



INSTITUTE FOR DEFENSE ANALYSES

Information Sharing and Collaboration Business Plan

LTG Peter A. Kind, USA, Ret., Task Leader

J. Katharine Burton

June 2005

Approved for public release;
unlimited distribution.

IDA Document D-3206

Log: H 05-002001

This work was conducted under contracts DASW01 04 C 0003 and W74V8H 05 C 0042, Task ER-5-2370, for the Department of Homeland Security, Information Sharing and Collaboration Office. The publication of this IDA document does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

© 2005, 2006 Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (NOV 95).

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-3206

**Information Sharing and Collaboration
Business Plan**

LTG Peter A. Kind, USA, Ret., Task Leader

J. Katharine Burton

Preface

This document was prepared by the Institute for Defense Analyses (IDA) under the task order Homeland Security Information Technology Strategy Analyses. Information Sharing and Collaboration (ISC) across an organization as large and diverse as DHS is a daunting challenge. ISC across the full range of stakeholders throughout all government agencies and levels, private sector and cooperating allies and at appropriate levels of information security classification approaches being intractable. None-the-less, it must be done to accomplish effective homeland security.

This Business Plan focuses on ISC internally in the Department of Homeland Security, addresses ISC with its key stakeholder partners and provides recommended actions to proceed.

The following IDA research staff members were a reviewer of this document: Dr. Bill Brykczynski, Ms. Vivian A. Cocca, Ms. Marilee O. Cunningham, and Dr. L. Roger Mason, Jr.

Contents

Executive Summary	ES-1
1 Introduction.....	1
1.1 Purpose	1
1.2 Background.....	1
1.3 Mission and Goals	3
2 TO-BE (Where We Want to Go).....	5
2.1 Information Sharing Vision.....	5
2.2 Collaboration	6
2.3 Users	10
2.4 Information Sources	11
2.5 Services.....	11
2.6 Seamless Environment	12
2.7 Resourcing.....	14
2.8 Design Considerations	14
2.9 Functional Requirements	15
3 Where We Are Now (AS-IS)	19
3.1 Existing capabilities in the DHS Enterprise IS&C Environment	19
3.1.1 Existing DHS Architectures and EA Efforts.....	20
3.1.2 Data Resources	22
3.1.3 Sources of Information	23
3.2 Analysis of As-Is Capabilities	24
3.2.1 Gaps and Overlaps.....	24

3.2.2 As-Is Issues.....	26
3.2.2.1 Governance.....	26
3.2.2.2 Standards and Policies	26
3.2.2.4 Cultural Resistance.....	27
3.2.2.4 Resources.....	28
3.2.2.5 Access and Dissemination Control.....	29
3.2.2.6 Collaboration	29
3.2.2.7 Architecture Issues.....	30
3.2.3 Security (Information Assurance)	37
3.2.4 Needs Analysis.....	38
3.3 Law and Policy	39
3.3.1 Context	39
3.3.2 Process.....	39
3.3.3 Control and Ownership.....	42
3.3.4 Constraints.....	42
3.3.5 Sources	43
4 Implementation Plan (Roadmap)	45
4.1 Strategy.....	45
4.1.1 Planning, Management, and Oversight.....	45
4.1.1.1 Federated Governance.....	45
4.1.1.2 Portfolio Management.....	47
4.1.1.3 Phased Acquisition	47
4.2 Critical Success Factors.....	48
4.2.1 Cultural.....	48
4.2.2 Value of Information Sharing and Collaboration	50
4.2.3 Other Critical Success Factors.....	51

4.3	EO 13356 and IRPTA Requirements	53
4.4	DHS Additional Needs and Specific Actions	62
4.4.1	Immediate (0-6 months)	62
4.4.2	Near Term (6-18 months)	62
4.4.3	Mid-Term (18-36 months)	62
4.5	ISC Capability Maturity Model	62
4.6	Moving Forward – DHS Enterprise	64
4.7	Recommended Actions	66
5	Risk Management	69
5.1	Overview	69
5.2	Risk Management Process Procedures	69
5.2.1	Responsibility/Organization	70
5.2.2	Risk Management Procedures	70
5.2.3	Risk Planning	70
5.3	Risk Assessment (DHS Info sharing Risk Matrix)	70
5.4	Risk Mitigation	71
5.5	Risk Monitoring	72
6	Summary	73
Annex A	References	A-1
Annex B	Acronyms	B-1
Annex C	Glossary	C-1
Annex D	From Enabling Information Sharing to Facilitating Community Collaboration	D-1
Annex E	DHS Response to OMB Data Call	E-1
Annex F	eSurvey Information Sources and Products (published separately)	
Annex G	System of Record Notices (published separately)	
Annex H	Selected System and Project Summaries (published separately)	

Figures

Figure 1.	Data to Meaning Hierarchy	ES-2
Figure 2.	From Data Through Collaboration to Coordinated Action.....	ES-2
Figure 3.	Information Needed to Govern and Protect	ES-4
Figure 4.	Information Sharing and Collaboration Maturity Model	ES-9
Figure 5.	From Data Through Collaboration to Coordinated Action.....	7
Figure 6.	Advanced Collaboration Cycle	8
Figure 7.	Seamless Environment	13
Figure 8.	Value Chain	21
Figure 9.	Mapping of DHS Systems to Strategic Goals	22
Figure 10.	Sources of Homeland Security Information	24
Figure 11.	COP Survey, E-Survey, Enterprise Architecture Gaps and Overlaps ..	33
Figure 12.	Federated Approach	46
Figure 13.	Portfolio Management	47
Figure 14.	Information Sharing and Collaboration Capability Maturity Model ...	63
Figure 15.	Risk Management Process	70

Tables

Table 1.	Functional Requirement Definitions.....	16
Table 2.	Existing Environment in Terms of Functional Requirements.....	19
Table 3.	Functional Requirements Gaps and Overlaps.....	24
Table 4.	DHS Information Sharing Policy Framework	44
Table 5.	ISC Phased Approach Overview.....	61
Table 6.	DHS Information Sharing Risk Matrix.....	72

Executive Summary

Intelligence and Information Sharing for a 21st Century Department

On the most basic level, we need to take a step back and focus on the fundamental question: Why was the Department of Homeland Security created? It was not created merely to bring together different agencies under a single tent. It was created to enable these agencies to secure the homeland through joint, coordinated action. Our challenge is to realize that goal to the greatest extent possible.

*Let me tell you about three areas where I plan to focus our efforts to achieve that goal. First, we need to operate under a **common picture of threats** we are facing. Second, we need to **respond actively** to these threats with the **appropriate policies**. Third, we need to **execute** our various **component operations in a unified manner** so that when we access the intelligence and we have decided upon the proper policies, we can carry out our mission in a way that is coordinated across the board .*

Secretary Chertoff, *Statement for the Record Before the United States Senate Subcommittee on Homeland Security*, 20 April 2005.

The *sine qua non* that enables success in all three areas identified by Secretary Chertoff is information sharing and collaboration. A better intelligence process alone is not sufficient. A **common picture of threats** is impossible without sharing throughout the intelligence and information domains. **Active and appropriate policy response** can only be accomplished well with sharing across the domains of intelligence, emergency responders, law enforcement, and homeland security. **Unified execution of component operations** mandates sharing across all activities involved.

Information Sharing and Collaboration. A common information requirement has been simply defined as the right information in the right amount in the right place at the right time. Effective use of information is far more complex. The hierarchy from data to understanding, knowledge and meaning involves levels of information and input.

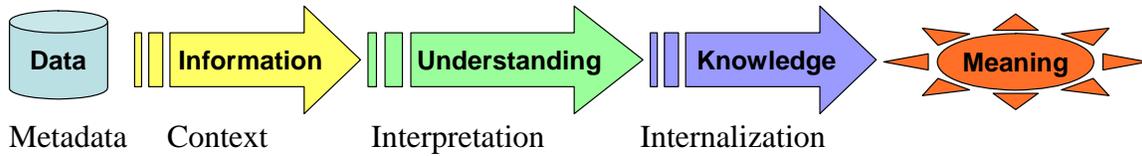


Figure 1. Data to Meaning Hierarchy

Metadata (information about information) helps increase accuracy and extends data use, while context and circumstances help turn the data into information. The interpretation of that information by communities with specific backgrounds and expertise leads to understanding. The process of internalizing these new interpretations of information in context leads to the creation of new knowledge. Knowledge and meaning on an individual basis enable individual action. Information sharing implies availability in multiple places but information sharing alone is not effective without context and mutual understanding. Experts may argue about at which level or at how many levels the sharing should take place, but the objective is to jointly construct shared knowledge, enabling meaning and unified action.

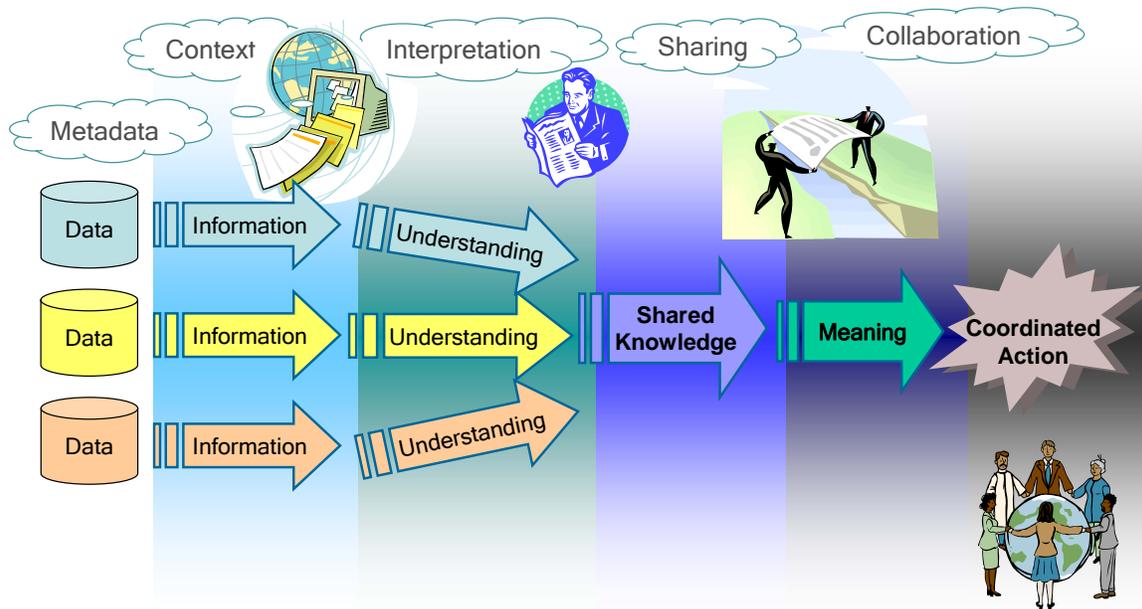


Figure 2. From Data Through Collaboration to Coordinated Action

Structured data is individually interpreted and internalized in context. Communities share that information, enabling them to collaboratively construct meaning and take coordinated action.

Collaboration adds the richness of context, sharing and questioning, opposing viewpoints and considerations, legal, technical and logistical limitations, rapid access to experts, modeling and simulation insight, and the common understanding that enables the components to operate in a unified manner. Facilitating knowledge sharing across communities of interest that do not yet have established processes for information sharing involves creating the infrastructure, mindset, and tools needed to support a new culture of collaboration and sharing. A number of different factors influence community members' participation, involvement, and the eventual success of the collaboration. These include the degree to which users are aware of the various communities, information, and knowledge available in the environment (awareness), the ease of finding useful information in a timely manner (structure), and whether or not they perceive an immediate benefit from collaborating with others (motivation).

Vision.

Vision of an Interoperable Terrorism Information Sharing Environment

The vision of the interoperable terrorism information sharing environment, created and maintained in full partnership by all levels of Government, effectively supports detection, prevention, disruption, preemption, and mitigation of the effects of terrorism against the territory, people, and interests of the United States of America. It does so by enabling the interchange of terrorism information among and between appropriate Federal, State, Local, tribal, and territorial authorities, foreign partners and the private sector. It will support the ability of agencies to acquire additional such information, and, it will protect or enhance the freedom, information privacy, and other legal rights of Americans in the conduct of their activities. (*Information Sharing Council, December 20, 2004*)

Scope. *The information landscape has been considerably enlarged since 9/11.* In addition to national intelligence with highly classified sources and methods, we now recognize the need to integrate information from diverse activities including traditional foreign intelligence, border authorities, law enforcement investigations and intelligence, emergency responders, state and local activities and citizens. Individual adversaries involved may include citizens for whom the rules are different. The domestic operational environment is very different – it's our own business, infrastructure, and people. Many of the people involved are not cleared for classified information. Information may be submitted by concerned and vigilant citizens. The Federal government cannot be successful in deterrence, detection, and prevention of terrorism without willing cooperation of all the domestic partners, to include operator and intelligence collaboration.

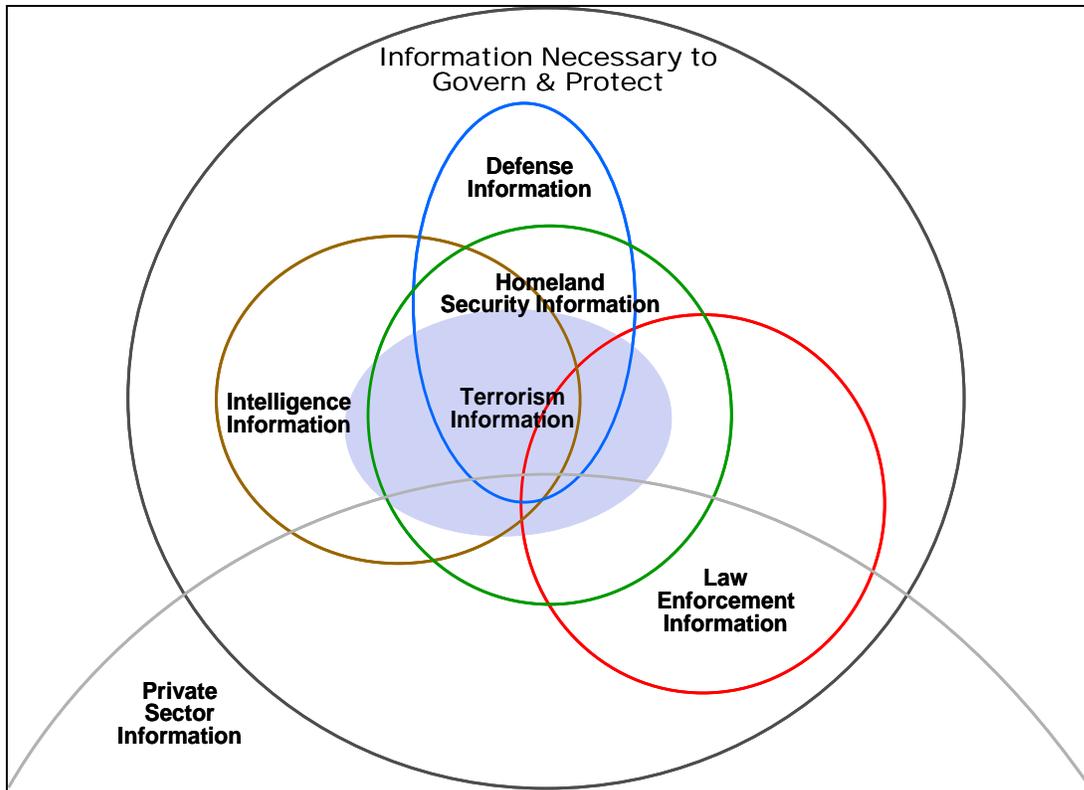


Figure 3. Information Needed to Govern and Protect

Problem Structure. The ISE vision describes in broad terms the capabilities desired for use in Terrorism Information Sharing, and done right, information sharing in general, since the requirements for other purposes are generally (with the current exception of wireless) a lesser included set. The DHS depiction of the *Information Needed to Govern and Protect* outlines the greater scope and relationships, all of which must be incorporated for the coordinated action envisioned by the Secretary. While terrorism information is the central focus of multiple commissions, legislation, executive orders and Homeland Security Policy Directives since 9/11, it is important to note that

- Not all terrorism information is recognized as such when first gained or without analysis.
- Terrorists frequently use non-terrorist activities to finance and otherwise support them or their terrorist acts.
- There can be considerable overlap between resources and procedures to accomplish other homeland security missions such as disaster response and terrorist event mitigation.
- Information to govern and protect should flow as freely between all activities concerned consistent with protection of individual civil liberties and privacy.

The Intelligence Community (IC) has done extensive work maturing and expanding standards and infrastructure to support processing of highly classified data. No such process exists for the equivalent needs in the much larger Sensitive But Unclassified (SBU) and For Official Use Only (FOUO) areas. While the processes for CONFIDENTIAL through TOP SECRET security and transmission are included in the IC structure, the more common needs and applications need to be addressed within the State, Tribal and local governments, some private sector, and even elements of the Federal government and Non-Government Organizations (NGO) whose roles prior to 9/11 were less active from a Homeland Security perspective. DHS operates throughout all seven of the communities defined in the *Implementation Plan for Executive Order 13356, Strengthening Terrorism Information Sharing* (law enforcement, homeland security, diplomatic, private sector, defense and State, Tribal and local). DHS is thus pivotal to successful information and intelligence sharing throughout all of the key stakeholders and disciplines.

Basics and Best Practices. While there is no single recipe for success in information sharing or progressing to the future, some basics do apply.

- Top leadership vision and support are essential to aligning business process, information sharing and resources.
- Business process and information technology support must be aligned for operational effectiveness and resource efficiency.
- User focus and user involvement up front and throughout is essential to effective functionality and user acceptance. Users exist at multiple levels and capacities.
- Data should flow freely in accordance with agreed business rules. Data need not follow hierarchy, but must follow business rules. Decisions are made hierarchically, but not timely or optimally if data is impeded.
- Data alone is not sufficient. Knowledge and understanding come from context (metadata) as well as content. Collaboration confirms understanding and enables unified operations.
- Productive information technology support planning and implementation requires an architectural construct consistent with business plans. A skyscraper requires a different foundation than a suburban residence. Both serve their purpose better when consistent with environmental planning.
- Good metadata is essential to transparent and efficient data/information sharing.
- Information Assurance and all its inherent protections must be designed in from the beginning. Bolt on additions are expensive and fail.
- Good information assurance supports privacy and civil liberties and vice versa.

- Grand designs historically fail. Manageable and iterative steps succeed.
- Metrics tell the story. If you can't measure it, you can't manage it.
- The most important predictor of top governance performance is the percentage of managers in leadership positions who could accurately describe their enterprise's IT governance. (*IT Governance*, Sloan School Center for Information Systems Research).

Current status

- The Secretary's testimony encapsulates the operational vision for the Department – unified execution of operational missions. The ISE vision and capabilities scope the broad technical parameters.
- Business processes remain largely stove-piped throughout DHS. Some cross functional information flows exist through the Homeland Security Operations Center (HSOC).
- Data does not flow freely. Existing collaboration is manual, slow and suboptimal.
- The DHS Metadata Center of Excellence (COE) has been initiated and further adopted by the Federal Chief Information Officer (CIO) Council for the Federal government and by Department of Justice (DOJ) for the joint DHS/DOJ Global Justice. The Metadata COE is born but still in infancy. It needs to be nurtured and grown by the whole village.
- The DHS Enterprise Architecture Version 2 provides limited structure and is incomplete. The joint CIO/Chief Financial Officer (CFO)/Information Sharing and Collaboration Office (ISCO) developed data base of systems supporting terrorism information sharing prepared for OMB data request 05-34 is user validated. The ISCO/CIO jointly prepared eSurvey focusing on mission critical information sources, products, supporting systems, functionality, classification, users and additional information is in final stages of collection. The ISCO has prepared a database of System of Record Notices (SORN) for DHS systems containing personally identifiable information which can provide an excellent foundation for information sharing and collaboration architectural views and integration with business process analysis and alignment.
- Current information security measures restrict rather than enhance information sharing.
- Metrics are not in place. ISC principles and assessment have recently been added to the Investment Review Board process, but should be tested and strengthened through use and experience. Best commercial practices are not uniformly employed, e.g., Service Levels of Agreement (SLA) have not been established

consistently throughout the DHS. Components have no measure of their information sharing.

A means is needed to align DHS business processes, information sharing, and resourcing.

Business Plan. This business plan addresses the current (as-is) status of information sharing and collaboration within the Department of Homeland Security (DHS) and with its key stakeholders throughout the Federal, State, Tribal, local, non-government organizations, private sector and other cooperating governments. It describes the envisioned state (to-be) and actions necessary to attain the envisioned state. DHS participated significantly in the preparation of the Implementation Plan in response to Presidential Executive Order 13356, *Strengthening Terrorism Information Sharing*. Because participation in the Information Sharing Environment (ISE) established therein is essential to DHS success more so than any other Department, this plan incorporates the ISE and supplements where necessary to satisfy unique DHS requirements. One principal supplement is the extension of this plan to include all information sharing and collaboration needs, not just the terrorism sharing needs that were the focus of the ISE Implementation Plan.

When the Business Plan tasking was received and the Information Sharing and Collaboration Office was established, it was agreed that we would not wait for the completion of the plan to begin actions necessary for implementation of a full business plan. Accordingly, many actions have begun in conjunction with the plan, and whether complete or not are included in the As-Is discussion and analysis, and serve as a foundation for additional near and long term actions. Several but not all of these are listed in Annex H, Selected DHS System Summaries.

Capabilities addressed in the business plan are not detailed in this executive summary, but include user friendly features such as single log on, direct access to information required in accordance with user authorizations and environment, and information assurance provisions to protect information and users.

