoWorkSpace (IWS) collaboration tool offering the following IWS capabilities: instant messaging, controllable presence information, text and audio chat, shared whiteboard, text editor, personal file storage, collaborative spaces (building, floors, rooms), persistent room tools and a conference center	X	X	X				O	Funded Program		TS			
19	Intelink	DNI CIO	Intelink Management Office	Yes	Intelligence Community Instant Messaging - offers a secure, scalable open standards based user friendly IM capability to connect people to people through integration with the Directory Services	X	X					O	Funded Program		TS			
20	Intelink	DNI CIO	Intelink Management Office	Yes	Blogging – provides a freewheeling unconstrained personal or group journaling capability.	X	X	X	X			O	Funded Program		TS S SBU			

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
21	Intelink	DNI CIO	Intelink Management Office	Yes	Intelink Forums – exist as a web based capability for users to create discussion threads, where questions can be asked and responses provided.	X	X	X	X			O	Funded Program		TS S SBU	DNI Best Practice		
22	DoD Metadata Registry	DOD	Dr. Glenda Hayes, glenda.hayes.ctr@disa.mil	Yes	Existing registry of approved DOD data types	X	X	X	X			O	Funded Program			DoD Best Practice		
23	Scattered Castles	DNI CIO	Carl Foerster	Yes	Directory of People and Security Clearances	X	X			Database	Database	O	Program	Restricted Access		JWICS	Oracle Database	
24	IC Full Service Directory	DNI CIO	Bob Wrede	Yes	IC Directory Service- Major contributors are CIA, NSA, DIA/DODIIS, NGA, IMO (Community Services	X	X		NO	LDAP	LDAP	O	Program Funded by DNI/CIO	Authoritative data for various Agency population				
25	Common Services Full Service Directory	DNI CIO	Bob Wrede		Common Services Border Directory supports those agencies or commands not covered by any of the other major border directories: CIA, NSA, DIA, NRO, NGA	X	X	Is used to support services	NO			O	Program Funded by DNI/CIO	Authoritative data for various Agency population	Agency Population of Data	JWICS	Oracle Database	
26	USP3	DHS/FBI	Art Fierro, DHS/HSOC, Art.Fierro@HQ.DHS.GOV, (202)329-5669	?	Alert and collaboration service; active membership of 40,000+ first responders; potential to be used as "credential service provider" to reach DHS or FBI data services	X	X			HTTP/HTTPS	LAMP - (open source)	O	Program		SBU			

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
27	NCTC Online (NOL)	NCTC	Robert Cranston (571)280-5616	Yes, CIA IPC	NOL provides a secure web-based searchable repository of terrorism related products to audiences on multiple networks. Views of the products are filtered appropriately for each users accesses and group memberships. Additionally, NOL provides collaboration capabilities that facilitate communication among mission partners across organizations.	X	X	X		PKI,XML, JAVA, PERL	Identity mngmt Access Mgmt PKI	JWICS - O STGH - O SIPR - O SBU - D(IOC)	SOR	Need to know Secure enclave with HCS and PKI Reqt for high side, limited use for other networks currently, although moving towards a more open approach for the future (protected and unprotected zones)	JWICS, SIPR, STGH, SBU	Largest Collection of CT Domain personnel Secure enclave with enhancedaccess control and auditing Cannhandle data at HCS Has presence at all 3 primary network domains	APP - Web app server MWARE - BEA WebLogic Data - Oracle with SAN	
28	Cyber Identity Management (CIM) service	DHS	Martin Smith, DHS/OCIO, martin.smith@dhs.gov	?	Departmental access-management service, serving internal (DHS) and external applications. Service will also publish a "White Pages" of included employees and contractors; service is designed to "federate" via SAML with non-DHS services	X	X			SAML, HTTP; LDAP	SAML, HTTP; LDAP	D	Program		SBU			
29	DOS PKI	DoS	Sally Caldwell (202) 203-7808	Y	Certificate system for buidling and system access. Built on Entrust	X				X509		O/D	Program		SBU			
30	DoD PKI	DOD	Shawn O'Brien, shawn.obrien@disa.mil, 410-854-4913	Yes	PKI Certificate for Authentication of People and Components	X		X				O	Funded Program		SBU/SIPRNET			
31	DOJ-DHS Global Address Lists	DOJ-DHS	Barbara Brown, DOJ	Yes	Contact information for DOJ & DHS employees exchanged and available in (Outlook) address lists	X				LDAP		O	Program		SBU			
32	LEO Directory	DOJ/FBI/ CJIS	Scott Lamoreaux, FBI/CJIS	?	Contact information for LEO users (~50K local, state, & federal law enforcement)	X						O	Program					
33	RISS Directory	Independent - funded by DOJ grants	George March, RISS	Not required	Contact information for RISS users (primarily local & state law enforcement)	X						O	Recurring DOJ grants					

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
34	DOJ-FBI Secret Global Address Lists	DOJ, FBI	Jeff Cotter, DOJ	Yes	Contact information for FBINet and (rest of) DOJ classified (S) domain accounts exchanged and available in (Outlook Active Directory) address lists	X				LDAP		O	Program					
35	HR Online	Dos	HR Helen Daniels 202-663-3727	Y	Database of DoS federal employees and their expertise.	X				XML		O	Program		SBU			
36	E*Phone	DoS	Michael Bishton (703) 875-7422		The e*Phone Directory is an on-line, Browser-Based employee locator service.	X				HTTP		O	Program		SBU/Classified			
37	DS Badge	Dos	Tony Mosley (703) 923-6822		Database of all DoS govt & contractors with clearance information. Access control to facilities	X						O	P		SBU/U			
38	AF PKI Implementation (GCSS AF)	DOD	Maj Dave Gindhart, AFXOI, david.gindhart@pentagon.af.mil	Yes	Large scale authentication service with edge caching	X					WS Security, SAML, XACML	O	Funded Program			DoD Best Practice		
39	CIA PKI	CIA	John Saunders	Yes - Internal	PKI Certificates	X		X		TCP/IP, LDAPS, HTTP, HTTPS		O		Internal use only; policy; no expertise listed				
40	Enterprise Directory Service (JEDS)	DOD	Dot Blain, blaind@ncr.disa.mil	No	People Discovery and Support of attributes for people	X					LDAP (GDS)	D	not funded		SBU/SIPRNET	JEDS has a federated structure		
41	Federal White Pages	?	Martin Smith, DHS/OCIO, martin.smith@dhs.gov	N	CONCEPT ONLY: Ressurrect former Federal White Pages electronic directory, based on synchronization of existing agency LAN and e-mail directories	X						Concept	None: Estimated resources required ~ $500K		Public or SBU			
42	Pegasus Directory	Independent - funded by DOJ		Not required	POC information for local, state, and federal law enforcement organizations/offices		X				web ui	O	DOJ grants					
43	FirstGov.gov	U.S. GSA	FirstGov	Yes	FirstGov.gov, the official U.S. gateway to all government information, is the catalyst for a growing electronic government. Our work transcends the traditional boundaries of government and our vision is global–connecting the world to all U.S. government information and services.		X	X				O	Funded Program		Public			

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
44	Terrorist Group/Entity Name Assistance System TGENASys	NCTC	Robert Cranston (571)280-5616	No, in progress - CIA IPC	Terrorist Group/Entity Name Assistance System (TGENASys) is a web-based service repository and deconfliction service for other information systems to incorporate the NCTC approved spellings of terrorist group names. TGENASys is designed to provide lookup functions via standard protocols for poulating data lists where data integrity is required.		X				TWPDES	D	OTF					Name Lookup Deconfliction repository approved lists
45	Web page of State & local "Fusion Centers"	DHS + ?	Martin Smith, DHS/OCIO, martin.smith@dhs.gov	N	CONCEPT ONLY: simple listing of contact info for State and local Fusion and Emergency Operation Centers. Listing has been compiled and is available in document form.		X			HTTP/HTTPS	HTTP/HTTPS	CONCEPT. Estimated IOC 30 days	None. Est. resources required <$100K	Funding; sponsor/operator	Public or SBU			
46	Web page listing of Federal Agency Information Sharing POCs	ISE PM		N	CONCEPT ONLY: Publish listing of "Federal agency info sharing POC" based on results of 12.2005 ISC tasking to agencies.		X					Concept	None: Estimated resources required ~ $100K		Public or SBU			
47	Air Force Directory Service Program	DOD	Maj Dave Gindhart, AFXOI, david.gindhart@pentagon.af.mil	Yes	Ties legacy AF directories across AF Major Commands and programs; supports attributes				X		LDAP	O	Funded Program		SBU	DoD Best Practice		