Since DHS must continue ongoing operations and has urgent needs for improvement, a logical way to proceed is to identify the principal workhorse functions of the Department and its interface with others, identify their information needs and products, and iteratively add information sharing capability to those systems yielding greatest potential return in effectiveness and efficiency. The net effect will be to ramp up effectiveness and reinforce the mainstream systems. In the process, the lesser productive systems can then be identified and functions upgraded or merged into other continuing systems with increased efficiency and little to no operational loss.

This work has already begun. DHS and DOJ are cooperatively leading information exchange from native terminals between the Homeland Security Information Network, Law Enforcement Online (LEO) and the Regional Information Sharing System (RISS), allowing users using their own terminals to access information from other systems not previously available. Internally, IA and CBP have begun identification of information sharing needs and value added processes.

Using working prototypes in this manner has the added advantage of providing users a visible and working vehicle for discussion of the “what can be” and in so doing results in better understanding and definition of next iteration capabilities.

This model should be implemented across the Department for high payoff operational and risk mitigation information sharing. Major synergy and productivity gains can be made by selecting enterprise workhorse systems and mapping uses and needs to determine exploitation potential. The eSurvey Information Sources and Products and the DHS response to OMB BDR 05-34 on Systems Supporting Terrorism Information provide an initial analysis capability for enterprise discussion. An early adopter operational candidate is Customs and Border Patrol (CBP) and IA information sharing effort already addressed to improve suspicious activity reporting, analyses and feedback. Risk mitigation candidates include provision of biological agent information as soon as determined in an incident to emergency responders including Emergency Preparedness and Response (EP&R), local fire, medical and law enforcement as well as State, Tribal and local government emergency managers.

You can't manage what you can't measure. A Capability Maturity Model (CMM) is presented to describe and measure the goals and state of DHS ISC with the Department and its components. While specific metric design is needed for individual capabilities and processes, the model presents a unifying and descriptive means to progress. It is adapted from the Software Development Capability Maturity Model developed by the Software Engineering Institute of Carnegie Mellon University to bring discipline and efficiency to Department of Defense software development. The CMM is widely accepted both commercially and in defense industry world wide. The following ISC CMM was developed using similar principles and application.

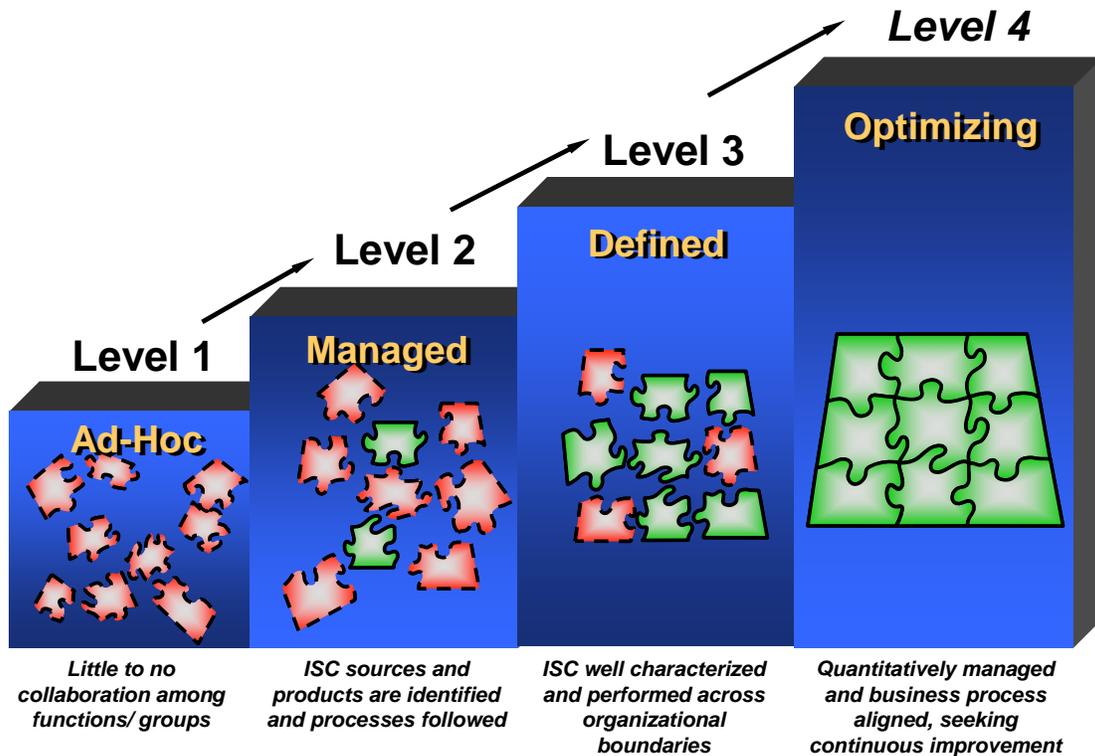


Figure 4. Information Sharing and Collaboration Maturity Model

DHS at large is at Level I.

Recommended Actions.

1. Leadership affirm and support the need to manage Information Sharing and Collaboration
 - a. Establish and personally (Secretary or Deputy Secretary) chair the Business Process/Information Sharing and Collaboration Council to make and oversee Business Process/ISC decisions related to principles, business application needs, ISC architecture, ISC Infrastructure and ISC investment and prioritization in support of business process needs.
 - i. In the first meeting review the DHS OMB 05-34 data on systems supporting terrorism information sharing, the eSurvey summary of information sources and products, and the System of Record Notice listing.
 - ii. In the second meeting select the DHS workhorse systems as the baseline for completing metadata and expanding information sharing.

- iii. In each meeting following, review progress in sharing, select next systems to be added and review investment needed.
 - b. Resource the Information Sharing and Collaboration effort – staffing and funding
 - c. Align and formalize responsibilities and relationships
 - i. Business Process
 - ii. Information IT Infrastructure
 - iii. Information Sharing and Collaboration
 - iv. ISC Investment and Investment Review Board
 - v. Relationship with and POC to PM ISE
- 2. Formalize and emphasize the governance, processes and information data-basing and access for
 - a. Facilitating and recording Information Sharing Agreements
 - b. Information Sharing and Collaboration Business Rules
 - c. Business Process and Information Sharing and Collaboration
 - d. Enterprise Architecture
 - e. Metadata
 - f. Information Assurance
 - g. Metrics (general and specific to each business process and functional area)
- 3. Publish a DHS Mission, Organization and Functions Manual
 - a. Sufficient detail to help DHS people find people and data of interest
- 4. DHS take active lead with DOJ, HHS, HQDA, State, Tribal, local and private sector agencies and activities in establishing needs, standards, procedures and best practices for the sharing and use of SBU and Collateral information.
- 5. Establish 90 day time limit for DHS components to complete System of Record Notices (SORN) for systems carrying individual identifying information to bring DHS in compliance with Federal law.

6. Establish a 90 day review and report on ongoing initiatives and programs to resolve State, Tribal and local issues to ensure cohesion and prioritization of effort in accordance with State, Tribal and local needs, e.g., June 9, 2005, CRS Report

The major state and local homeland security issues are:

- The fact that state and local governments cannot use homeland security funds to pay for personnel.
- The need for statewide interoperable communications.
- The impact of reductions in first responder funding.
- The setting of standards for first responder equipment.
- Access to classified information

1. Introduction

1.1 Purpose

The purpose of this plan is to describe the key activities that will support the Department of Homeland Security (DHS) to transition from the existing information sharing and collaboration environment to an environment that will better support the DHS in meeting its goals and objectives, including a description of the benefits of making this transition. This business plan is intended not only to describe opportunities for better information sharing and collaboration within the DHS enterprise in order to make informed choices, but also to support subsequent work to realize the benefits. In short, this plan should be used as a long range guide to drive results.

1.2 Background

In May, 2004, Secretary Ridge directed the Under Secretary for Information Analysis and Infrastructure Protection (IAIP) to develop a DHS-wide business plan for comprehensive information sharing and collaboration system, and directed participation by all DHS directorates and offices.

On 20 April 2005 Secretary Chertoff testified to the United States Senate Subcommittee on Homeland Security:

Intelligence and Information Sharing for a 21st Century Department

On the most basic level, we need to take a step back and focus on the fundamental question: Why was the Department of Homeland Security created? It was not created merely to bring together different agencies under a single tent. It was created to enable these agencies to secure the homeland through joint, coordinated action. Our challenge is to realize that goal to the greatest extent possible.

*Let me tell you about three areas where I plan to focus our efforts to achieve that goal. First, we need to operate under a **common picture of threats** we are facing. Second, we need to **respond actively** to these threats with the **appropriate policies**. Third, we need to **execute** our various **component operations in a unified manner** so that when we access the intelligence and we have decided upon the proper policies, we can carry out our mission in a way that is coordinated across the board.*

Secretary Chertoff, *Statement for the Record Before the United States Senate Subcommittee on Homeland Security*, 20 April 2005.

The *sine qua non* that enables success in all three areas identified by Secretary Chertoff is information sharing and collaboration. A better intelligence process alone is not sufficient. A **common picture of threats** is impossible without sharing throughout the intelligence and information domains. **Active and appropriate policy response** can only be accomplished well with sharing across the domains of intelligence, emergency responders, law enforcement, and homeland security. **Unified execution of component operations** mandates sharing across all activities involved.

The landscape has been considerably enlarged since 9/11. In addition to national intelligence with highly classified sources and methods, we now recognize the need to integrate information from diverse activities including traditional foreign intelligence, border authorities, law enforcement investigations and intelligence, emergency responders, state and local activities and citizens. Individual adversaries involved may include citizens for whom the rules are different. The domestic operational environment is very different – it's our own business, infrastructure, and people. Many of the people involved are not cleared for classified or otherwise restricted information. Information may be submitted by concerned and vigilant citizens. The federal government cannot be successful in deterrence, detection, and prevention of terrorism without willing cooperation of all the domestic partners, to include operator and intelligence collaboration.

DHS, by mission, operates throughout all seven domains identified in the Executive Order 13356 Implementation Plan, and by mission and position bridges these domains for all Departments and Agencies. As such, DHS must

- Collect, analyze, validate, broker and disseminate actionable information in user language and context when and where needed.
- Facilitate, define, develop and support information sharing and collaboration services in coordination with business owners to optimize business effectiveness and efficiency consistent with investment wisdom.
- Be the authoritative source of information. Open sources may have parts of information before us or information we don't have validated, but DHS information is accurate or appropriately caveated.
- Assist business owners in understanding the effective use of information sharing and business process, especially effective and routine processing of information which can be treated as such and efficient means of dealing with information that can't.
- Provide essential services such as the 24x7 Operations Center which monitors, alerts, facilitates, answers, brokers, covers for and supports mitigation and the Metadata Center of Excellence which enables information sharing and understanding across all domains

DHS has been given the mandate to improve homeland security information sharing by prescribing and implementing procedures across the federal government and from the federal government to state, local, and tribal entities with a role in securing the nation's

critical infrastructures.¹ In addition, DHS' internal missions include enforcement of specific federal criminal laws and response to disasters, both those caused by terrorism and by other causes. These other missions must be considered in any activities designed to improve efficiency and effectiveness through better information sharing and collaboration.

The Secretary of DHS delegated the DHS authorities for information sharing to the DHS Information Sharing and Collaboration Office (ISCO) by memorandum dated May 11, 2004. That memorandum charged the ISCO with coordination and facilitation of information sharing efforts throughout the Department and with its customers and partners - the Federal, state and local, tribal, international, and private sectors. The ISCO will develop and facilitate implementation of the Department's strategy and plan for improving sharing of information assets among all partners in accordance with four imperatives: 1) within DHS directorates, 2) across DHS, 3) across the Federal government, and 4) with our state, tribal, local and cooperating governments, and our private sector partners.

DHS participated significantly in the development of the Implementation Plan developed in response to Executive Order 13356, *Strengthening Terrorism Information Sharing*. Because of this significant participation, DHS interests and needs are well represented in the vision, gaps, challenges, capabilities and requirements section and are represented as such in this plan. Because of DHS' pivotal role in both terrorism and homeland security information throughout the Federal government it is appropriate and necessary to endorse and support the common vision and direction for information sharing. Additional details unique to DHS needs are added where appropriate.

The Implementation Plan assessed the current and future states in terms of governance, standards and policies, cultural resistance, resources, access and dissemination control, collaboration and functional requirements/capabilities. We use this construct for compatibility but add discussion where appropriate, e.g., State, Tribal and local considerations.

1.3 Mission and Goals

The 2004 U.S. Department of Homeland Strategic Plan outlines the Department mission as:

We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to the threats and hazards

¹ Executive Order 13311 (delegating the President's authority pursuant to 6 U.S.C. para. 483 (Section 892 of the Homeland Security Act))

to the Nation. We will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce.

The Department's primary strategic goals are as follows:

2004 DHS STRATEGIC GOALS

Awareness—Identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to our homeland security partners and the American public

MISSION GOALS

Identifying threats and vulnerabilities to the homeland

Facilitating the flow of goods and people

Preparing for and preventing incidents

Responding to incidents

Conducting law-enforcement and post-incident investigations

Investigating and recovering from incidents

Developing plans, policies, and standards

Performing research and development

Managing information technology

Disseminating and communicating information

Resource management functions, e.g., financial management, grants management, acquisition management, and asset management

In addition, DHS has expressed the following mission direct and mission supporting goals (SAIC 2004):

2. TO-BE (Where We Want to Go)

Vision of an Interoperable Terrorism Information Sharing Environment (ISE)

The vision of the interoperable terrorism information sharing environment, created and maintained in full partnership by all levels of Government, effectively supports detection, prevention, disruption, preemption, and mitigation of the effects of terrorism against the territory, people, and interests of the United States of America. It does so by enabling the interchange of terrorism information among and between appropriate Federal, State, Local, tribal, and territorial authorities, foreign partners and the private sector. It will support the ability of agencies to acquire additional such information, and, it will protect or enhance the freedom, information privacy, and other legal rights of Americans in the conduct of their activities.

Initial Plan for the Interoperable Terrorism Information Sharing Environment, prepared by the Information Systems Council in response to EO 13356, 20 December 2004.

2.1 Information Sharing Vision.

The above vision is based in good part on the significant participation of the DHS in the development of the Information Systems Council's Initial Plan for the Interoperable Terrorism Information Sharing Environment, 20 December 2004, developed in response to Executive Order 13356, *Strengthening Terrorism Information Sharing*. Because of this work, DHS interests and needs are well represented in the vision, gaps, challenges, capabilities and requirements section.

Since DHS plays a pivotal role in both terrorism and homeland security information throughout the Federal government it is appropriate to endorse and support the common vision and ISE contained in that plan. Unique DHS requirements are addressed as developed and added where appropriate. In particular additional emphasis and explanation is given to

- Requirements for Sensitive But Unclassified and Collateral (Confidential through Top Secret) sharing in the extensively expanded community of State, Tribal and local governments and private sector as well as the broader community of Federal departments and agencies now playing a much larger role in homeland security inter-agency operations
- Collaboration in a significantly enhanced and effective mode.

- Information Sharing and Collaboration Capability Maturity Model to assess ISC organizational status
- Risk management model
- ISC with coalition allies and cooperating governments

2.2 Collaboration

What is Collaboration? Collaboration means different things to different people. Working together to provide a shared and improved result is commonly accepted. Many educators and military personnel see video teleconferencing, perhaps with a shared white board capability as collaborative technology. Carried to its ultimate, collaboration can be much more robust, effective, efficient and lasting. In this section, we describe the importance of collaboration, the collaboration support capabilities already in place, the technological and social requirements for a more integrated and adaptive collaboration environment, the potential we could attain with more advanced capabilities, and specific examples of those capabilities.

Why Collaborate? Collaboration adds the richness of context, sharing and questioning, opposing viewpoints and considerations, legal, technical and logistical limitations, rapid access to experts, and modeling and simulation insight, and develops the common understanding that enables the components to operate in a unified manner. Facilitating knowledge sharing across communities of interest that do not yet have established processes for information sharing involves creating the infrastructure, mindset, and tools needed to support a new culture of collaboration and sharing. A number of different factors influence community members' participation, involvement, and the eventual success of the collaboration. These factors include the degree to which users are aware of the various communities, information, and knowledge available in the environment (awareness), the ease of finding useful information in a timely manner (structure), and whether or they perceive an immediate benefit from collaborating with others (motivation).

From an informational perspective, connecting communities of interest and providing more information at users' fingertips means increasing the volume of data that a user must search through in order to finding the most relevant information. Guidelines, roadmaps, metadata, structures, and tools for finding relevant information in not only information-based, but also *community-based* contexts are essential, and must be constantly updated and maintained.

How do we collaborate? Data stored in physical databases, filled perhaps with spreadsheets, documents, images, and videos are the first required element for collaboration. Metadata (information about information, such as categories and formats) helps increase the accuracy of this data and extends its use, while context and circumstances help turn the data into information. Metadata (information about information) helps increase accuracy and extends data use, while context and circumstances help turn the data into information. The interpretation of that information

by communities with specific backgrounds and expertise leads to understanding. The process of internalizing these new interpretations of information in context leads to the creation of new knowledge. If this knowledge is not documented or shared, it often become tacit cognitive knowledge stored in users' heads. While knowledge and meaning on an individual basis enable individual action, coordinated action requires communities to share information across multiple domains, but information sharing alone is not effective without context and mutual understanding. Experts may argue about at which level or at how many levels the sharing should take place, but the objective is to jointly construct shared knowledge, enabling meaning and unified action.

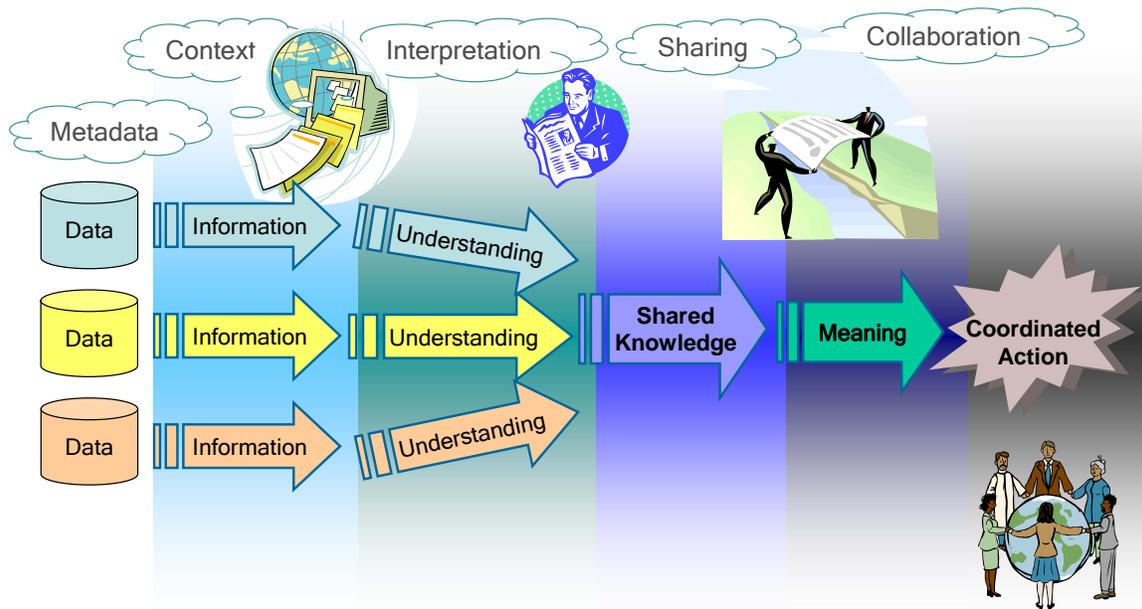


Figure 5. From Data Through Collaboration to Coordinated Action

Structured data is individually interpreted and internalized in context. Communities share that information, enabling them to collaboratively construct meaning and take coordinated action.

How can we support effective collaboration (Social Point-of-View)? Effective information sharing across organizations with different objectives and perspectives means sharing the right information, at the right level of detail, using the right language, at the right time, in the right context, with the right people. A failure related to any one of these factors can lead to an information sharing breakdown. Supporting the effective use of shared information is even more complex because access to information does not necessarily lead to effective knowledge sharing and collaboration. When users from different communities share information, they interpret that knowledge in new contexts, transforming and creating new knowledge, while at the same time contributing toward the development of the communities grounding that knowledge.

Enabling, encouraging, and facilitating information sharing and collaboration require different supportive mechanisms culturally and technologically. Enabling information sharing is the first step, involving cross-organizational access to information according to sharing policies and procedures. But access to information does not necessarily lead to effective knowledge sharing and collaboration. When people share knowledge, they are not just sharing information; they are also sharing cultural and social references. Likewise, when people seek knowledge, they are not just seeking information; they are seeking information grounded in, and carrying different meanings to different social communities. Information is viewed, perceived, and used differently by each community. When users from different communities share information, they interpret that knowledge in new contexts, transforming and creating new knowledge, while at the same time contributing toward the identity of the communities grounding that knowledge.

The role of the information sharing environment, then, is to encourage, support, mediate, and guide this cyclic process of community development through knowledge seeking, sharing, joint understanding, and social knowledge building. In this way, data is contextualized and transformed into information, which is in turn shared, interpreted, and socially transformed into knowledge. As this knowledge is developed and integrated and used by components that operate collaboratively, it is understood and given different meanings and applications.

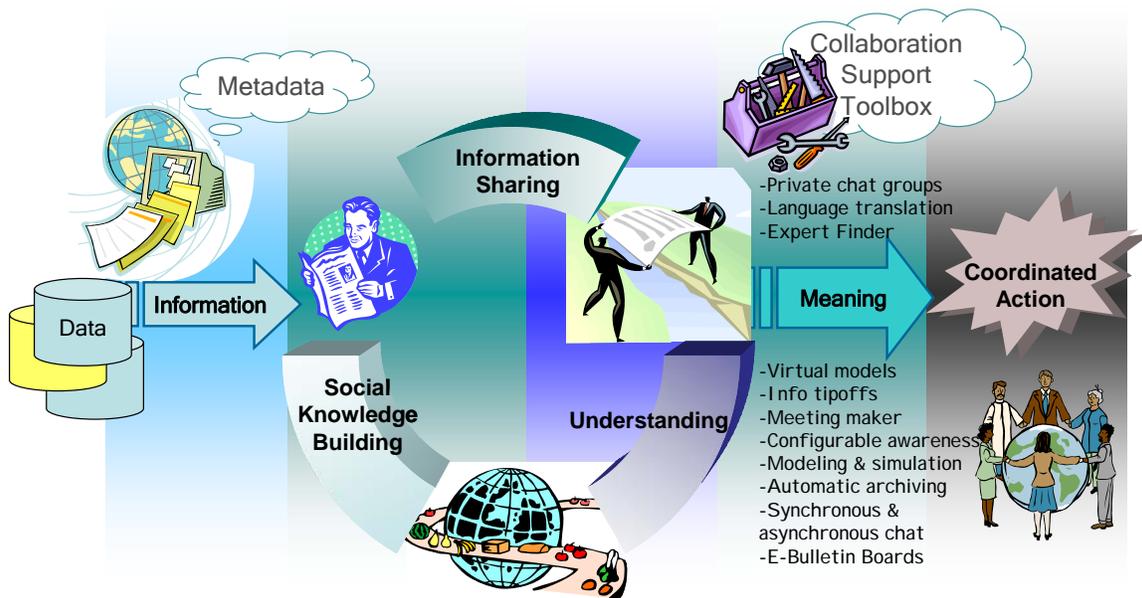


Figure 6. Advanced Collaboration Cycle

Communities that effectively share structured information enter a cycle of reifying (considering abstract concepts as real), collaboratively interpreting and understanding, and building new knowledge together. Advanced technologies such as collaborative language translators and virtual meeting environments facilitate the joint construction of meaning and support coordinated action.

How can we support effective collaboration (Technological Point-of-View)?

Collaboration technology should at the very least enable natural information exchange, coming as close as possible to supporting the kinds of activities in which collaborators engage (e.g. including features that play the roles of supporting body language and mediating communication for face-to-face interaction). A more developed collaborative environment would in addition provide context sensitive support which could include a variety of services including information tipoffs, relevant status, what experts are looking at, available knowledge sources, expert contact information, information others seek or use in similar circumstances, language translation, private chat groups, reminders of missing or out of norm steps, capability to interact with large scale virtual and physical models, databases, modeling and simulation on line, automatic archiving and distribution, dynamic reconfiguration, meeting maker and update for indisposed members, individual tailorability, access control and authorization, information and transaction auditing and more. Automated data organization, indexing and directory services/search assistance to find information whatever the venue in a user friendly mode would substantially improve efficiency and effectiveness. Most importantly, collaboration services would be easily accessible and usable when and where needed by all parties.

In the current environment, agencies collaborate through physical acts (e.g., participating in task forces, sending detailees, hand-delivering information) and, to a limited degree, through virtual acts (e.g., through online, interactive collaborative tools). Even after roles and responsibilities are better defined, participants will still need to work together, analytically and operationally, to provide context and produce improved results in the fight against terrorism.

Collaboration tools and environments in use today often are not interoperable, making it difficult or impossible for users separated by geography or network topology to effectively reach one another and communicate. Processes, procedures, and technology must be introduced to enable efficient work across organizations, geography, jurisdictions (i.e., foreign and domestic), and domains. There must be a mandate requiring each party with authority over a possible terrorist situation to collaborate. New collaboration processes should provide agency context and/or background for information. Exchange of permanent liaison personnel should take place at all 24x7 national operations and intelligence/information fusion centers. Collaboration policies should seek to encourage productive on-going collaboration (e.g., Terrorist Threat Integration Center (TTIC), Joint Terrorism Task Forces, state and local intelligence/information fusion centers), and to formalize the existence of such activities where they have been created in less formal settings.

Technical collaboration capabilities needing enhancements include white board, context sensitive tip-off, language translation, translingual chat, translingual retrieval, expert contact information, and real-time transcription. Collaboration tools in this environment would also include directories in which individuals or organizations can be located. It means enabling individuals using networks with different security levels to communicate with each other.

Cross-community discussion groups that are linked to integrated data sources may help to give more context and meaning to the content. For example, users and groups could collaborate in online discussion forums that are directly linked to the imagery and reports they are sharing, commenting and explicitly making linkages (e.g. arrows, highlights) to sections of the shared items being discussed. Rating or voting tools might also help community members determine what information (discussion items, images, etc.) is helpful for what purposes.

Information from one producer is often repeated in many different reports and repositories. Other users in turn may replicate and pass this same information along to others. Users cannot know the confidence they should have in the data. A fact seen in many places might appear to be highly corroborated when in fact a single observation is being repeated many times. A mechanism for producers to easily indicate the source of information contained in a report should be developed. A companion mechanism to display the information to the consumers of the reports would be necessary.

What can we expect from the collaboration? Effective information sharing communities will share quality, understandable information with other communities that do the same. The perceived and measured benefit of collaborating is predictive of the level to which community members continue to collaborate with each other over time; therefore, communities must be rewarded for their sharing efforts. For example, members should be provided with summative feedback about their participation and collaboration. Augmenting participation and activity statistics with suggestions and comments may also help community participants understand what is working, and why or why not. Evaluation and assessment should be done at each phase of development and deployment with a high level of community involvement. For example, each organization should understand what knowledge was shared and how it was used by other organizations.

The war on terror is a global war. National boundaries have been a haven for terrorists who find they can take haven by moving from one country to another. One of the ways our country can combat terrorism is to support cooperation with our allies and coalition partners. They can help both by providing us information and by apprehending terrorists inside their borders. Information sharing with our allies and coalition partners has the same kind of benefits as sharing information between U.S. government organizations. The environment needs to permit, encourage, and facilitate the exchange of information with our foreign partners.

2.3 Users

The user communities are the much broader scope throughout all government levels, private sectors and cooperating foreign governments. The needs of the varied communities span unclassified, Sensitive But Unclassified, each of the levels and compartments of classified information as well as the additional and various categories and caveats associated with the private sector and foreign governments. Each of the users has their concerns about receiving information and about use of the information they might provide.

Users need access to and use of many different information types (e.g., structured data, audio, video, imagery, and documents). Users need the capability to discover the information they need without knowing its location or even that it exists in the environment. Users need to have confidence in the information they receive or have some measure of the uncertainty associated with the underlying data so they can make decisions and act with confidence

2.4 Information Sources

Information Sources may provide organized processed data or free-form raw data to interested parties. They may provide information through a structured information source such as those with well-defined and categorized data about specific entities. Information may be gained through full-text information sources such as free-form narrative text documents. Open source information can be very helpful, but needs to be assessed in terms of accuracy, context and misinformation potential. GIS perspective helps decision makers considerably in terms of viewing the situation, assessing time and distance related actions, and estimating consequences of alternative plans.

2.5 Services

Services can be described in two groupings. The first, Enterprise (ISE terms these Environment) Services, are core capabilities required to enable information sharing through the infrastructure. They require interacting with the environment using coordinated governance mechanisms, and use of standards to interface with others in the environment. Enterprise Services are used to locate users, services, providers of data, retrieve the data from the providers, collaboratively process the data and make reliable information accessible to authorized users.

The second is Independent Services. Independent Services require little or no coordination by the environment's governance mechanisms, although they must still be compliant with appropriate standards to allow the services to be located and leveraged by other participants. Independent Services thus allow organizations to create and share new functionality and grow the environment's overall capabilities. Examples of Independent Services are: fingerprint analysis, language translation or fusion/analytic centers that provide specialized processing. Even though they may be grown independently where such services do not exist or do not exist in sufficient functionality to meet the need, the first choice should be to use or build on what exists already if at all feasible. Many independent services will migrate to Enterprise Services as they mature to enhance interoperability, efficiency and service availability to all.

There are five types of Enterprise Services: information, collaboration, information security/assurance, location, and configuration and network management services. Each environment service and the capabilities they provide are discussed below.

Information Services. Information Services allows users to find and retrieve data, determine relationships between such data and notify processed intelligent information to

interested parties. *Search* and *retrieval* are two of the most common methods for providing this service. Search allows users to locate shared data items based on content or structured attributes; retrieval is used to retrieve complete data items from partner data sources. Besides search and retrieval, *subscription* is another information service that allows notification to a User when new data items match their subscription template. Also, *correlation* is an information service that facilitates the identification of associations between content, people, places, and organizations.

Collaboration Services. Collaboration Services include tools and applications to enable multiple people to interact with each other on areas of mutual interest. These services cross organizational boundaries with rich media content. A few examples of a collaboration service are: email, notification and groupware. Email provides secure electronic messaging; notification is used to notify Users of various events (such as subscription matches) through various means such as email, pager, radio, telephone, etc.; and, groupware provides mechanisms for collaboration among users, such as shared workspaces.

Information Security / Assurance Services. Information Security and Assurance Services are used to ensure reliable data is shared with the right individuals for appropriate reasons. Included in these types of services are things like authentication (verify users), authorization (verify whether users are authorized to access a particular resource in a given location or environment) and audit (verify that the authentication/authorization rules are being adhered to and to investigate possible misuse).

Location Services. Location Services are used to find services, providers, users and raw or processed information. There are three main kinds of location services: Data Directory which indexes data items from all data sources by entities and attributes; User Directory which stores contact information, group membership and roles for all users; and Service Directory which stores information on the Services provided by the partners in the environment. The Service Directory Service provides information on which partners support which Services and the technical details on how to connect with those Services.

Enterprise Management Services. Enterprise Management Services are used to ensure that reliable and acceptable performance is available to the users of the ISE. Performance services monitor key metrics to ensure established requirements are met (e.g. latency of the different requests) and Availability services monitor the Services to ensure they are available.

2.6 Seamless Environment

The mission requirement is to provide an environment that is seamless regardless of seams created by the national security classifications of information or the physical separation of existing networks. Cross-Domain solutions will be used to exchange information between the different security levels in the environment.

Figure 7 depicts the multiple security levels found in the environment and the Cross-Domain Mechanisms for exchanging information between the levels.

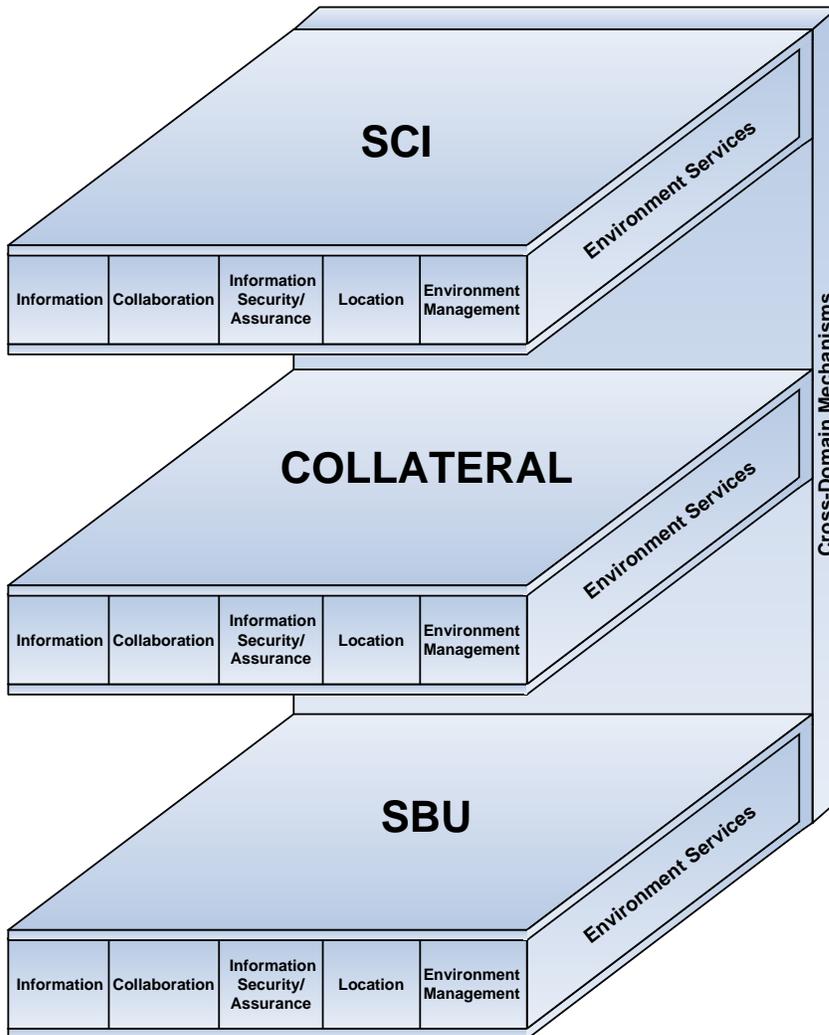


Figure 7. Seamless Environment

The Cross-Domain Mechanisms of the environment are designed to facilitate sharing and coordination between different classification levels. A few examples of mechanisms include, *Tearlines* (move information to a lower security domain by extracting the portions that are shareable at that level), *Proxies* (used by a higher level domain user to access Services at a lower level domain while complying with domain security requirements), *Organizational Messaging* (exchange of organizational electronic

messages between two domain levels) and *Chat* (synchronous online conversations by multiple users from different domain levels).

2.7 Resourcing

Implementation must be resourced for it to occur. While some programs can be accomplished using existing funds through coordinated effort, and this should be done wherever feasible, some ISC needs cross so many boundaries and involve so many organizations and activities that waiting for requirements, funding, acquisition, testing, accreditation, training and implementation by all is lengthy at best and infeasible.

Economy, speed of implementation and efficiency could be well enhanced if services are provided by the Federal Government or several federal agencies in cooperation. The National Y2K Information Coordination Center (ICC), in preparation for the millennium rollover, developed and provided two way critical infrastructure, business and system information sharing with the Federal, State, Tribal, local and private sector agencies in three months from programmer availability to operational system. This was accomplished under central leadership in collaborative development with the stakeholders. Stakeholders helped define information they could provide, e.g., business operations and critical infrastructure status, and information of use to them, e.g., status of essential Federal and private infrastructure services, e.g., financial, power and telecommunications. The win-win strategy succeeded in good part because each party that provided information was also able to obtain information that they wanted, search for specific items locally, and see status of critical national systems and infrastructure.

The ICC was centrally funded and provided services to State, Tribal, NGO and private sector activities. Central funding enhanced the speed of funds availability, standards definition, contracting, testing and deployment. This model can and should be employed selectively where it can meet needs quickly and efficiently.

Whatever resourcing mechanism is selected, the most important factor of success is the involvement of *all* key stakeholders in ISC requirements definition and implementation.

2.8 Design Considerations

User Friendly. The system must be easy to use. If it is not easy to use, users will not use it, will find expensive and insecure workarounds, and ISC will occur only at the most inefficient levels.

Environment. The fundamental technical design consideration is one that provides flexibility through a services-oriented architecture. The architecture must be designed to accommodate new technologies, methods and solutions .

It is essential for speed and economy to leverage use of existing assets where feasible. Industry open standards will be adopted wherever possible. Using well-adopted standards

such as Justice XML, Web Services Framework and UDDI will significantly reduce both the risk and cost of implementation and technology insertion as it becomes available.

Information. Virtually any kind or format of data will be supported in the environment - text, images, audio, or video; unstructured, structured, or semi-structured; .doc, .xls, .ppt, or .pdf. Shared data may remain distributed – stored at and managed by the organization that owns and shares it. Rather than requiring a centralized data warehouse, the environment will establish metadata standards that enable users to search a multitude of heterogeneous shared repositories to find relevant data. Where feasible and efficient, the environment will provide managed, distributed warehouses which are electronically and physically secured for use by components using ISE standards for interoperability. DHS normal and COOP functions can be more expeditiously accomplished reliably and at much less cost using managed, secured, distributed data warehousing. These would be implemented using existing facilities which meet criteria or can feasibly be upgraded.

In addition to this "pull" model for location and retrieval of information, the environment will support a "push" model where new or modified data items are delivered immediately to the appropriate users based on predefined subscriptions.

Data standards are key to achieving the environment. At the highest level, standards for categorizing and naming data enable participants to describe their information with terminology that has common, well-defined meaning. Metadata standards will allow environment-wide capabilities (such as locating data by content) to operate over heterogeneous information sources from all participants. Finally, standards for structuring data will minimize the effort required to automate the integration of data from different sources for analytics or any other purpose. The DHS Metadata Center for Excellence (COE) has been selected by the Federal CIO Council to be the Federal Metadata COE as well.

The ISE will create a data reference model (DRM) to be created for the environment to realize the benefits described above. By its role as Metadata COE DHS will play a significant support role in the DRM. DHS should require all of its system developers to support and use the DRM and the Metadata COE in all system development.

2.9 Functional Requirements

However successful the vast improvements in information sharing since 9/11, a large number of important functions remain that cannot be performed today. The proposed environment needs to resolve as many of them as possible and as quickly as feasible. Capabilities required for a DHS IS&C environment were identified in the ISC report in response to EO 13356 and are listed below. As identified in Table 1, the following provide the highest level functional requirements for the proposed environment:

Table 1. Functional Requirement Definitions

A virtual trusted sharing environment	The technical requirement for the environment ensures information gets to the people who need it, while appearing to the user as though it is a seamless trusted sharing environment. This serves as the most basic requirement for the environment.
Single log on	When users log on to their home environment, that logon should provide them with access to whatever information they need from the interoperable terrorism information sharing environment. They should not have to “log on to” a different environment. Instead, the proposed capability to share information should be a part of all users’ “home” environments.
Easy to use	The environment must be easy enough to use so anyone capable of using the Internet can perform the primary functions without any classroom training. The large majority of the functions should be sufficiently user-friendly such that most users can learn how to use them from computer-based training.
Timely information	The environment needs to be able to detect when relevant, new information is available and automatically provide it to users in real-time/near real-time.
Federated queries	Users should be able to issue a single query to return information from all relevant sources.
Subscription and pushed information	Most users need similar information day in and day out to perform their jobs. They should not have to issue the same queries every time they need the information. Instead, they should be able to subscribe to particular sources or establish profiles both of which would send information to them as soon as it is available.
Provide answers to questions when appropriate	Some users, particularly those with operational responsibilities, often need questions answered and not simply access to reports. The environment needs to develop a capability to address questions across the range of networks and classification levels with the intent of getting an answer. While, in some instances, the answer may be provided completely electronically, in most one or more humans will be participants. A concept of operations for such a capability must be developed, which also identifies the functional technology requirements to support it.
Common search, discovery and analysis tools	Users anywhere in the virtual environment must have access to a common set of tools to find, discover, and analyze information.
Lexicon for information sharing	The proposed environment will need a common definition of terms and dictionaries of competing terms where common definitions are not possible.

Accessible to locally provided tools	In addition to the availability of common tools, local networks (from which the users access the larger environment) have their own tools to help address the local missions. The information in the larger environment needs to be easily accessible to local applications so users can integrate the information in the larger environment into their every day work.
Producer support tools	An environment such as this depends not only on the technology available to the consumer, but also on the ways the producers prepare information for consumption. Producing products in web formats such as HTML and adding consistent and ubiquitous metadata greatly improves the ability of the search, discovery and analytic tools.
Mobile users	The environment needs to be able to support stakeholders from a variety of locations, using mobile hardware (e.g., PDAs, cell phones, text pagers).
Global environment visibility and configuration management	Overarching management of the interoperable environment, including global environment and configuration management, is necessary to assure availability, reliability, restoration, security, integrity, and efficiency. Networks and the environment are always changing. New customers join, new information and connectivity needs are identified, new technology is developed/inserted, new threats appear ranging from viruses and worms through denial of service attacks targeted at vulnerable points in the system as well as end users, network interruptions occur from ice storms, hurricanes and other natural and human error events, and a variety of stresses such as elections, sports events and others constantly require the ability to forecast, see real time and dynamically reconfigure networks and services to meet customer needs. Proactive environment management design and capability enable graceful degradation - a means to ensure when disruptions do occur, rather than collapse catastrophically, services are continued to high priority customers while service to others is provided on a more limited basis or time allowed for saving data and implementation of alternative measures. Exceptions may be necessary for some highly-classified systems.
Reliability	The environment must be available 24 x 7. Support staff needs to be available 24 x 7. Users should have a reasonable expectation there will be no unscheduled down time or unacceptable delays.
Flexibility	The proposed environment must be adaptable to changes in technology and requirements. To the extent possible, the system should be designed and implemented in a way that change can be inserted without the need for a massive redesign.
Data integrity	The proposed environment must contain mechanisms to protect against the unintended or malicious alteration of data. Further, it must provide the means for "cleansing" and "harmonizing" data to ensure the highest number of appropriate correlations. The technology must also capture collectors' assessments of the credibility of the information.

Consistent with privacy, security, policy and resource guidelines

The environment needs to incorporate the requirements pertaining to dissemination rules, standards and policy, and resource considerations.

3. Where We Are Now (AS-IS)

3.1 Existing capabilities in the DHS Enterprise IS&C Environment

Table 2 describes the status of the existing IS&C environment in terms of the 17 functional requirement categories listed in the Functional Requirements section.