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
48	Intelink	DNI CIO	Intelink Management Office	Yes	Intelink Topic Directory - is a service mean to be similar to the directory on the GOOGLE home page, the "Find it Fast" listings on AOL and similar capabilities on MSN and Yahoo. These directories provide users a listing of Internet topics organized by categories. For many situations, a topical "look-up" is faster than searching on keywords. This directory is designed to provide a logical place to store and find information on specific topics. The categories have been carefully compared with existing categorization systems used in the CIA World Factbook, Intelligence Function Codes (IFC) and the National Intelligence Priorities Framework (NIPF) to ensure their applicability throughout the community. The Directory, while still a work in progress, contains an initial set of key							O	Funded Program		TS S SBU	DNI Best Practice		
49	Intelink	DNI CIO	Intelink Management Office	Yes	MetaCarta Geographic Text Search – characterizes data in a geo context making geospatial information in unstructured documents, text, and databases searchable. “Pull” capability based on key word input.				X			O	Funded Program		TS S			

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
50	Intelink	DNI CIO	Intelink Management Office	Yes	Inteligence Community Delivery Service – collects and organizes new intelligence products for delivery as they are published, enables browsing and searching by region, country, and subject, and provides customizable profiles and realtime delivery of new products matching user profile(s). It gives open access to browsing and searching, but requires an account for saving profiles and setting display preferences. Content comes from Google, Dispatcher, and IntelReader. ICDS accounts are ICPKI certificate-based, because secure COI content will eventually be included for authorized users							O	Funded Program		TS S SBU	DNI Best Practice		
51	GLOBAL XML metadata registry	DOJ	DOJ OCIO	?					X			O	Program		Public			
52	CASPER	DNI CIO	Lora Voas	Yes	Application, Service and Protocol List			X	X	List	List	O	Program			JWICS	Excel Spreadsheet	
53	NCES	DOD	Col Gary Langston, gary.langston@disa.mil	No	Service Discovery			X			UDDI, WSDL	D	Funded Program		SBU/SIPRNET			
54	NCES	DOD	Col Gary Langston, gary.langston@disa.mil	No	Content Discovery				X		WSDL, SOAP,	D	Funded Program		SBU/SIPRNET			
55	DHS Metadata Registry	DHS	Brad Eyre, DHS OCIO	N	In-development registry of approved DHS data types and data-exchange schemas				X			D	Program		Public or SBU			

Existing EDS Initiatives/Capability Matrix

	Name	Dept/ Agency	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain	Strengths Associated	Core Technical Components	Mission Capabilities
56	Intelink	DNI CIO	Intelink Management Office	Yes	Wiki's – (under development) are very simple web sites where users can very quickly and easily create HTML through web browsers. Wiki's allow "open editing" where users can edit any of the content creating self correcting bodies of knowledge.							D						
57	Initial ISE Services Directory	DOD & DHS?	Martin Smith, DHS/OCIO, martin.smith@dhs.gov	N	CONCEPT ONLY: Field UDDI Services Directory in SBU ISE (Extranet)			X		HTTP/HTTPS, UDDI	HTTP/HTTPS, UDDI	CONCEPT. Estimated IOC 90 days	None. Est. resources required <$300K		Public or SBU			
58	Web page listing of "Terrorism Information Systems"	ISE PM		N	CONCEPT ONLY: Publish listing of "terrorism information systems" based on "system inventory" conducted by OMB & ISE PM.			X				Concept	None: Estimated resources required ~ $100K		Public or SBU			
59	Web page listing of major terrorism-related data collections	DHS + ?		N	CONCEPT ONLY: Gather and publish high-level inventory of major Federal agency data collections. Intended use is to increase awareness of resources and provide ocntat info for potential users.				X			Concept	None: Estimated resources required ~ $500K		Public or SBU			