Table 2. Existing Environment in Terms of Functional Requirements

FUNCTIONAL REQUIREMENTS AREA	STATUS (As Is)
A virtual trusted sharing environment	Largely non-existent Some networks have been linked to each other to create sharing environment, but these are only islands largely unconnected with other islands. For example, there are networks at the Sensitive Compartmented Information (SCI), Collateral, and SBU levels, but they do not communicate with each other nor do they connect with all the networks at the same security levels. There are also numerous state and local agency networks that neither connect nor communicate with each other nor with the federal government networks. (ISC 2004, 55) The principal steps forward are the DHS and DOJ led HSIN/LEO/RISS networking and the DHS Metadata Center of Excellence work with Global Justice and the Federal CIO Council
Single log on	All users (i.e., information producers and consumers) spend most of their time on the environment provided by their own organizations. Their jobs, in general, span activities beyond counter-terrorism. Their organizations provide them with information and tools they need to perform their jobs. (ISC 2004, 56)
Easy to use	Multitude of portals, non-user friendly interface, inability to transport data across network boundaries
Timely information	Frequently delayed, excess time required to search for and access
Federated queries	ICE, USSS, and IAIP each further identified the key issue associated with accessing timely and relevant data – the lack of standard ways of expressing and recording information in the multitude of relevant databases. (ISCO 2005, 20)
Subscription and pushed information	Push by email with limited and slow search. Essentially no subscription other than commercial open source services
Provide answers to questions when appropriate	Cultural resistance

Common search, discovery and analysis tools	Lack of enterprise access to data
Lexicon for information sharing	The DHS Metadata Center of Excellence is developing a lexicon, a monolingual on-line handbook, and a thesaurus and ontology of abbreviations, acronyms, and terminology. (ISCO 2005, 18)
Accessibility to locally provided tools	Very limited
Producer support tools	DHS needs a better understanding of the needs at the local levels. (ISCO 2005, 21)
Mobile users	Generally not available
Global environment visibility and configuration management	Non-existent
Reliability	Varied
Flexibility	DHS can and will take reports through any media and in any format, without dictating how to report to LE and private sector entities (ISCO 2005, 31)
Data integrity	Varied
Consistent with privacy, security, policy and resource guidelines	The biggest issues in the information sharing problem space are those associated with terminology or semantics. Different communities can, and frequently do, observe the same phenomena and describe it differently (ISCO 2005, 18)

3.1.1 Existing DHS Architectures and EA Efforts

The collection of data and information describing the existing and target DHS information sharing and collaboration environment relies heavily on work that the DHS has done over the past two years in developing an enterprise information architecture. Previous DHS analysis of the architecture has identified gaps, overlaps, disconnects and barriers to DHS information sharing and collaboration. In particular, the DHS architecture version 2.0 reports and appendices have been used to identify what has been done and what is yet to be accomplished in several representations ranging from degree of alignment with the DHS strategic goals to degree of alignment with customers of the information. Further analysis of the architecture is contained in this report to determine what is necessary to complete a description of the As Is and To Be DHS enterprise IS&C environment.

HLS EA Version 2.0, which was released in the fall of 2004, is the most recent version of the EA. In addition, virtually all organizational components of DHS have their own EAs that were created by the Office of the CIO. The architects from all those organizations, including the DHS OCIO architecture team, formed the DHS Architecture Working Group, now called the EA Center of Excellence.

Some other DHS architecture related products include:

- Homeland Security Enterprise Architecture Framework (HEAF)—Guides and standardizes enterprise architecture delivery across DHS
- Security Architecture Framework Extension (SAFE)—Identifies a compilation of the major security work products to be developed as an extension of the DHS EA framework. These work products provide the foundation for ensuring the appropriate security mechanisms are in-place for maintaining the confidentiality, integrity, and availability of DHS systems and data
- EA Governance Structure—Defines IT management practices and EA control structures needed to ensure successful and ongoing EA development, evolution, and impact on DHS.
- Stakeholder Analysis—Identifies and describes key people or organizational entities inside and outside of DHS and the government that have a vested interest in the DHS mission and its delivery

The “HLS enterprise architecture As-Is Characterization” report version 2.0 dated October 12, 2004, provides a framework for analysis shown in 7 based on DHS strategic goals and a value chain that supports achievement of those goals.

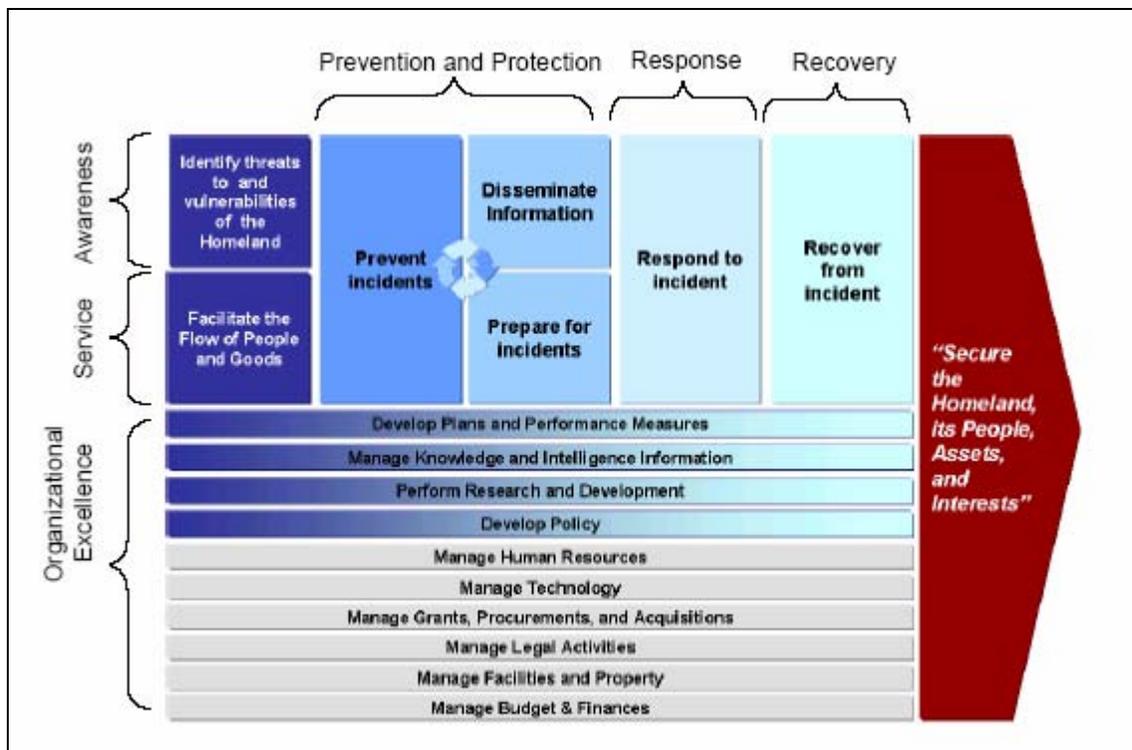


Figure 8. Value Chain

Existing or As-Is capabilities and findings cited in the report are based on data collected through surveys of individual organizations within the DHS. Findings include:

- 1) identification of over 1400 systems across 22 agencies that, to varying degrees, provide information that should be shared and used for collaboration purposes

- 2) as shown in 9 below most systems supported the achievement of organizational excellence as opposed to the other areas in brackets.

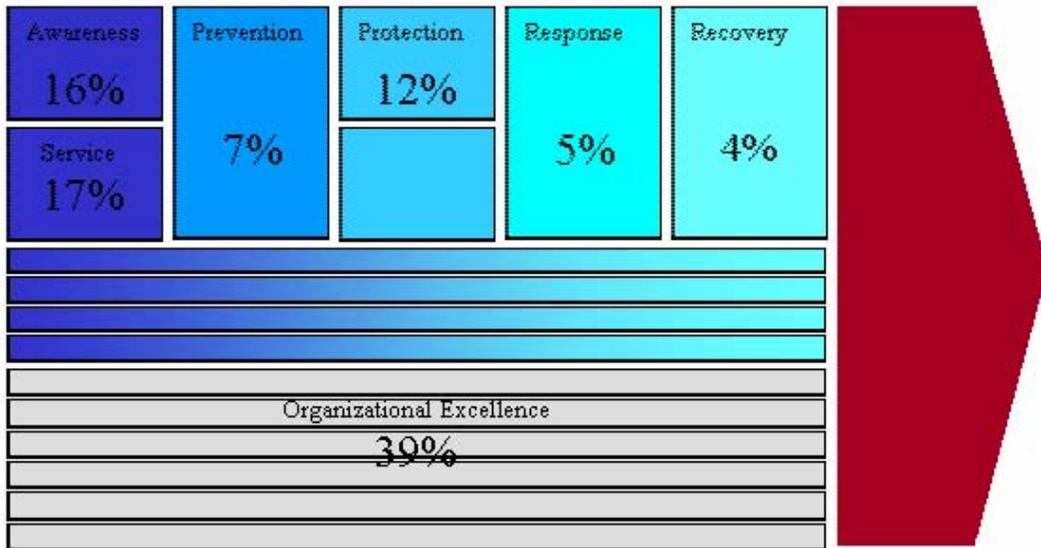


Figure 9. Mapping of DHS Systems to Strategic Goals

3.1.2 Data Resources

Five recently completed and ongoing efforts that have substantially contributed to understanding of DHS systems and their functionality as well as helping to define the as-is environment are:

- 1) The Office of Management and Budget (OMB) Data Request 05-34 requested Data on Investments Supporting Terrorism Information Sharing. The ISCO/CIO and CFO collaborated with DHS components to provide user validated system functionality data. Annex E describes the systems that were identified and their functionality.
- 2) ISCO initiated an eSurvey of mission critical information sources, products, supporting systems, functionality, classification, and users within the DHS. The initial data minus one component has been collected is being queried and collated.
- 3) Information Sharing Agreements (ISA) – ISCO sought to better identify all of the stakeholders who should be included in information sharing agreements (ISAs), commonly referred to as Memoranda of Understanding (MOUs), and memorialize business rules currently in use by these stakeholders. This project was the first step in capturing the As-Is environment for ISAs. During the process, over 192 stakeholders were identified and 27 key stakeholders were interviewed. These interviews enabled ISCO to capture and understand the business rules currently in

place for ISAs. In addition, ISCO was able to validate that the ISA Question Matrix is a valuable tool for assisting in the ISA process. Key findings from this project validated that there is not a standardized process in place to assist those engaged in Information Sharing Agreements (ISAs) nor is there a central repository to capture existing ISAs. ISCO is deploying the Information Sharing Agreement Management System (ISAMS) which will address these key findings and will better facilitate sharing of information within DHS components.

- 4) ISCO initiated a search and summary of all DHS systems for which System of Record Notices have been published. Such notices are necessary for systems containing data which contain personally identifiable information.
- 5) HSOC has initiated an effort to define and develop a Common Operating Picture (COP). The COP will be the primary tool for sharing dynamic, geospatially referenced situational awareness information. The COP will provide a timely, fused, and accurate display of shared information across the enterprise that assists all echelons to achieve situational awareness. The COP is managed information drawn from track, link intelligence, and amplifying data from various information sources. A COP can also be described as an integrated collection of operational information that can be viewed in different ways from different perspectives.

3.1.3 Sources of Information

A wide range of information sources are needed to achieve the goals of this effort. Figure 10 shows key sources of information.

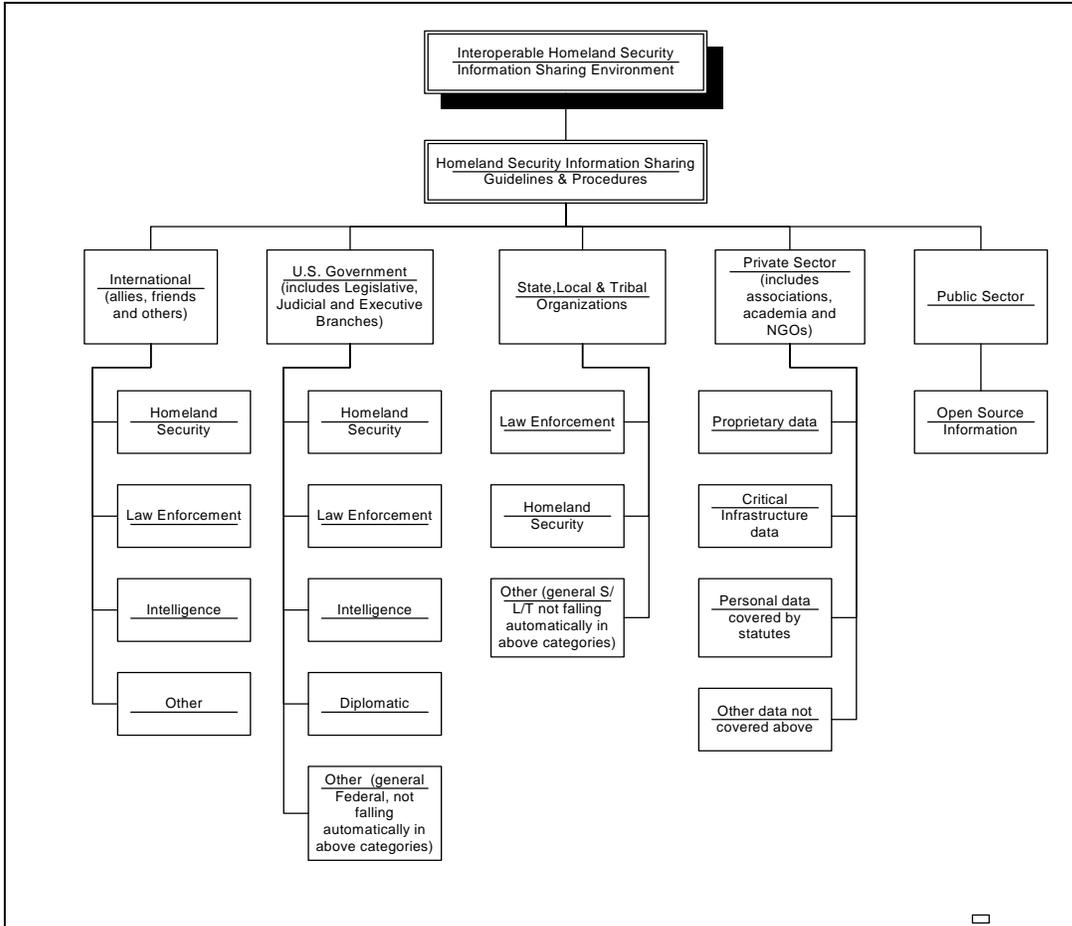


Figure 10. Sources of Homeland Security Information

These efforts now provide a baseline for analysis of gaps, potential synergy and actions needed to help make the DHS whole much greater than the sum of the parts.

3.2 Analysis of As-Is Capabilities

3.2.1 Gaps and Overlaps

Table 3 below shows results of a gap and overlap analysis of the functional requirements for the IS&C environment based on information in the ISC initial plan.

Table 3. Functional Requirements Gaps and Overlaps

FUNCTIONAL REQUIREMENTS AREA	GAPS/OVERLAPS
A virtual trusted sharing environment	There are networks at the Sensitive Compartmented Information (SCI), Collateral, and SBU levels, but they do not communicate with each other nor do they connect with all the networks at the same security levels. There are also numerous state and local agency networks that neither connect nor communicate with each other nor

	with the federal government networks.
Single log on	at this time, there are hundreds of DHS websites and 14 independent DHS portals. A seamless interface is not possible currently and there are disparate architectures; collaborative portal requirements are not being met. (DHS “As Is”)
Easy to use	Due to the lack of common data standards, it is a challenge to locate the record of an individual in multiple systems. This is often due to differences in the spelling of a name or non-standard formats for data fields such as date of birth. Also, there is no linkage between the systems that are used by ICE, nor is there an automated method for searching all systems based on one query
Timely information	Gap
Federated queries	Gap
Subscription and pushed information	Gap
Provide answers to questions when appropriate	Limited, manually intensive and time consuming. Cannot not do all required for multiple incidents
Common search, discovery and analysis tools	To date, there is no common, standard repository or access mechanism for documented research on terrorism that can be shared throughout the Federal, State, and Local communities.
Lexicon for information sharing	One of the potential ISC gaps is the appropriateness and adequacy of the inclusion of intelligence and law enforcement standards as well as the inclusion of existing Intelligence Community (IC) and Department of Defense (DoD) standards in the DHS lexicography products.(ISCO 2005, 18)
Accessibility to locally provided tools	Very limited. Necessary tools not provided to users, e.g., Analyst Workstations
Collaboration tools	Rudimentary and not populated to users, e.g., even VTC use is very limited
Mobile users	Only independent systems, largely unsecured
Global environment visibility and configuration management	Major gap
Reliability	Limited – dependent on email which fails frequently
Flexibility	Limited
Data integrity	Gap
Consistent with privacy, security, policy and resource guidelines	Overlaps in which office in DHS is responsible for establishing enterprise policies and overseeing IT/IM resources.(ISCO 2005, 18) Prior to 9/11, jurisdictional overlaps already existed and federal agencies worked with varying degrees of success to deal with them. Laws, Executive Orders, and other policy documents issued since 9/11 appear to have compounded the confusion. Most agencies agree there is overlap among these documents, but often disagree about who has the specific responsibility or lead.” *(ISCO 2005, 13)• Sharing and collaboration with private infrastructure operators and State and Local (S&L) government organizations is confounded by multiple uncoordinated DHS products or overlapping requests for information. Examples within DHS include S&L representatives receiving redundant warning and threat bulletin information. Private infrastructure owners receive overlapping Infrastructure Coordination Division (ICD) coordination, PSD vulnerability

assessment visits, and Protected Critical Infrastructure Information (PCII) outreach advice. A lead organization needs to be established to identify and resolve these types of issues.(ISCO 2005, 14)
--

3.2.2 As-Is Issues

This section describes some of the high-level policy issues identified in the ISC initial plan.

3.2.2.1 Governance

The issues associated with establishing, building, and maintaining an interoperable terrorism information sharing environment across agencies are long-term. A permanent governance body will need to address issues ranging from investment strategy to recommended changes in law or policy to facilitate the process. Further, the governing body will be needed to coordinate issues such as security clearances and existing but overlapping information sharing programs. It will also need to serve as the arbiter over inter-agency disputes regarding information sharing.

A critical decision in the development of an interoperable terrorism information sharing environment is providing for its management. The environment will have an impact on budgets and operations of all federal departments with any counter terrorism mission, and all state, local, tribal, and territorial organizations addressing counter-terrorism. None will agree to abdicate authority to an organization without their representation. None of the existing counter terrorist or homeland security organizations meet those criteria. Many agencies have broad authority in the areas of counter-terrorism and homeland security, but none have high level management representation across the spectrum of organizations whose budgets and operations will be affected by the proposed environment.

An overarching, permanent governance authority, with representation from key stakeholders to include state, local, tribal, and territorial authorities, is essential for the implementation of the recommendations within this report. Members must have the domain knowledge of the organizations they represent and be sufficiently available to make timely decisions to support daily information sharing. The director of this permanent organization with a full time staff must be given the responsibility and authority to develop and manage the proposed interoperable terrorism information sharing environment. It must have the authority to create working groups to resolve temporary issues. The governance authority will be responsible for establishing the capability and making certain sufficient funding is available to ensure success. The staff must also include a privacy officer, who reviews all activities for privacy issues.

3.2.2.2 Standards and Policies

Executive Order 13356 anticipates a level of intra-governmental cooperation and information exchange far exceeding anything the country has ever attempted. For the effort to succeed, clear policies need to be issued clarifying roles, responsibilities and

missions; common interoperable terrorism information sharing environment standards and procedures across roles (i.e., intelligence, law enforcement, public safety, defense, critical infrastructure, and mitigation of effects) must be established among participants (i.e., law enforcement; defense; homeland security; intelligence; state, local, tribal, and territorial; private sector; and diplomatic); and the scope of terrorism information must be clearly defined. All policies, standards, and definition must be created on a collaborative basis, with all stakeholders represented. In addition to the larger issue of mandating information sharing, there are a host of more detailed policy issues that need resolution.

The procedures for determining who can and cannot see information are complex, inconsistent, and not well defined. It is extremely difficult to know in advance how information will be used and who will need it. Existing policies may discourage information sharing more than they should. For example, as determined through the 45-Day Information Sharing Agreement Business Rules Project (see Annex H), component policies have not been updated since the creation of DHS. Due to this outdated policy, many components treat other DHS components as 3rd party, placing restrictions on the sharing of critical information. As part of an ongoing project within ISCO, these policies will be reviewed and updated. ISCO seeks to develop and implement a policy that views DHS as one entity and does not require components to develop formal information sharing agreements with each other to grant access to systems.

Another issue concerns incorporating private sector data in the environment. There are two types of private sector data of concern: business proprietary data and personally identifiable information. There is a huge volume of data in the private sector, only some of which is useful. Determining what is the useful information subset, locating it, and using it effectively and appropriately will require new technical tools as well as defined relationships between government and the private entities who collect or maintain that data. The handling of business proprietary data submitted as PCII (Protected Critical Infrastructure Information) as defined in the HSA 2002² is addressed in DHS Management Directive 11042. Other business proprietary data not submitted within this process may require different handling. Personally identifiable information (PII) is covered, for the most part, by a variety of laws and regulations, however there are gaps and exceptions that must be addressed depending upon the type of PII collected and how it will be used. When incorporating such information, the public's perception must overwhelmingly be that the protection of privacy, citizen's rights, and property rights are of paramount concern, and that this private sector data is only used when absolutely necessary.

3.2.2.4 Cultural Resistance

Organizations may feel that others do not have the skill or knowledge to interpret and use their information properly. They may feel other organizations do not understand their view of the world, and sharing may mean giving up expert resources to help in the proper

² 6 USC 131(3) and covered by 6 CFR Sec 20.2 and DHS Management Directive 11042.

interpretation of the shared data , making sharing more effort than it is worth. They may also feel there is competition between organizations, in which case sharing might result in a reduction or loss of control over resources.

Cultural barriers to sharing information need to be understood and systematically addressed. Sometimes overcoming cultural barriers is a simple matter of addressing misconceptions. At other times conditions themselves need to be changed. For example, organizations may need help understanding that different communities of interest have different sets of objectives and may still collaborate effectively to share information without necessarily aiming to attain the same goals.

Helping communities develop their own awareness and understanding of other communities' knowledge, problems, and goals may very well be one of the most difficult challenges. Rather than forcing users to agree on a common language and perspective, we might want to lean toward supporting awareness, tolerance, and understanding of how different perspectives differ, and meaningful analogies to facilitate this conceptual translation. Supporting these processes might translate into knowledge seeking and searching tools that attempt to understand the user's core community perspective and guide him toward the most appropriate knowledge sources tailored to his needs. Other awareness tools might help communities frame their knowledge in terms and languages that are most useful to other known communities, developing implicit links between similar concepts and programs. Social awareness and social networking tools would be useful for connecting community members and enabling them to attach meaning to tacit knowledge that was developed in specific contexts.

3.2.2.4 Resources

In building a terrorism information sharing environment to span the stakeholder community, certain resource issues will arise. Where appropriate, common standards for resources must be defined (e.g., security clearance practices, training, and infrastructure requirements). To properly resource this environment a central funding base should be authorized and funded. Special emphasis should be placed upon the following:

- Getting intelligence into actionable information down to the Sensitive But Unclassified (SBU) level as early in the process as feasible
- Expediting and standardizing security clearance processing
- Reciprocity of security clearances between agencies
- Establishing joint information sharing and operations facilities and infrastructure
- Providing necessary common operational services to all participants
- Harnessing and focusing research and development efforts to support information sharing

3.2.2.5 Access and Dissemination Control

Users face a vast, confusing array of systems, databases, networks, and tools that require different access methods and controls. It must be made easier for the user to “enter” the environment and use its facilities. Users cannot be expected to have to remember a large number of different passwords and login paradigms to gain access to the tools and information they need to do their jobs. Experience has overwhelmingly shown that most users will spend the majority of their time on their native environment rather than logging on to a different network. Additionally, the different networks represent different levels of technical maturity forcing them to learn different ways of using the different capabilities. This not only further discourages them from using a different system (that they do not understand well), but can lead to errors.

Even with easy entry, actionable information does not always get to the people who need it when they need it. Timely, actionable information needs to get to those on the front lines of the war on terror: the first responders, law enforcement personnel, and local officials. The actionable information they need often does not need to be classified. Dissemination through use of tear-lines and write-to-release; harmonizing “need to know” with “need to share;” and using open source data responsibly can help. The goal is to permit easy access to the information for appropriately-cleared personnel who have a need-to-know, while denying access to those who do not have the need or the necessary clearance.

While granting security clearances to everyone is not the answer in and of itself, expanding access to classified information for select state, local, and tribal organizational elements is needed. More broadly, we need to produce useful, actionable information by removing the sensitive context that makes it classified and then distributing it in a timely manner to the right people. One of the current impediments is that it is difficult for users to create products that meet the standards so they can be moved to other environments. We need to make it simpler for providers to produce information in sharable and interoperable formats.

3.2.2.6 Collaboration

In the current environment, agencies collaborate through physical acts (e.g., participating in task forces, sending detailees, hand-delivering information) and, to a limited degree, through virtual acts (e.g., through video-conferencing).

Collaboration tools and environments in use today often are not interoperable, making it difficult or impossible for users separated by geography or network topology to effectively reach one another and communicate. Processes, procedures, and technology must be introduced to enable efficient work across organizations, geography, jurisdictions (i.e., foreign and domestic), and domains. There must be a mandate requiring each party with authority over a possible terrorist situation to collaborate. New collaboration processes should provide agency context and/or background for information. Exchange of permanent liaisons should take place at all 24x7 national operations and intelligence/information fusion centers. Collaboration policies should seek to encourage

productive on-going collaboration (e.g., National Counterterrorism Integration Center (NCTCC), Joint Terrorism Task Forces, State and local intelligence/information fusion centers).

Technical collaboration capabilities needing enhancements include white board, context sensitive tip-off, language translation, trans-lingual chat, trans-lingual retrieval, expert contact information, and real-time transcription. Collaboration tools in this environment would also include directories in which individuals or organizations can be located. It means enabling individuals using networks with different security levels to communicate with each other.

Information from one producer is often repeated in many different reports and repositories. Other users in turn may replicate and pass this same information along to others. Users cannot know the confidence they should have in the data. A fact seen in many places might appear to be highly corroborated when in fact a single observation is being repeated many times. A mechanism for producers to easily indicate the source of information contained in a report should be developed. A companion mechanism to display the information to the consumers of the reports would be necessary.

3.2.2.7 Architecture Issues

The EA As-Is Characterization and Attachments, Version 2.0 (EAv2 Report) and the associated HLS EA As-Is Database (EAv2 Database) version 2 is extensive but still incomplete. The EAv2 Database captures some of the salient features of 1,463 systems out of a potential DHS universe variously estimated at between 2,500 and 10,000 depending, in part, upon how the term “system” is interpreted.

USCG systems comprise over 40 percent (540) of the systems in the EAv2 Database. Those systems include radar, altimeter, direction finder, secure telephone, etc. All of these items are accurately described as information technology systems, and many are or should be used in the ISC process. Furthermore, approximately 300 of these USCG systems are owned and maintained by the US Navy but used by the USCG due to their close affiliation and wartime requirements. Other agencies within DHS may not have considered this broader definition of a system responding to the CIO’s data call.

Based on this initial review, there appear to be 37 watch list systems operated by different parts of DHS. These systems are subject to senior management attention, but only seven were identifiable in the Exhibit 300s and only 19 were captured in the EAv2 Database. The problem is likely due to lack of rigorous adherence to naming standards and at least within BTS will be addressed by the Office of Screening Coordination. Similarly, it can be expected that HSPD-11 implementation efforts will help DHS address this issue.

Although the collection of data about DHS systems is not yet complete, ISCO believes that the data support some statistical observations.

1,463 key systems from 12 organizational entities compose the systems inventory.

Over 50 percent of DHS systems do not interface outside of the organization that owns the system.

17 percent of DHS systems interface with only one external entity.

Over 40 percent of EP&R systems do not have internal interfaces.

Over 40 percent of the systems used by DHS support less than 100 users. Approximately 75 percent of the systems represented by the 102 available Exhibit 300s (FY05) (Appendix D) are for systems that began their acquisition life cycle prior to the origin of DHS.

Of the 102 OMB Exhibit 300s, 56 percent of the systems provide back office support.

About 10 percent of systems represented by the 102 Exhibit 300s (FY05) are in development. These systems deserve special attention to ensure they conform to the emerging EA and ISC vision.

Systems are almost evenly split between those that support operational missions and those that support management and administrative functions.

The following series of exhibits is intended to provide an appreciation of how DHS systems are distributed, allocation by strategic goals, and where FY05 investments are being made. Additionally, the EAv2 Database is used to derive an initial number of DHS systems that have a possible information sharing and collaboration capability.

For example, the Interagency Border Inspection System (IBIS) combined access to Border Patrol and INS systems when they were separate agencies, but IBIS had limited utility. The ISC mission and objectives will be better served by adoption of an integration model such as that implemented by the Foreign Terrorist Tracking Task Force.

The OCIO efforts are not focused directly on information sharing and collaboration capabilities however the data does provide some insights. Key data fields in the database provide insight into who uses the data, how it is connected to other agencies, the type of system, and the business use of the system. For example, a system that is described as collecting information, processing it, and then disseminating the data to multiple offices/agencies would be considered an information sharing system.

A comparison of content of three of the related principal efforts is of interest.

The eSurvey focuses on information sources and products used in the Department. Which systems are associated with use of the sources and products is one of the questions asked in the eSurvey. This information source and product data begins a foundation for information flow and business process modeling. It also has expanded the horizon on visibility into business process and information flow. Additionally, it provides insight into questions which can help DHS ensure compliance with law. For example, 179 systems referenced in the eSurvey were reported to contain personally identifiable information

but for which no SORNs have been issued. This data is now in the data cleansing and analysis phase and will be taken back to the components for validation and discussion.

The Common Operating Picture is intended to be the primary environment for sharing dynamic, geospatially referenced situational awareness information. The COP provides a timely, fused, and accurate display of shared information across the enterprise that assists all echelons to achieve situational awareness. It is managed information drawn from track, link intelligence, and amplifying data from various information sources. A COP can also be described as an integrated collection of operational information which can be viewed in different ways from different perspectives.

The COP Integration Team brings together representatives from the DHS organic components/organizations, and other agencies partners and stakeholders to develop a common framework and methodology is necessary for the DHS COP. This is particularly important as DHS moves to a unified structure of sharing information among agencies, and retrieving information from many sources across the enterprise and from external sources. The result of the integration will initially be visualized at the HSOC.

Some of the issues discussed in the COP Integration team meetings include how data flows from organization to organization. One of the main problems is that there are no analysts to drill down and make sense of the data so that the different organizations can use it more effectively. Each organization in DHS has different resources, functions, tasks, capabilities, views, and needs, and will interpret and use the COP for different purposes. In this way, it makes more sense to think of the COP as a Common Operational Database with a Mission Specific Operating Picture (MSOP).

Along these lines, the COP Integration Team believes that it is not the data we need to share, but the *Knowledge*. Questions about the granularity and appropriateness of information need to be asked. If information is available at a very low level (high granularity), then it will be useless to those components that do not have the resources to interpret it. Some organizations worry that sharing information may mean sharing the personnel that are needed to interpret the information, and they cannot afford to share the time of their high quality personnel, compounding the issues and barriers to information sharing.

The COP team has begun to analyze the overlaps and gaps between the surveys of DHS systems under consideration for the COP Implementation. The COP survey includes 87 systems, and the E-Survey includes 251 systems associated with information sources and products. Twenty-one of these systems overlap both the COP and E-Surveys. The combined 94 systems in the COP and E-Surveys represent only 6.4% of the 1464 systems in the Enterprise Architecture (see diagram).

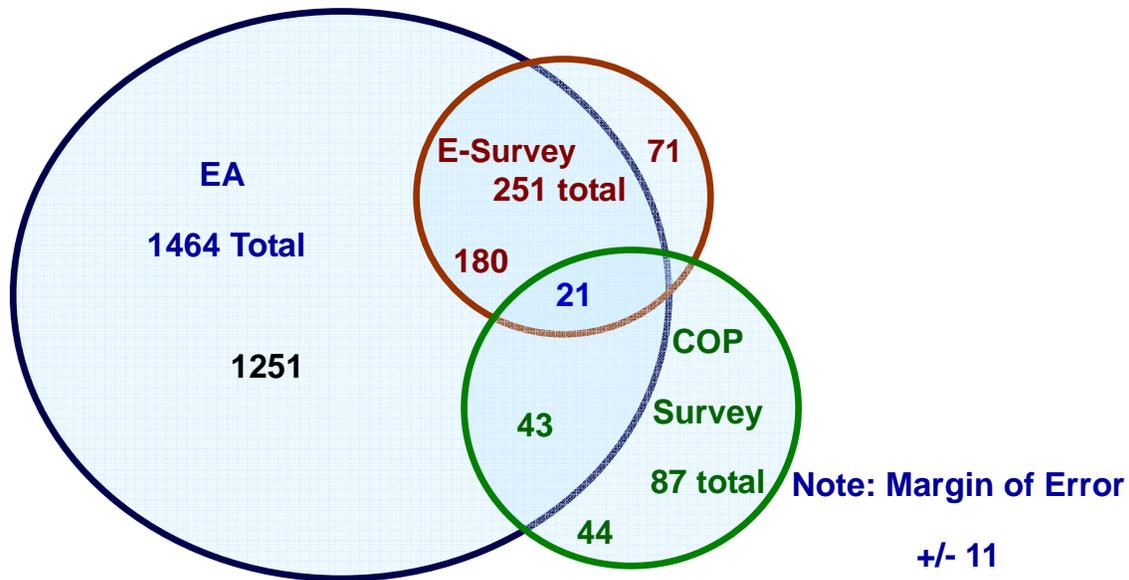


Figure 11. COP Survey, E-Survey, Enterprise Architecture Gaps and Overlaps

Further analysis is needed to determine whether or not the COP Survey is comprehensive enough to serve the needs of the various DHS components and organizations that will rely on the COP for critical operations. Next steps include identifying those information sources and products from the E-Survey that should be considered as part of the COP, and determining whether or not any of the other 1251 systems from the EA should be included. Finally, mappings must be developed between the Information Sharing Agreements (ISA) and the selected COP systems.

A more complete system inventory process is needed so that accurate metrics can help to determine which systems can be consolidated, enhanced, retired or modified to better align with strategic goals and objectives.

Information that is associated with performing key processes that support achievement of strategic goals and functional requirements needs to be identified. This will help to determine the information that needs to be shared and used for collaboration purposes as well as solutions to meet those needs.

In addition, a broader set of gaps and requirements from the ISC report that highlights major implementation issues and risks of not resolving those issues are listed below.

- a. GOVERNANCE
 - i. Information enterprise management
 - ii. Need for common governance standards regarding
 - 1. data standards
 - 2. info protection polices
 - 3. clearance policies/procedures
 - 4. infrastructure/architecture standards
- b. STANDARDS & POLICIES
 - i. Lack of an Interagency Oversight/Management Group (IWG)

- ii. Lack of clarity of roles, responsibilities and missions (who's in charge of what and when)
 - iii. Lack of common information sharing processes and procedures
 - 1. True partnership among federal, state, local, and tribal governments
 - iv. Different standards among agencies:
 - 1. to determine dissemination of terrorism information;
 - a. inconsistent C&A standards
 - 2. what qualifies as terrorism information;
 - 3. who requires the information and
 - 4. when the information is needed.
 - v. Inability to ensure integrity of data from intentional or unintentional alteration
 - vi. Inability to share information gained within a joint organization back to one's home agency (the "rules of the road" issue).
 - vii. Inconsistent decisions between the need to protect sources/methods and the need to (rapidly) share information.
 - viii. Inconsistency between the legal prohibition against certain parts of the intelligence community reviewing public/private information derived in the United States and the fact that a large amount of critical counterterrorism information is in the private/public sector and contains information on US persons.
 - ix. Inconsistent information protection standards from one federal organization to another.
 - x. Data used in a manner inconsistent with or out of context from original intent.
- c. CULTURAL RESISTANCE
- i. Lexicon – differing terminologies which cause failure to communicate appropriate information, severity, or immediacy.
 - ii. Lack of trust when information is shared
 - 1. Fear that shared data will be misused
 - 2. Fear that shared data will be misinterpreted
 - 3. Fear that shared data will be used to beat collector to wider dissemination
 - 4. do not trust that they are receiving all available information
 - 5. do not trust reliability of information shared
 - 6. do not trust products, want raw data and ability to conduct own/alternative analysis
 - iii. Fear of sharing data in violation of privacy laws
- d. RESOURCES
- i. Education of users, senior/middle management
 - ii. Inability to administer security clearance process
- e. ACCESS TO INFORMATION
- i. Content management

1. Lack of uniform methodology to correct errors in data
- ii. Lack of a unified terrorist watch list and the ability for immediate query against it (with appropriate security measures for the list and audits for inappropriate request patterns)
- iii. Inability to access terrorism-related information for federated queries across federal, state, local, and tribal entities
- iv. Lack of integrated collection management
- v. Inability to meet or recognize critical time to pass information between agencies (e.g., person in custody requires speedy response; investigative requests may not need the same level of fast response)
- vi. Significant delays in pushing out possibly critical information out because permission must be granted by the data steward.
- vii. Inability to access right information in a timely manner
- viii. Inability to access data by those managing consequences because security and law enforcement agencies tend to compartmentalize information
- ix. Inability to access threat related information because it is compartmentalized
- x. Inability to fuse data
- xi. Some foreign government laws prevent sharing of information

f. DISSEMINATION CONTROL

- i. Tension between traditional requirement of establishing “need to know” and current recognition of “need to share” because parties are not omniscient and cannot always predict what they would learn.
- ii. Inability to easily and timely move appropriate information from a higher classification network to a lower classification network.
- iii. Information provided by foreign governments is not readily shared throughout the US Government

g. COLLABORATION

- i. Insufficient analysis of collaborative processes
- ii. Insufficient moderation/mediation of collaboration and inter-community processes
- iii. Lack of community and information awareness
- iv. Lack of analysis and inter-agency decision support
- v. Lack of role based access (authorization)
- vi. Failure to consistently include state, local, and tribal representation throughout the information sharing structure (including highest levels)
- vii. Failure to ensure state, local, and tribal understanding
 - a. cultural issue – re: federal sharing
 - b. training

- viii. Lack of analysis and decision support
- ix.
- h. TECHNOLOGY
 - i. Lack of collaborative tools
 - ii. Lack of analytic tools
 - iii. Lack of interoperable analytic tools
 - iv. Lack of infrastructure to access protected/classified/compartmented information
 - 1. facilities
 - 2. licenses
 - 3. training
 - 4. human capital
 - 5. funding
 - v. Lack of an interoperable trusted environment
 - 1. Lack of connectivity among trusted partners
 - vi. Inability to move information
 - 1. as well as across various security level domains
 - 2. Lack of connectivity between necessary partners
(e.g., HSIN/JREIS, CISANet, LEO, RISSnet, JWICS, SIPRNET)
 - vii. Lack of system support for collaboration
 - 1. Directories
 - 2. User Validation
 - 3. User & Community awareness
 - 4. Information & knowledge sharing
 - 5. Organizational learning & understanding
 - 6. Synchronous and Asynchronous mediated interaction
 - 7. Access to experts & expertise
- i. INDUSTRY AND NON-GOVERNMENTAL ORGANIZATIONS
 - i. Fear that sharing industry critical infrastructure vulnerability information with the government could be used by the government in legal action against them.
 - ii. Insufficient numbers of cleared members of industry with whom to share classified threat assessments (especially critical infrastructure)

In addition to the categories defined by the ISC, the following category was added to provide more focus on specific issues

- j. FOREIGN GOVERNMENTS
 - i. Inability to share information among coalition and US Only networks.
 - ii. National Disclosure & DCI Disclosure policy
 - iii. Affects timeliness

- iv. Multiple disclosure policies at individual Federal-non-IC/
State/Local/Tribal jurisdictions
- v. Fear and mistrust by foreign governments of US Government
misuse of their information
- vi. Foreign government stovepipes preclude sharing/action within US
Government

The war on terror is a global war. National boundaries have been a haven for terrorists who find they can take haven by moving from one country to another. One of the ways our country can combat terrorism is to support cooperation with our allies and coalition partners. They can help both by providing us information and by apprehending terrorists inside their borders. Information sharing with our allies and coalition partners has the same kind of benefits as sharing information between U.S. government organizations. The environment needs to be able to permit the exchange of information with our foreign partners.

3.2.3 Security (Information Assurance)

Information Assurance addresses the full range of measures taken to assure the timely protection and delivery of information. It includes measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. The measures include providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

Key concepts and definitions in information assurance include:

- **Authentication:** security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
- **Availability:** timely, reliable access to data and information services for authorized users.
- **Confidentiality:** assurance that information is not disclosed to unauthorized individuals, processes, or devices.
- **Integrity:** protection against unauthorized modification or destruction of information.
- **Non-repudiation:** assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Information Security and Assurance Services are used to ensure reliable data is shared with the right individuals for appropriate reasons. Included in these types of services are

things like authentication (verify users), authorization (verify whether users are authorized to access a particular resource in a given location or environment) and audit (verify that the authentication/authorization rules are being adhered to and to investigate possible misuse).

In an environment that maximizes information sharing, it is critical to ensure that information technology will be used to protect information from abuse or misuse. Anonymization technology should be applied by users to the greatest extent possible. If properly applied, it will allow multiple information holders to collaborate and analyze information while simultaneously protecting the privacy and security of the information.

3.2.4 Needs Analysis

The following initial electronic services capability needs have been identified. Electronic services should

- Be created on a collaborative basis, with all stakeholders represented, promoting a culture of open, active, and appropriate collaboration
- Implement consistent policy guidelines and technology to enhance accountability and facilitate oversight, ensuring users have access to all the information they are entitled to, but restricting their access from information they are prohibited from seeing
- Provide actionable and timely information to end users at all levels who need it, regardless of network, while appearing to the user as though the environment is a seamless, trusted environment
- Ensure information is provided with appropriate context to maximize its usefulness, indicating to consumers in appropriate detail the sources of information contained in a report, and the confidence assessment of those sources
- Ensure that all new information, and active legacy information, is registered and tagged using common metadata standards, to facilitate timely and accurate search and information discovery, data quality, and data confidence
- Ensure that all information is protected appropriately to protect against the unintended or malicious use or alteration of data, building in proactive protection of individuals' privacy and civil liberties into policies, processes, and procedures
- Leverage ongoing efforts and build upon current capabilities, while maintaining flexibility to respond to unanticipated needs as they arise maintain and eliminating single points of failure

3.3 Law and Policy

This section addresses major legal and policy considerations concerning information sharing.³ Law and policy provide both imperatives and constraints on information sharing. Statutes, executive orders and other documents address the types of information to be shared and the purposes of sharing and whether information must, may or may not be shared. They may prescribe whether there are constraints on with whom information may be shared or how sharing may occur. Additionally, whether information to be shared is proprietary or confidential, or classified in accordance with national security directives⁴ also complicates the information sharing issue.