Appendix D – Current Sharing Initiatives Matrix

EDS Sharing Initiatives/Capability Matrix

Name	Owner	Partner Dept/ Agency	Systems/ Capabilities connected	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain
Intelink	DNI CIO	IC			Yes	Organizational Pages/ Points of Contact (POCs) – a directory of organizations that have information spaces registered with the Intelink Management Office (IMO). The listing is updated every twenty minutes with the last known operational status of each server. POC information is provided for non-operational servers	X	X	X		HTML		O	Program		TS/SCI
IC Full Service Directory	DNI CIO	DOD	DODIIS-IC FSD	Bob Wrede	Yes	White Page Directory of IC members	X	X			LDAP	LDAP	O	Program	Authoritative data for various Agency population	TS/SCI
DOJ-FBI Address Lists	DOJ	FBI	DOJ Secret (JCON-S) Outlook Directory + FBI Secret (FBINet) Outlook Directory	Jeff Cotter, DOJ (Jeff.Cotter@usdoj.gov, 202-305-3178)	Yes	Names, telephone numbers, and email addresses are exchanged between DOJ Secret (JCON-S) and FBINet Global Address Lists. The information is then available for access through each organization's email client and/or address book application (DOJ: Outlook & Address Book).	X					LDAP	O	Program	Not all FBINet accounts being exchanged (only those mapped to SIPRNET addresses - ~8000 so far)	Secret
Intelink	DNI CIO	IC			Yes	OSIS Point of Contacts listed alphabetically noting their organization, OSIS responsibilities, unclassified email and unclassified phone number	X	X					O	Funded Program		SBU

EDS Sharing Initiatives/Capability Matrix

Name	Owner	Partner Dept/ Agency	Systems/ Capabilities connected	POC	C&A	Description	People	Org	Services	Data	Protocols Used	Standards Used	Status (Operational, Development, Planned)	Funded (One-time, Program, System of Record)	Impediments	Domain
DOJ-DHS Global Address Lists	DOJ	DHS	DOJ Outlook Directory + DHS Outlook Directory	Barbara Brown, DOJ (Barbara.A.Brown@usdoj.gov, 202-353-8754)	Yes	Names, telephone numbers, and email addresses are exchanged between DOJ and DHS Global Address Lists. The information is then available for access through each organization's email client and/or address book application (DOJ: Outlook & Address Book). DHS data includes over 7000 HQ employees.	X					LDAP	O	Program	Incomplete data (phone numbers only present on ~50% of records); Not all DOJ components have access to the address book (on separate email systems).	SBU
DOJ-DHS Global Address Lists	DOJ	DHS	DOJ Outlook Directory + DHS Outlook Directory	Barbara Brown, DOJ	Yes	Contact information for DOJ & DHS employees exchanged and available in (Outlook) address lists	X					LDAP	O	Program		SBU
USP3	DHS/FBI	SLT, PS, and Federal		Art Fierro, DHS/HSOC, Art.Fierro@HQ.DHS.GOV, (202) 329-5669		Alert and collaboration service; active membership of 40,000+ first responders; potential to be used as "credential service provider" to reach DHS or FBI data services	X				HTTP/HTTPS	LAMP - (open source)	O	Program		SBU
Enterprise Directory Service (JEDS)	DOD	Dot Blain, blaind@ncr.disa.mil			No	People Discovery and Support of attributes for people	X					LDAP (GDS)	D	not funded		TS/SCI, Secret, SBU
Terrorist Group/Entity Name Assistance System TGENASys	NCTC			Robert Cranston (571)280-5616	No, in progress CIA IPC	Terrorist Group/Entity Name Assistance System (TGENASys) is a web-based service repository and deconfliction service for other information systems to incorporate the NCTC approved spellings of terrorist group names. TGENASys is designed to provide lookup functions via standard protocols for poulating data lists where data integrity is required.	X	X			TWPDES		D	OTF	Name Lookup Deconfliction repository approved lists	TS/SCI