3.3.1 Context

Three major elements constitute the context of the legal and policy background for this plan: (1) statutory definitions of “homeland security information” and “terrorist information”; (2) the communities that constitute the sources of information described earlier in this plan (homeland security, law enforcement, intelligence, defense, diplomatic, state/local/tribal, and private sector); and (3) the types of information (on people, places and things) to be shared.

3.3.2 Process

The primary statutory source directing information sharing is **HSA 2002**⁵, which contains explicit language mandating the sharing of homeland security information. It contains sections providing both broad access authority for the Secretary, DHS, (§ 202) and a wide-ranging information sharing mandate—including a requirement for the use of “information sharing systems”—related to homeland security (§ 892). Specifically, “under procedures prescribed by the President, all appropriate agencies, including the intelligence community...shall, through information sharing systems, share homeland security information with Federal agencies and appropriate state and local personnel to the extent such information may be shared...” Section 892 defines “homeland security information” as “any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; and (D) would improve the response to a terrorist act.”

³ Much of this discussion comes from CRS Report for Congress RL32597, Information Sharing for Homeland Security: A Brief Overview, January 10, 2005.

⁴ EO 13292, “Further Amendment to Executive Order 12958 As Amended, Classified National Security Information”, 25 March 2003. This document prescribes a uniform system of classifying, safeguarding, and declassifying national security information.

⁵ HSA 2002 PL 107-296, 116 Stat. 2135.

Prior to this definition of homeland security information, five subsections establish procedures and conditions regarding such information. The first of these requires the President to prescribe and implement procedures under which relevant Federal agencies (A) share relevant and appropriate homeland security information with other Federal agencies, including the Department [of Homeland Security] and appropriate State and local personnel; (B) identify and safeguard homeland security information that is *sensitive but unclassified*; and (C) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information [from its protected status], as appropriate, and with which such personnel it may be shared after such information is removed.

Neither this section nor the other provisions of the Homeland Security Act define what constitutes “sensitive but unclassified” homeland security information. The remaining portions of the subsection require the President to “ensure that such procedures [as he prescribes] apply to all agencies of the Federal Government”; stipulate that these new procedures “shall not change the substantive requirements for the classification and safeguarding of classified information”; and specify that the new procedures “shall not change the requirements and authorities to protect [intelligence] sources and methods.”

The second subsection prescribes refinements to the procedures established by the President pursuant to the first subsection. “Under [the] procedures prescribed by the President,” it is stated, “all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with” the President’s procedures, “together with assessments of the credibility of such information.” Each of these information sharing systems must (A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ; (B) have the capacity to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient’s need to know such information; (C) be configured to allow the efficient and effective sharing of information; and (D) be accessible to appropriate State and local personnel.

Other provisions require the establishment of conditions on the use of shared information “(A) to limit the re-dissemination of such information to ensure that such information is not used for an unauthorized purpose; (B) to ensure the security and confidentiality of such information; (C) to protect the constitutional and statutory right of any individuals who are subjects of such information; and (D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.” The information sharing systems are to “include existing information sharing systems, including, but not limited to, the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.” Federal agencies having access to information sharing systems have access to all of the information shared in those systems. The prescribed procedures are to “ensure that appropriate State and local personnel are authorized to use such information sharing systems (A) to access information shared with

such personnel; and (B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.” This shared state and local information is to be reviewed and assessed, under procedures prescribed jointly by the Director of Central Intelligence (DCI) and the Attorney General, by each appropriate federal agency, as determined by the President, and integrated with existing intelligence.

The third subsection authorizes the President to “prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected” after being reviewed for removal from its protected status. To facilitate such sharing, a “sense of Congress” provision recognizes the use of background investigations and security clearances, non-disclosure agreements regarding sensitive but unclassified information, and “information sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation, the Anti- Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups.”

The fourth subsection specifies that the head of each affected agency shall designate an official having administrative responsibility for that agency’s compliance with the information sharing requirements of Sections 891-899. Finally, the fifth subsection states: “Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information.” Presumably, it is the President who prescribes the referred-to procedures. Significantly, information shared with a “subnational” (state or local) jurisdiction pursuant to these procedures remains under the “control” of the providing federal agency and, because the information is under federal “control,” it is beyond the scope of state information access or freedom of information laws.

Executive Order 13310, issued on July 29, 2003, assigned responsibility for preparing the Section 892 homeland security information sharing procedures to the Secretary of Homeland Security. Others, in accordance with the provisions of E.O. 13310, provide input, including the Attorney General, the DCI, and specified officials with whom the Homeland Security Secretary is to coordinate. [IR&TPA 2004 may have superseded this E.O.]

Language in **IR&TPA 2004**⁶ addresses establishing an Information Sharing Environment (ISE) “for the sharing of *terrorism information* in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties...[that] provides and facilitates the means for sharing terrorism information among all

⁶ IR&TPA 2004, P.L. 108-458, § 1016(b)(1)-(2).

appropriate Federal, State, local and tribal entities, and the private sector...” [emphasis added].

The matrix at Table 1 lists these statutes and others that may have some applicability regarding the various sources of information and mandates for sharing.

3.3.3 Control and Ownership

Who “owns” or controls information matters. As stated above, HSA 2002 makes federal ownership of information shared with states explicit so that state information sharing and freedom of information laws will not apply to it. The reverse also applies: state data shared with a federal agency may be subject to federal FOIA disclosure if it is deemed to be a federal “agency record.”

3.3.4 Constraints

The constraints or limitations to the sharing of homeland security information are of two types. The first is concerned with national security information and classification of that information to protect it from disclosure to those who would do the U.S. harm. The second type concerns information about U.S. persons (whether financial, medical or other types of personal information) and how that information is to be protected to protect privacy and civil liberties.

Constitutional restrictions, derived chiefly from the First, Fourth and Fifth Amendments, limit the collection and use of “association” information that infringes on freedom of speech, association or religion, information derived from “unreasonable” search and seizure, information obtained from a person that might be considered a form of self-incrimination or information obtained in ways that are deemed invasive of personal privacy.

Privacy Act of 1974⁷ This statute is the primary constraint to sharing of personal information by Federal Departments and Agencies. Section 552a(b) proscribes the sharing of personal information between agencies. It states that “no agency shall disclose any record which is contained in a system of records by any means of communications to any person, or *to another agency*, except pursuant to a written request by, or with prior written consent of, the individual to whom the record pertains....” unless one of twelve specified exemptions applies. Because the Privacy Act predates the creation of the Department of Homeland Security, none of the specified exemptions are clearly applicable to homeland security information sharing and none of the statutes mandating homeland security information sharing or terrorism information sharing have created an exemption.

⁷ Privacy Act of 1974, 5 USC § 552a(b)

A number of other pre-existing statutes either explicitly or by implication may limit homeland security information sharing. These include:

Computer Matching and Privacy Protection Act of 1988

Foreign Intelligence Surveillance Act of 1978 (FISA)

Electronic Communications Privacy Act of 1986 (ECPA)

Health Insurance Portability and Accountability Act (HIPAA) of 1996 (medical information)

Gramm-Leach-Bliley Act of 1999 (also known as Financial Modernization Act) (consumer financial information)

Table 4 also lists additional statutes containing constraints on sharing of information.

3.3.5 Sources

Sometimes the type of source from which information is obtained limits its use. Examples of such sources include wiretaps, grand jury testimony, law enforcement searches, patent applications and information obtained under a variety of non-disclosure arrangements. While these source-based restrictions derive from a wide variety of statutes, rules, court decisions and other sources, they have in common that they strictly limit the use of information to the purpose for which it was originally obtained *and no others*. Often the basis for the restriction is constitutional, frequently based on Fourth Amendment or Fifth Amendment concerns touching on unreasonable search and seizure or self-incrimination concerns. In other cases it may rest on the proprietary or “ownership” nature of information that originates in the private sector.

The DHS Information Sharing and Collaboration Policy Framework shown in Table Four provides an initial means of structuring and viewing the wide variety and overlap of constraints and barriers.

Table 4. DHS Information Sharing Policy Framework

Information Sharing Legal & Policy Documents	Law Enforcement	Homeland Security	Intelligence	Defense	Diplomatic	Federal (general)	State, Local, Tribal	Private Sector	Personally Identifiable Information (PII)
Statutes									
National Security Act of 1947 (NSA 1947)									
Atomic Energy Act of 1954									
42 USC 3796h (2004) (From The Omnibus Crime Control and Safe Streets Act), 1968									
Fair Credit Reporting Act of 1970 (FCRA)									
Privacy Act of 1974 (PA1974)									
Air Transportation Security Act of 1974									
Family Educational Rights and Privacy Act of 1974 (FERPA)									
Foreign Intelligence Surveillance Act of 1978 (FISA1978)									
Electronic Communications Privacy Act of 1986 (ECPA)									
Computer Security Act of 1987									
Computer Matching and Privacy Protection Act of 1988									
Computer Matching and Privacy Protection Amendments of 1990									
Computer Fraud and Abuse Act of 1984 (CFAA)									
Drivers Privacy Protection Act of 1994 (DPPA)									
Paperwork Reduction Act of 1995 (PRA1995)									
Health Insurance Portability and Accountability Act (HIPAA) of 1996									
Telecommunications Act of 1996 (Customer Proprietary Network Information CPNI)									
The Intelligence Authorization Act of 1997									
Gramm-Leach-Bliley Act-Financial Services Modernization Act of 1999 (GLB)									
USA Patriot Act of 2001									
Aviation and Transportation Security Act of 2001									
E-Government Act of 2002 (E-Gov2002)									
Homeland Security Act of 2002 (HSA2002)									
Homeland Security Information Sharing Act of 2002									
Critical Infrastructure Information Act of 2002 (CIIA2002)									
Arming Pilots Against Terrorism Act of 2002									
Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA2004)									
DHS Authorization Act FY2006 Title II Subtitle B§216									
CALEA									
Freedom of Information Act (FOIA)									
EOP/Federal Policy									
EO 12333, Of United States Intelligence Activities									
EO 12958 Classified National Security Information									
EO 13292 Further Amendment to Executive Order 12958, as amended, Classified National Security Information									
EO 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001									
EO 13311, Homeland Security Information Sharing									
EO 13356 Strengthening the Sharing of Terrorism Information to Protect Americans									
HSPD 6, Integration and Use of Screening Information									
HSPD 7, Critical Infrastructure Identification, Prioritization, and Protection									
HSPD 11, Comprehensive Terrorist-Related Screening Procedures									
OMB Circular A-108 Responsibilities for the Maintenance of Records about Individuals by Federal Agencies									
OMB Memo M-99-05 Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"									
FTC Rules & Regulations									
FCC Rules & Regulations									
DOJ Policy									
IC Policy									
PCII Rules									
TSA Transportation Security Regulations (re:Sensitive Security Information SSI)									

4. Implementation Plan (Roadmap)

DHS is an operational Department with a NOW mission. It cannot just stop business to plan and implement new systems. Further, DHS operates within an environment of other communities with their own governance models, and so actions it takes must take consideration of DHS operational functions and missions as well as those of the key stakeholders we represent and interoperate with. This portion deals first with the ISE environment and then additional DHS specific considerations.

The EO 13356 Implementation Plan included a phased approach to implement enterprise ISE capabilities as shown below. DHS systems and activities defined as of November 2004 are included. Additional DHS specific needs and recommended actions are discussed following outline of the ISE Implementation plan.

4.1 Strategy

Two key concepts form the strategy for establishing the DHS enterprise IS&C environment capability. The first is planning, management, and oversight activities consisting of 1) a federated governance approach, 2) domain portfolio management and 3) a phased acquisition approach. The second concept is that of critical success factors.

4.1.1 Planning, Management, and Oversight

4.1.1.1 Federated Governance

Federated systems are the best commercial practice for quickly achieving information sharing across disparate legacy systems. The following discussion outlines factors appropriate to establishing federated systems in a DHS context, followed by a discussion of governance. Necessary to the successful systems operation of federated systems is participation by key stakeholders in governance.

Alignment with the management processes of the DHS as well as the broader enterprise is essential in order to successfully plan, manage, and oversee the establishment of the IS&C environment. Since the DHS comprises 22 federal organizations and the broader enterprise has many additional autonomous organizations, a business plan for transition from the existing to an improved environment is best implemented with a strategy that is based on the guiding principles of a federation.

For the DHS enterprise the planning, management and oversight of programs and initiatives can be federated by dividing efforts between Enterprise and Component levels, as illustrated below.

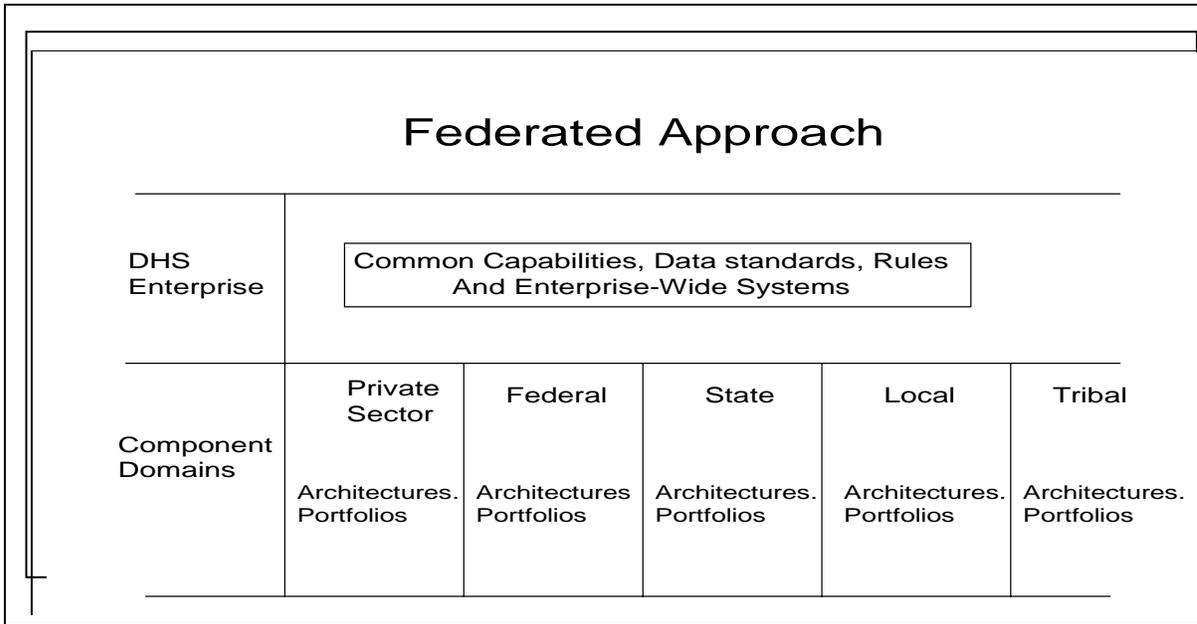


Figure 12. Federated Approach

DHS Enterprise level – A DHS-wide solution for a set of information capabilities with oversight by DHS headquarters. This level deals with capabilities, rules, data standards and operating requirements that are DHS-wide as established by statute, policy, or long-standing practice, and the systems that support those capabilities. It also includes DHS-wide system implementation efforts. The DHS enterprise information architecture will incorporate these capabilities, rules, and requirements.

Component Level – A Component-specific solution for a set of information capabilities, managed by the Component. This level deals with capabilities, business rules, and associated systems currently delegated to the DHS internal organizations or assigned to external organizations via statute, policy or long-standing practice. Component architectures will reflect component-specific capabilities, rules and requirements.

All capabilities to support DHS mission requirements, and the programs to implement those capabilities, will be defined and managed at the appropriate level.

Under the direction of a DHS oversight process, DHS will define and declare capabilities that should be common throughout the DHS enterprise and direct the implementation of enterprise-wide systems with greater visibility at the highest levels of leadership within the Department. Initially, the highest priority DHS-wide transformation efforts will be managed at the enterprise-level with the remaining programs managed by Components.

Over time, more capabilities that are common across Components may be managed at the DHS Enterprise-level.

Under this Federated approach, the DHS will leverage on-going efforts and balance the potential of high yield, higher risk enterprise-wide efforts (which could achieve the greatest DHS-wide efficiencies), against the promise of lower risk Component efforts, whose benefits by definition would be component-specific.

4.1.1.2 Portfolio Management

A second key feature for establishing the DHS enterprise information sharing and collaboration environment is the use of portfolio management techniques to plan, manage, and oversee activities in each component of the DHS enterprise. During each phase of the DHS enterprise information sharing and collaboration program (IS&CP), a portfolio of projects requiring investments in specific DHS enterprise component should be developed and maintained in the three categories shown in Figure 13. Legacy refers to those projects and services that are currently operational. Improvements are enhancements to existing capabilities. Frontier projects are intended as advancements beyond the state of the art. The mix of projects in the three categories can change over the life of the IS&CP. In addition, projects that start in one category may be transferred to another category as the project matures.

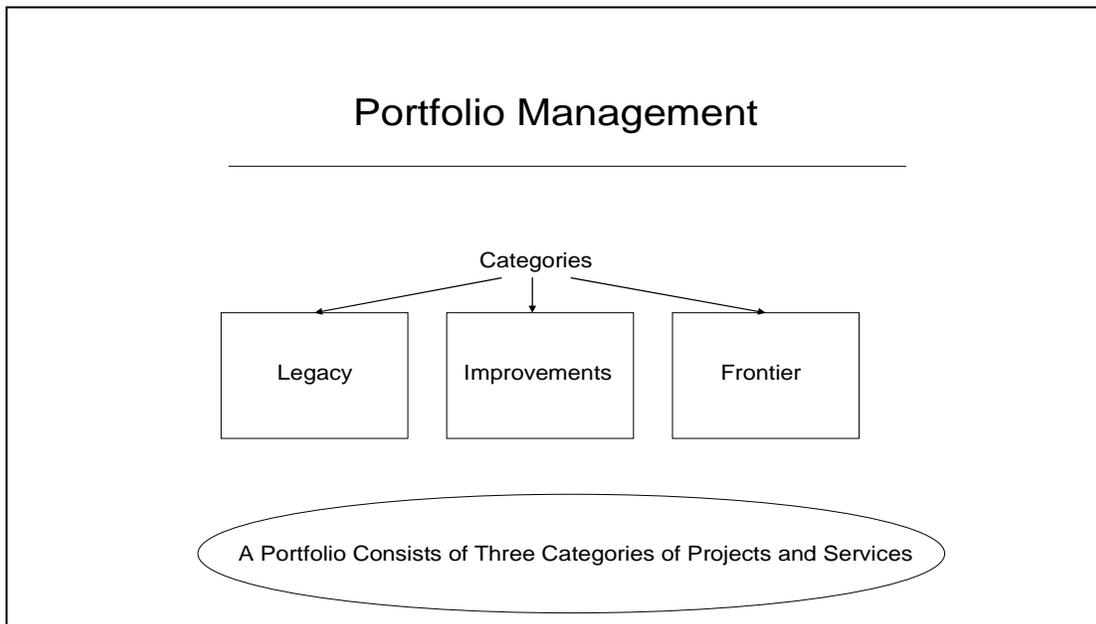


Figure 13. Portfolio Management

4.1.1.3 Phased Acquisition

A phased approach to implementation of the IS&C environment capability that is event driven and allows time for socialization to occur can increase the chances for successful change in performance in a timely fashion. Phased increments of planned changes are described below.

Phase 1 (Near Term– 6 months). Initiate the development and deployment of the proposed environment. Establish a governance authority with key stakeholder participation to provide interagency oversight and management of the environment. Prioritize, complete and/or expand ongoing initiatives to expedite information sharing

Phase 2 (Initial Operating Capability or IOC – 18 months). Implement search capabilities across all appropriate information, email across the community and chat functioning across security domains for all major federal, state, local and tribal networks included in the environment.

Phase 3 (Enhanced Operational Capability – 36 months). Achieve robust capability for most of the requirements of the environment. Users will be able to easily and reliably access timely information relative to their missions, find other users and integrate information from other sources. Publishing, subscription and discovery tools will be operational.

Phase 4 (Beyond 36 months). Add capabilities reflecting changes in threat methods and capabilities, technology, enhanced semantic web services and application of Research and Development products.

4.2 Critical Success Factors

Several key success factors are critical to achieving success in information sharing and collaboration. The first is overcoming cultural barriers to information sharing and collaboration. The second is demonstrating the value of information sharing and collaboration. Others include fostering trust and respect, establishing effective, timely and appropriately secure communication, obtaining top management support, ensuring organization leadership continuity, and generating clearly identifiable membership benefits.

4.2.1 Cultural

Successful information sharing...has as much to do with personal relationships and clearly defined processes as it does with information technology. (ISCO 2004)

DHS sharing of information must incorporate processes and structures for defining and shaping the culture of the relevant community of practice, and the behavior and interactions of its members. This must include formal training elements, but it must also take into account the social fabric of the organizations involved.

Planning must go beyond the mere sharing of information. Frequently, what is most important are what insights are gained and what inferences are drawn from available

information, not the information itself. Indeed, people can have access to information without even noticing it, or noting its potential significance. Too much information can be as bad as too little. Selecting and interpreting that which is important will depend on a complex set of attitudes, biases, prejudices, and preferences as well as the supporting infrastructure, tools and availability of information itself. These qualities depend on the people involved, their interactions, and the cultural norms of the organizations of which they are members. Improvement in how data is interpreted and understood, not merely whether it is shared, must be a chief goal of any business strategy.

People relate not only to information, but also to one another, according to their own proclivities, the social (including professional, educational, and peer) group of which they are members, and the nature and function of the organization to which they belong. These factors determine how individuals will use information, and its potential utility to them. The business strategy must take these elements into account, and incorporate procedures for accommodating them.

Modulating, and if necessary creating, appropriate attitudes and behavior, must be an integral part of the business strategy. For this reason, creation of cross-disciplinary groups and teams that cross organizational boundaries is crucial for real information sharing. The size and composition of these groups, whether formal or informal, will determine what information is shared and how that information is exploited. Studies have shown that small groups are better than large groups for sharing insights. Existing groups—especially those that are informal—must be identified, and where necessary, procedures instituted that will induce positive behavior. However, since DHS is a new organization and many of the interactions required will be with organizations not previously in intimate contact, new affiliations and working relationships will need to be fostered.

Furthermore, processes must be instituted that will nurture positive behavior in such groups. In a successful collaborative group, the vision, style, and culture of the group shape and reinforce the behavior of members even when they are not interacting with members of the group. The group can help members develop a shared understanding of basic concepts, master new techniques, hone the members' ability to speak the jargon of their own discipline or related disciplines, orient members on the issues or questions of the day, act out those issues in discussions or arguments, and provide a social cement for members' interactions.

Behavior, including the sharing of information and its interpretation, occur in informal as well as defined organizational structures. The business plan must implicitly address both. Often, information that is shared is itself of minor importance, but the sharing serves to build rapport and understanding within a group or between individuals, or is meant to articulate, demonstrate, or foster, a shared commonality of interests, goals, or values. Particularly because of the disparate nature of the organizations among which DHS must coordinate and collaborate, infrastructure and processes must incorporate mechanisms for socializing these functions among its partners.

The plan must address how the collaborative groups or individuals operate. Groups, consisting even of only a few members, have internal structure. This structure may be externally imposed, or it may develop informally. Nurturing a structure and a set of focused activities apt to result in useful collaborations of group members, including the sharing of information and of insights, and the development of a common language and a shared perspective, is an essential component of any successful information sharing program.

In summary, effective collaboration is not just about sharing information. It is about a complex of issues involving social behavior among people. These issues must be addressed if the sharing of information is to be useful.

4.2.2 Value of Information Sharing and Collaboration

The value enabled by information sharing and collaboration is partly about being able to meet requirements from Congress, the President and other internal customers, but it is also about being able to understand the broader benefits (and costs) to the Federal government, the nation and the world. The value proposition embodies the tenant of a common goal in the community involved with the ISE.

A key aspect of translating this to the ISE is the well-known principle of getting the right information, at the right time and the right place to the customer.⁸ Important opportunities to prevent terrorist attacks and the impact can be lost by not employing information effectively and not collaborating across organizations. Understanding, measuring, and using these types of value chains is critical to proving a business case to guide how much should be spent on information sharing against the return on investment, and most importantly when decisions have to be made between alternatives, these decisions can be well informed on the value and benefit possible. Thus, metrics need to be established to measure the value of information sharing and collaboration.

Value Proposition: To make the DHS whole greater than the sum of its parts. This is accomplished by creating and executing logical links between action and payoff. Examples include customer intimacy, product-to-market excellence, and operational excellence.⁹

Other views of the value proposition are that the ISE should be able to improve:

- growth and innovation in organizations,
- productivity and efficiency,

⁸ It's the Data: Getting the Right Data in the Right Place at the Right Time, Robert Grossman, http://www.uic.edu/cba/crim/CrimNewsFiles/Colloquia/Grossman_11-08-02.ppt

⁹ If Only We Knew What We Know, Carla O'Dell and C. Jackson Grayson, Jr., The Free Press, 1998

- customer relationships,
- employee learning, satisfaction and retention, and
- management decision-making.

It has been noted that an organization's self-knowledge must be tied to knowledge of its customers, their hierarchy of needs, and leverage these points at moments of potential value.¹⁰

These customers need to be aware of, prevent, protecting from, respond and recovering from terrorism and non-terrorism disasters.

Customers have a variety of alternatives for dealing with their missions. In many cases, organizations can establish their own internal sources of information and expertise, or perform their functions with less information or capability. The key areas that ISE will provide value to the nation in dealing with terrorist and disaster threats are:

- Increased efficiency, speed and productivity of operational and human resources;
- Integration of disparate data sources for more robust analyses; and
- Elimination of errors / Confidence in analyses.

4.2.3 Other Critical Success Factors

In 2001, the GAO conducted a study (GAO 2001, 7) to identify critical success factors in building information sharing relationships that can benefit critical infrastructure protection. It found five critical success factors.

1) Foster trust and respect

Trust is critical to overcoming the reluctance to share information for fear of disclosing weaknesses, vulnerabilities, and other confidential or proprietary business information to other members, some of whom were business competitors. Trust must be built over time and through personal relationships. Some steps that can be taken to facilitate the trust building process include:

Regular meetings to discuss issues and establish face-to-face contact

Consistent member participation - trust was built most effectively when members consistently attended and participated in the organizations' activities.

¹⁰ Into the Networked Age; James Cortada; 1999 Oxford University Press

Evaluation of prospective members - Most followed established procedures or performed background checks to evaluate prospective members before allowing their participation.

Atmosphere of mutual respect among the members so that each member's issues and expertise merited consideration as well as subordinating individual or individual organizations' interests to the interests of the entire information-sharing group.

Procedures for handling violations of the rules because any violation of trust undermined the organization's purpose and diminished members' willingness to share in the future.

- 2) Establish effective, timely, and appropriately secure communication through

Regular meetings,

Information technology, such as web sites or secure telephone lines to facilitate communication. The organizations tended not to use email for security reasons, favoring phone calls and regular mail.

Standard terms and reporting thresholds so that communications could be easily and consistently understood.

Member input in developing new systems and mechanisms for communicating information, thereby better fulfilling member needs and giving the members a sense of ownership in the system or product.

- 3) Obtain top management support to *share information and obtain funding.*
- 4) Ensure organization leadership continuity through personal long-term relationships and institutionalizing roles.
- 5) Generate clearly identifiable membership benefits such as

Access to other experts.

Exposure to cutting-edge technology.

Shared lessons learned.

Real-time assistance in response to problems.

More cooperative relationships with law enforcement entities than would have otherwise occurred.

Better overall security of the nation's critical infrastructures.

4.3 EO 13356 and IRPTA Requirements

On December 17, 2004, the President signed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which included provisions for the re-designation of the Information Systems Council created by EO 13356 to the Information Sharing Council, and for the presidential appointment of a Program Manager to develop the Information Sharing Environment with phased requirements and milestones. DHS must also interface with these requirements. The four phases of the Implementation Plan are now described in detail.

1. Phase 1 – Near Term (6 Months)

In order to successfully implement the proposed environment, a coordinating organization, either the Council or its successor, must provide overall interagency oversight/management. With representation from all participating sectors, this organization will be responsible for the initiation and sustainment of the overall endeavor.

The coordinating organization needs to be vested with the responsibility and authority to approve proposed environment-wide policies on sharing terrorism information and the authority to commit the necessary resources to implement the sharing environment.

The near term plan anticipates the delivery of substantial improvements in information sharing using existing programs and funding. These near term improvements can be accomplished without implementing new policies or additional funding. This is based on the assumption the approval of the plan by the coordinating organization will provide enough impetus and priority to result in delivery of planned products earlier than currently anticipated.

At the end of the first 6 months, the fusion center pilot will not only provide improved information sharing between state, local, and tribal fusion center networks and the SBU networks, but will provide a proof-of-concept interconnectivity among networks across all sectors at various security levels is possible. The capability to share SBU information with the state, local, and tribal agencies is a crucial first step in getting vital information to the first responders. The successful pilot implementation will serve as the model for quickly expanding the capability across all networks and sectors. These efforts include:

Phase 1 – Near Term (6 Months)		
Task #	Task Name	Task Description
1	<i>Connect Existing Networks</i>	Accelerate the planned interconnection of existing networks at the SECRET, Collateral, and SBU levels.

2	<i>Conduct State Fusion Center Pilot</i>	Implement a pilot linking a state fusion center to the newly linked SBU networks (as described in Task #1). Pilot participants will be provided assistance and expertise on the linked networks to help them take advantage of the new technical capabilities.
3	<i>Make Information Available Across Networks</i>	Implement the capability which will provide high priority information from the network on which it was generated to networks on which it is needed.
4	<i>Accelerate Real-Time Electronic Access</i>	Accelerate real-time electronic access to the Terrorist Screening Database to Federal, State, Local, and Tribal law enforcement communities.
5	<i>Expand Access</i>	Expand the Terrorist Threat Integration Center On-Line information to second party and coalition partners.
6	<i>Expand Delivery</i>	Accelerate the delivery of the integrated wireless network activities by DHS, DOJ, and Treasury.
7	<i>Establish Necessary IOC Foundation</i>	<p>Much of the activities to be accomplished in Phase 1 will establish the necessary foundation for the initial operational capability (IOC) delivered by the end of Phase 2. These activities include:</p> <ul style="list-style-type: none"> • Establish initial lexicon to facilitate improved communication and coordination across sectors. • Identify the critical legacy data repositories not compatible with the environment and recommend how the information from these critical legacy data repositories will be transitioned into the environment. • Establish the minimum standards for access to the environment, including appropriate system identification and authentication mechanisms. • Establish the minimum standards for accountability and auditing within the environment. • Define and document the requirements for analytic tools used by information

		<p>consumers for information exploitation with proposed performance metrics.</p> <ul style="list-style-type: none"> • Define the first increment of the data standards for the environment. • Establish baseline metrics for the environment. • Develop a plan expediting the deployment of Cross Domain Solutions for use within the environment. • Establish the metadata standards to be used within the environment. • Establish the requirements for a policy-based access control decision engine. This is an essential capability needed to implement the vision of the environment where real time information access decisions will be made. This capability will provide information consumers with all of the information they are entitled to, but restrict their access from information they are prohibited from accessing. The engine will also contain a “data owner” override, as well as role-based access to information. This service will provide access decisions based on factors such as users role, real-time cyber situational awareness, authenticated identity, clearance level, sensitivity of the information, and many other factors.
--	--	---

2. Phase 2 – Initial Operational Capability (18 Months)

By the end of 18 months, the environment should achieve an initial operational capability (IOC). At this point, all major state, local, tribal, and federal networks will be included in the environment. Most information appropriate to a sector of the environment will be accessible to the entire environment. Search capabilities across all appropriate information will be available. E-mail will be available across the community and a chat capability will function within security domains. Collectively, these deliverables will provide a substantially greater capability for users to access the core functions. At a minimum this means:

Phase 2 – Initial Operational Capability (18 Months)		
Task #	Task Name	Task Description
1	<i>Connect All Major Federal Networks</i>	All major networks containing terrorism-related information at federal levels will be included in the environment.
2	<i>Connect All Major State, Local, Tribal Networks</i>	All major networks containing terrorism-related information at the state, local, and tribal levels will have the option to be included in the environment.
3	<i>Make Highest Priority Information Accessible</i>	The highest priority information appropriate to each network will be current and accessible to users on each network.
4	<i>Implement Single Sign Access</i>	Users will be able to access the environment from their local networks with a single logon.
5	<i>Deploy Common Search Tools</i>	Common search tools will be accessible across the environment for sectors to deploy.
6	<i>Initiate E-mail Exchange</i>	Users will be able to easily exchange e-mail with each other anywhere in the environment.
7	<i>Implement Chat Capability</i>	Users will, at a minimum, be able to chat with others within their security domains.
8	<i>Establish Federated I&A</i>	A federated identification and authentication (I & A) for the SBU security level throughout the federal government will be established.
9	<i>Complete Data Standardization</i>	Data standards will be completed and delivered by calendar year end 2005.
10	<i>Ensure Interoperability Between Networks</i>	Information Technology system standards and communication standards used to ensure interoperability between the networks which will be interconnected to establish the environment will be finalized.
11	<i>Publish Public Key Standards</i>	Published standards for secure data exchange supporting data exploitation applications that integrate commercial web services with public key certificates will be available.

12	<i>Further Expand Interconnected Networks</i>	The total number of interconnected networks to include those at all security levels, including Second Party and other foreign partner networks, and other major networks not included in the first six months will be expanded.
13	<i>Establish Email Capability</i>	An initial electronic capability to exchange email with attachments between and among all organizations comprising the environment will be established. This includes exchanging email between networks at the same security level as well as at different security levels.
14	<i>Complete Pilot Programs</i>	<p>Pilot programs will be completed to:</p> <ul style="list-style-type: none"> • Accelerate the current tear-line pilot program being conducted at the Terrorism Threat Integration Center, and upon its conclusion, transition the pilot program into full production solutions within the federal government. • Provide an operational federated query tool that operates across networks at different security levels with a limited number of users. • Implement a “Write to Release” process to be operational with an initial set of users. • Automate push and/or pull of information. This will allow information consumers to receive information by multiple methods. Automated push is similar to delivering information by email lists. Auto pull is allowing the consumer to have a tailored space (like a portal) that receives information to which they subscribed. • Automate content management and distributions (publish and subscribe). This program will allow consumers to subscribe to a topical area and have all information delivered to them that is related to the topical area. The

		<p>information will be delivered at the appropriate security level. The benefit is to get the right information to the right people at the right time at the right security level to accomplish the mission.</p> <ul style="list-style-type: none"> • Demonstrate a distributed trust model for authentication at the SBU security level.
--	--	--

3. Phase 3 – Enhanced Operational Capability

Between 18 and 36 months, the environment will deliver a robust capability for the majority of the requirements as defined by functional and system requirement documents. Users will be able to log on from their native workspace (e.g., desktop, laptop, PDA etc.) to the environment. Users will have a single workstation, which connects to the environment as opposed to today, where each network requires its own, distinct workstations. They will be able to easily and reliably access timely information relevant to their missions. They will be able to find other users elsewhere in the environment and establish ad hoc communities of interest in near real-time, without pre-coordination. Tools will be available not only to find information, but also to help users discover information useful to them. Information will be pushed to them quickly and reliably. Some advanced tools to help users link or integrate information from multiple products or sources will be operational. The deployment of a fully functional single sign on capability will be available so users will only have to log on once. Capabilities available to users based on the deployment schedule of each sector will also include:

Phase 3 – Enhanced Operational Capability		
Task #	Task Name	Task Description
1	<i>Implement Robust Data Capabilities</i>	At Operational Capability the environment will have robust information discovery, knowledge extraction, collaboration, and information delivery capabilities across security domains.
2	<i>Deploy Subscription Capabilities</i>	Subscription capabilities now include advanced capabilities where systems provided automated assistance to users in determining the relevant information topics for the problems they are working on. Sharable information will be able to be extracted from

		restricted sources and delivered to authorized users via subscription services.
3	<i>Make Collaboration Tools Available</i>	Collaboration tools will be available across security domains so users at one level can chat with users at another, much the same way they can talk over open phone lines today. Automated facilities will monitor the information exchanges of cross domain collaboration sessions to prevent unauthorized transfer of information. Implement an encrypted email capability will be available throughout the environment for those users who need it.
4	<i>Implement Simplified Single Sign On</i>	The distributed identification and authentication mechanisms will be sufficiently developed and broadly implemented so that users realize a simplified single sign on capability for the applications and data sources that comprise the mainstream of their workflows.
5	<i>Provide Access To Legacy Data</i>	Facilities will be established to provide access to legacy data by using the environment data standards either by converting legacy data sets where feasible or implementing enterprise application interface services.

4. Phase 4 - Beyond Thirty Six Months

With the rapid changes in world events associated with terrorism and advancements in technologies used to support the sharing of terrorism information, we can be certain there will be important enhancements and changes to the proposed environment needed. What those changes will be is difficult to know at this point. However, there are a few general issues that can be predicted.

Counter-terrorist personnel are quite mobile and need to be able to easily access the environment from networks managed by others, a capability that will likely not be generally available in 36 months. Currently underway are efforts to develop a semantic web search capability which will provide a way to not only match a query character string, but will be able identify the meaning of the content of information. While some preliminary semantic web capabilities will be delivered in the first 36 months, the opportunities offered by this new technology far exceed what will realistically be available in the next 3 years. If the semantic web continues to advance, it will be able to provide some very helpful capabilities.

After Phase 3 is complete, the environment will continue to be enhanced. The problem of making sense of dispersed and unstructured information is of tremendous interest to

industry. We can expect significant advancements will be made during the time the environment is being implemented.

Phase 4 – Beyond 36 Months		
Task #	Task Name	Task Description
1	<i>Participate in Research And Development</i>	<p>The longer term plan for the shared environment will include active participation in research and development (R&D) efforts dealing with web environments, search, discovery, and analysis of web-based information. Some areas requiring R&D include, but are not limited to:</p> <ul style="list-style-type: none"> ▪ Auditing capabilities ▪ Network security and defense ▪ Cross domain solutions ▪ Query and search tools ▪ Language translation
2	<i>Identify New Capabilities</i>	<p>To augment the information discovery and knowledge extraction advancements that will be made by industry, capabilities specific to the terrorism problem must be continually identified so the solutions being developed in industry can be adapted.</p>
3	<i>Implement Translingual Capabilities</i>	<p>Translingual collaboration services will be needed so language barriers will not hamper interaction among the collaborators and even foreign language information will be presented in a form all can understand.</p>

Table 5. ISC Phased Approach Overview

Interoperable Trusted Terrorism Information Sharing Environment Milestones						
		6 months	18 months	36 months	> 36 months	
Network Architecture						
	Connect Networks	X	X			
	Deploy Shared Space	X				
	Deploy Desktop Reduction	X		X		
Information Assurance						
	Deploy PKI Service	X				
	Deploy Distributed Trusted I&A	Pilot SBU	SCI	Collateral & SBU		
	Deploy Audit Capabilities	X		X	X	
	Provide Role-based Authorization	Pilot		X	X	
	Deploy Cross Domain Solution	Current	Tearline & Other	Other	X	
	Deploy Single Sign-On	Phase I Pilot		Full Deployment	Enhancements	
Location Services						
	Provide Data Directory	X		X		
	Provide User Directory	X		X		
	Provide Service Directory	X		X		
Collaboration Services						
	Provide E-mail capabilities	Exchange anywhere		Encrypt w/ attachments		
	Provide Chat capabilities	Chat w/in security level		Cross Domain Chat	Language	
	Provide Notification capabilities	Single Security Level		Cross Security		
	Deploy Groupware	Single Security Level		Cross Security	Language	
	Provide VTC capabilities	Establish Standard				
Information Services						
	Provide Discovery Search capabilities	Within Security Level		Cross Security	Language	
	Provide Retrieval capabilities	Within Security Level		Cross Security		
	Provide Subscription capabilities	Initial		Enhanced		
	Provide Push/Pull capabilities	Pilot		Full Deployment		
Data Standardization						
	Deploy Metadata Registry	Phase I	Phase II			
	Deploy Data Standards (Lexicon)	Initial	Full			
	Identify/Convert Legacy Data	Identify Repositories		Convert Data		
Fusion Center		Pilot			X	

4.4 DHS Additional Needs and Specific Actions

The ISE at OMB's direction was principally focused on taking the technical requirements out of play for Terrorism Information Sharing. For the larger and broader DHS mission additional and more specific actions come into play described by phases as follows.

4.4.1 Immediate (0-6 months)

- Develop initial information architecture for ISE (operational, systems, technical)

- Use eSurvey as baseline for information sharing today

- Identify Gaps and Overlaps between As-Is and To-Be

- Determine gateways between systems, examples of what is being planned

- HSIN and HSIN-S

- Develop and begin Outreach plan for Stakeholders

- Identify standards to be developed

4.4.2 Near Term (6-18 months)

- Develop expanded information architecture for ISE (operational, systems, technical)

- Develop standards

- Implement Active Directory

- Pilots

- Develop budget/justification methodology (Investment strategy)

 - Start-up costs

 - Development and maintenance/sustaining costs

- Timeline

4.4.3 Mid-Term (18-36 months)

- Implement architecture

- Budget and timeline

4.5 ISC Capability Maturity Model

For perspective, for goal identification and to measure progress an Information Sharing and Collaboration Capability Maturity Model is recommended as shown below.

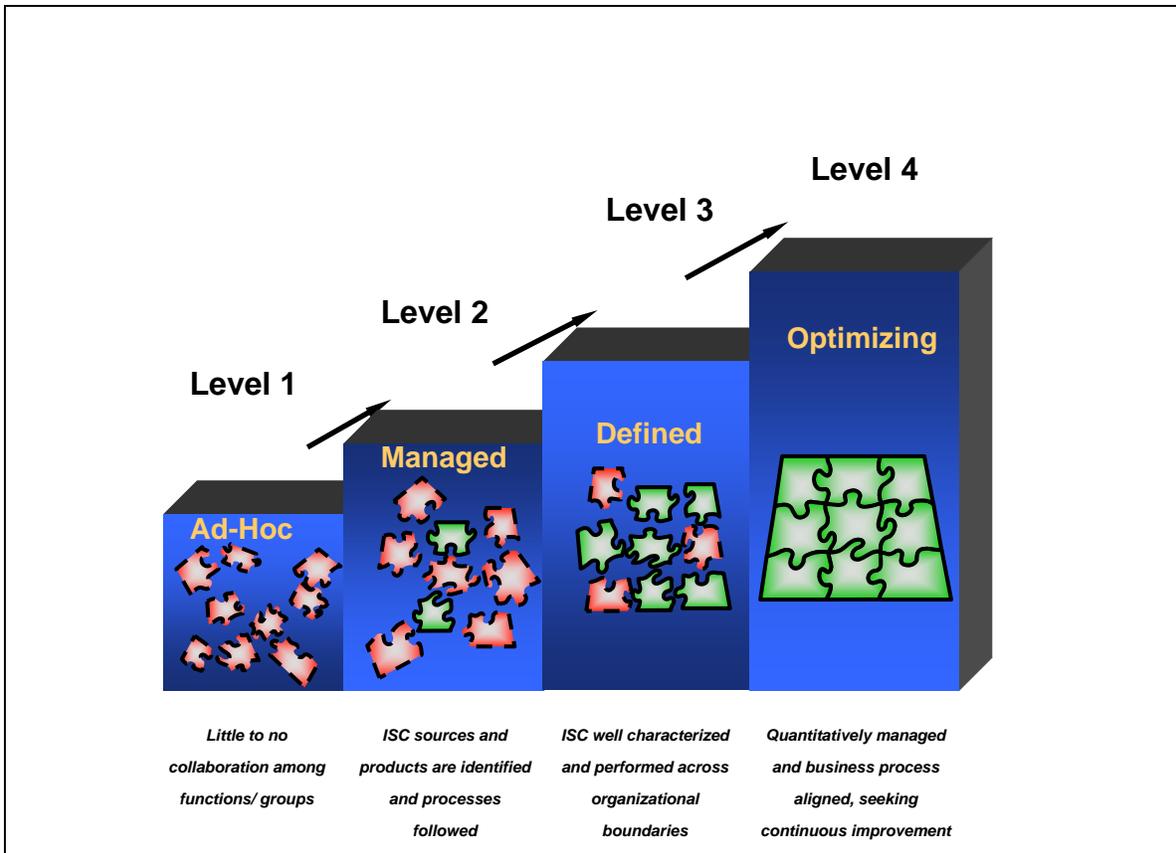


Figure 14. Information Sharing and Collaboration Capability Maturity Model

The Information Sharing and Collaboration Capability Maturity Model draws on the very successful Software Development Capability Maturity Model developed by the Software Engineering Institute at Carnegie Mellon University under contract from the Department of Defense. The objective was to bring discipline to what was then an evolutionary and non-standard process (software engineering and development). The parallels to information sharing and collaboration are striking. While better definition and application of the concepts is yet to be made, description of capability levels and process status is currently described as follows.

Level 1 – Ad-Hoc - Little to no collaboration among functions/groups

Processes ad hoc

Success dependent on individual networking and heroics

Cannot scale well to larger scale information sharing

Culturally bound

Not well founded in what is legal and what is myth

Level 2 – Managed –ISC sources and products are identified and processes followed

Information Sharing and Collaboration requirements are managed

Information sources, processes and products are known

Active directories of contacts, experts, means and communications are maintained

Processes are planned, performed, measured and controlled

Status of work products are visible to management at defined points

Information Sharing Agreements established between individual sources and boundaries

May still support legacy business process

Information Assurance requirements outlined

Level 3 – Defined – ISC well characterized and performed across organizational boundaries

Business rules agreed consistent IAW legal, privacy, civil liberty and policy provisions

ISC processes are well characterized, performed and measured

Complete metadata entered in Metadata Center of Excellence data base

Consistent with component business process

Data architecture defined

Information Assurance requirements defined

Scalable

Level 4 – Optimizing – Quantitatively managed and business process aligned, seeking continuous improvement

ISC sources, products, processes and needs well defined, performed and measured

Metadata complete and functioning, to include interface and definition necessary to support external sharing to include

High confidence Information Assurance

Responsive to innovation, policy change and changing requirements

4.6 Moving Forward – DHS Enterprise

We repeat Secretary Chertoff's direction for focus and emphasis:

Intelligence and Information Sharing for a 21st Century Department

On the most basic level, we need to take a step back and focus on the fundamental question: Why was the Department of Homeland Security created? It was not created merely to bring together different agencies under a single tent. It was created to enable these agencies to secure the homeland through joint, coordinated action. Our challenge is to realize that goal to the greatest extent possible.

Let me tell you about three areas where I plan to focus our efforts to achieve that goal. First, we need to operate under a common picture of threats we are facing. Second, we need to respond actively to these threats with the appropriate policies. Third, we need to execute our various component operations in a unified manner so that when we access the intelligence and we have decided upon the proper policies, we can carry out our mission in a way that is coordinated across the board .

Secretary Chertoff, Statement for the Record Before the United States Senate Subcommittee on Homeland Security, 20 April 2005.

The *sine qua non* that enables success in all three areas identified by Secretary Chertoff is information sharing and collaboration. A common picture of threats is impossible without sharing throughout the intelligence and information domains. Active policy and appropriate policy response can only be accomplished well with sharing across the domains of intelligence, emergency responders, law enforcement, and homeland security. Unified execution of component operations mandates sharing across all activities involved.

Since DHS must continue ongoing operations and has urgent needs for improvement, a logical way to proceed is iteratively add information sharing capability to existing systems yielding greatest potential return in effectiveness and efficiency. DHS and DOJ are cooperatively leading information exchange from native terminals between the Homeland Security Information Network, Law Enforcement Online (LEO) and the Regional Information Sharing System (RISS), allowing users using their own terminals to access information from other systems not previously available. Using working prototypes in this manner has the added advantage of providing users a visible and working vehicle for discussion of the “what can be” and in so doing results in better understanding and definition of next iteration capabilities.

This model should be implemented across the Department for high payoff operational and risk mitigation information sharing. Major synergy and productivity gains can be made by selecting enterprise workhorse systems and mapping uses and needs to determine exploitation potential. The eSurvey information sources and products provide an initial analysis capability for enterprise discussion. An early adopter operational candidate is Customs and Border Patrol (CBP) and IA information sharing to improve suspicious activity reporting, analyses and feedback. Risk mitigation candidates include

provision of biological agent information as soon as determined in an incident to emergency responders including Emergency Preparedness and Response (EP&R), local fire, medical and law enforcement as well as state and local government emergency managers.

4.7 Recommended Actions

4.7.1 Leadership affirm and support the need to manage Information Sharing and Collaboration

- a. Establish and personally (Secretary or Deputy Secretary) chair the Business Process/Information Sharing and Collaboration Council to make and oversee Business Process/ISC decisions related to principles, business application needs, ISC architecture, ISC Infrastructure and ISC investment and prioritization in support of business process needs.
 - i. In the first meeting review the DHS OMB 05-34 data on systems supporting terrorism information sharing, the eSurvey summary of information sources and products, and the System of Record Notice listing.
 - ii. In the second meeting select the DHS workhorse systems as the baseline for completing metadata and expanding information sharing.
 - iii. In each meeting following, review progress in sharing, select next systems to be added and review investment needed.
- b. Resource the Information Sharing and Collaboration effort – staffing and funding
- c. Align and formalize responsibilities and relationships
 - i. Business Process
 - ii. Information IT Infrastructure
 - iii. Information Sharing and Collaboration
 - iv. ISC Investment and Investment Review Board
 - v. Relationship and POC to PM ISE

4.7.2 Formalize and emphasize the governance, processes and information data-basing and access for

- a. Facilitating and recording Information Sharing Agreements

- b. Information Sharing and Collaboration Business Rules
- c. Business Process and Information Sharing and Collaboration
- d. Enterprise Architecture
- e. Metadata
- f. Information Assurance
- g. Metrics (general and specific to each business process and functional area)

4.7.3 Publish a DHS Mission, Organization and Functions Manual

- h. Sufficient detail to help DHS people find people and data of interest

4.7.4 DHS take active lead with DOJ, HHS, HQDA, State, Tribal, local and private sector agencies and activities in establishing needs, standards, procedures and best practices for the sharing and use of SBU and Collateral information.

4.7.5 Establish 90 day time limit for DHS components to complete System of Record Notices (SORN) for systems carrying individual identifying information to bring DHS in compliance with Federal law.

4.7.6 Establish a 90 day review and report on ongoing initiatives and programs to resolve State, Tribal and local issues to ensure cohesion and prioritization of effort in accordance with State, Tribal and local needs, e.g., June 9, 2005, CRS Report. This report states that the major state and local homeland security issues are:

- The fact that state and local governments cannot use homeland security funds to pay for personnel.
- The need for statewide interoperable communications.
- The impact of reductions in first responder funding.
- The setting of standards for first responder equipment.
- Access to classified information

5. Risk Management

5.1 Overview

Risk is inherent in any program and particularly important in large, complex programs. Effective risk management requires involvement of the entire program team and may require assistance from outside experts knowledgeable in critical risk areas. The DHS Information Sharing and Collaboration Initiative is no different, and will, because of its complexity, experience more than the traditional areas of risk (cost, schedule, performance). To ensure the success of this effort, a proactive, detailed Risk Management Plan (RMP) will be developed. This section provides the broad outlines of that RMP to be filled out with more detail in the next version of the Business Plan. The RMP should also be updated as needed to adjust the plan to address risks that may not have been foreseen or to reassess the impact or mitigation of risks already identified. The RMP will describe the methods for identifying, prioritizing and tracking risk drivers; developing risk mitigation plans; and planning for adequate resources to handle risk. It will assign specific responsibilities for the management of risk and prescribes the documenting, monitoring, and reporting processes to be followed.

5.2 Risk Management Process Procedures¹¹

The diagram below describes a Risk Management Process Model that will be applied to ISC planning. Definitions of the elements of the structure can be found in the Glossary.

¹¹ The discussion in this section was taken primarily from the Risk Management Guide for DoD Acquisition 2003 (Fifth Edition, Version 2.0), which is available at <http://www.dau.mil/pubs/gdbks/RMG%20June%2003.pdf>

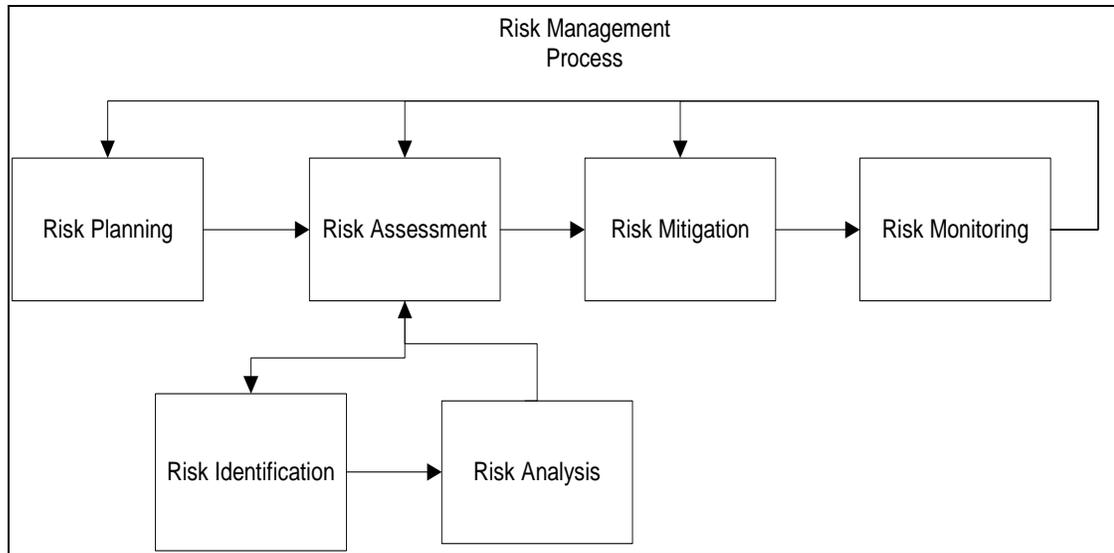


Figure 15. Risk Management Process

5.2.1 Responsibility/Organization

This section of the Plan will describe the place in the organization (whether ISCO or other) responsible for implementing the RMP as well as specific responsibilities of risk management participants.

5.2.2 Risk Management Procedures

This section will provide guidance for each of the risk management functions in the process. It is intended, when completed, to ensure a common and coordinated approach to risk management for the Information Sharing Initiative. It will include how the process will be documented and made available to all participants in the process, how risks will be tracked and specific metrics.

5.2.3 Risk Planning

This section of the RMP describes the risk planning process and provides guidance on how it will be accomplished, and the relationship between continuous risk planning and the RMP. It will also provide guidance on the updates of the RMP and the approval process to be followed for these updates.

5.3 Risk Assessment (DHS Info sharing Risk Matrix)

This section of the RMP describes risk assessment process and the procedures for examining the critical risk areas and processes to identify and document the associated risk. This stage of the Information Sharing Initiative will attempt to capture the major areas and some specifics of the risks that could impact a successful implementation. In

In addition to the risks, the team will categorize both the probability of that particular risk occurring, as well as the relative importance or priority of that risk to the overall project. The result will be a Risk Matrix, the initial version of which can be found at Table 6. Included in the matrix will be the following:

1. **Descriptions of the types of risk:** The major categories of risk on the matrix include: Organization, Study Phase Activities, Requirements Development, Contracts Vehicle, Performance, Cost, Schedule, Technical, Security, Cultural, Integration, and Other. The actual risk to be assessed will be described in a succinct statement under the appropriate category. As these risks will change as the Initiative progresses, more categories may be necessary and additional risk items will be added.
2. **Risk Ratings:** The risk listed will be evaluated using a number of different rating processes (depending on the complexity and type of risk) to result in one of these three categories. These ratings will be categorized as follows:

Risk Rating	Description	Color code
High	Major impact	Red
Moderate or Medium	Some impact	Yellow
Low	Minimum impact	Green

3. **Metrics:** The metrics to be used to evaluate the risk will be determined based on the type of risk described.

Also to be included with this section will be the following information:

- Overview and scope of the assessment process
- Sources of information used for the assessment
- Information to be reports and the formats in which it is to be reported
- Description of how risk information is to be document
- Assessment techniques and tools.

5.4 Risk Mitigation

This section will describe the procedures used to determine and evaluate various risk mitigation options and identify tools that can assist in implementing the process. It will also provide guidance on the use of the various mitigation options for specific risks. This section will also describe the residual risk that remains after all risk mitigation decisions have been implemented, how that residual risk will be monitored, and the thresholds for determining whether the residual risk must be mitigated or reduced. This section is

extremely important because these risk mitigation actions will significantly impact the success of the initiative.

5.5 Risk Monitoring

This section will describe the process and procedures to be followed to monitor the status of the various risk events identified. It will include criteria for the selection of risks to be reported on and the frequency of reporting. Guidance on the selection of metrics for this monitoring will also be addressed as well as thresholds for determining whether risks should be reevaluated and additional mitigation activity determined.

Table 6. DHS Information Sharing Risk Matrix

#	Risk	Probability (H, M, L)	Priority (H, M, L)	Consequence (H,M,L)	Risk Mitigation Activity	Resources
1	Organization					
	Stability					
	Internal Communications					
	Responsibility/Authority					
	Assignment of Qualified/empowered Program Manager					
2	Study Phase Activities					
3	Requirements Development					
4	Contracts Vehicle					
5	Performance					
	Program inadequately addresses requirements (implied or stated)					
	Program requirements change as program is executed					
	Performance of program does not meet milestones or requirement definition					
5	Cost					
	Funding not available for program execution					
	Funding insufficient for overall program execution					
	Cost for program exceeds estimates					
	Program requirements change as program is executed					
	Lack of Earned Value Methodology to track cost vs schedule vs deliverables					
6	Schedule					
	Program execution not in step with schedule					
	Program requirements change as program is executed					
	Unforeseen events cause delays					
7	Technical					
	Complexity of implementation				Use of Standards, best practices	
	Policy compliance					
	Use of unproven and uncommon technical solutions					
	Failure to address legal, regulatory, ethical concerns					
8	Cultural					
	Lack of acceptance by stakeholder communities					
9	Security					
	Failure to combat IT security vulnerabilities					
10	Integration					
	Testing & Evaluation					
	Interoperability					
11	Other					

Risk Assessment Color code
RED - HIGH: Major impact likely. Different approach may be required. Priority management attention required.
YELLOW - MODERATE: Some impact. Different approach may be required. Additional management attention may be needed
GREEN - LOW: Minimum impact. Minimum oversight needed to ensure risk remains low.

6. Summary

Information Sharing and Collaboration are essential to basic DHS mission accomplishment and even more-so to the successful integration, synergy and efficiency intended by the creation of DHS.

Active participation by key stakeholders from all Communities of Interest is necessary to the inclusion of needed information, adoption of collaboration tools and procedures, and to overcome the cultural and bureaucratic barriers.

Special emphasis and leadership is needed to insure that the information sharing environment supports access and distribution of information and collaborative tools throughout the greatly expanded domain of homeland security users. DHS is local. This is DHS' mission.

Standards are key, especially Metadata in which DHS plays a key role. Active participation in the Information Sharing Environment and support of/coordination with the PM ISE are necessary to sharing effectively throughout the key government and private sector activities. DHS plays a pivotal role.

People want to do well, but they need help, especially when culture and resources are involved as they are in ISE. Top Gun (Secretary/DEPSEC) leadership and program support is essential for meaningful Information Sharing and Collaboration change and success.

Annex A References

- Bina, Rebekah, and Nicolai, Caroline 2004 *The Legal Framework in U.S. Law for sharing Law Enforcement and Intelligence Information*, Spring 2004, available at <http://www.maxwell.syr.edu/campbell/Events/ISHS.htm>.
- Bolten, Joshua B. 2002 Memorandum for Heads of Executive Departments and Agencies, From: Joshua B. Bolten, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- Bush, George W. 2002 *[The President's Proposal for] The Department of Homeland Security*, June 2002.
- Cafano, James Jay and Heyman, David 2004 *DHS 2.0: Rethinking the Department of Homeland Security*, Heritage Foundation, December 13, 2004.
- Carter, David L. 2004 *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, School of Criminal Justice, Michigan State University. **November 23, 2004**
- Cho, H., Stefanone, M., and Gay, G. 2002 *Social information sharing in a CSCL community*. In Proceedings of the 2002 ACM CSCL Conference, pp.43-53. Lawrence Erlbaum Associates. Boulder, USA. Best Paper Award.
- Congressional Research Service (CRS) 2003 *Homeland Security Act of 2002: Critical Infrastructure Information Act*, CRS Report for Congress, February 28, 2003.
- Congressional Research Service (CRS) 2003a *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, CRS Report for Congress, February 14, 2003.
- Congressional Research Service (CRS) 2003b *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, CRS Report for Congress, Updated March 21, 2003.
- Congressional Research Service (CRS) 2003c *Critical Infrastructure Information Disclosure and Homeland Security*, CRS Report for Congress, Updated January 29, 2003.
- Congressional Research Service (CRS) 2004 *Information Sharing for Homeland Security: A Brief Overview*, CRS Report for Congress, Updated September 30, 2004.

Congressional Research Service (CRS) 2004a	<i>The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project</i> , CRS Report for Congress, August 18, 2004.
Congressional Research Service (CRS) 2005	<i>Information Sharing for Homeland Security: A Brief Overview</i> , CRS Report for Congress, Updated January 10, 2005.
Defense Acquisition University (DAU)	<i>Risk Management Guide for DoD Acquisition</i> , Fifth Edition, Version 2.0, 2003, http://www.dau.mil/pubs/gdbks/RMG%20June%2003.pdf
Department of Homeland Security (DHS) 2004	<i>Securing Our Homeland, U. S. Department of Homeland Security Strategic Plan</i> , 24 February 2004.
Department Of Homeland Security (DHS)	Interim Management Directive Number: 0450.1, <i>Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA)</i> .
Department Of Homeland Security (DHS)	Management Directive Number 11021, <i>Portable Electronic Devices in SCI Facilities</i>
Department Of Homeland Security (DHS)	Management Directive Number: 0460.1, <i>Freedom of Information Act Compliance</i> .
Department Of Homeland Security (DHS)	Management Directive Number: 0470.1, <i>Privacy Act Compliance</i>
Department Of Homeland Security (DHS)	Management Directive Number: 0550.1, <i>Records Management</i> .
Department Of Homeland Security (DHS)	Management Directive Number: 11010.1, <i>Issuance and Control of Credentials</i> .
Department Of Homeland Security (DHS)	Management Directive Number: 11041, <i>Protection of Classified National Security Information Program Management</i> .
Department Of Homeland Security (DHS)	Management Directive Number: 11043, <i>Sensitive Compartmented Information Program Management</i> .
Department Of Homeland Security (DHS)	Management Directive Number: 11045, <i>Protection of Classified National Security Information: Accountability, Control, and Storage</i> .

Department Of Homeland Security (DHS)	Management Directive Number: 11050.2, <i>Personnel Security and Suitability Program.</i>
Department Of Homeland Security (DHS)	Management Directive Number: 11051, <i>SCIF Escort Procedures.</i>
Department Of Homeland Security (DHS)	Management Directive Number: 11052, <i>Internal Security Program.</i>
Department Of Homeland Security (DHS)	Management Directive Number: 11060, <i>Operations Security Program.</i>
Department Of Homeland Security (DHS)	Management Directive Number: 4500.1, <i>DHS E-Mail Usage.</i>
Department Of Homeland Security (DHS)	Management Directive Number: 8200.1, <i>Information Quality; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies.</i>
Department Of Homeland Security (DHS) 2004	Management Directive, <i>Safeguarding Sensitive But Unclassified (For Official Use Only) Information. Management Directive Number: 11042, May 11, 2004.</i>
Department Of Homeland Security (DHS)	<i>Procedures for Handling Critical Infrastructure Information, 6 CFR Sec. 29.2 (a).</i>
Department Of Homeland Security (DHS)	<i>Records Management Handbook.</i>
Department of Homeland Security (DHS) 2004a	<i>Securing Our Homeland: Strategic Plan, 2004.</i>
Department of Justice (DOJ)	<i>Guidance Regarding The Use Of Race By Federal Law Enforcement Agencies.</i>
Department of Justice (DOJ)	<i>Resource Guide on Racial Profiling Data Collection Systems,</i>
Department of Justice (DOJ) 2001	<i>Memorandum for Heads of Department Components, From: The Attorney General, Subject: Prevention of Acts Threatening Public Safety and National Security, November 8, 2001.</i>
Department of Justice (DOJ) 2001a	<i>Memorandum to All United States Attorneys, From: The Attorney General, Subject: Cooperation with State and Local Officials in the Fight Against Terrorism, November 13, 2001.</i>

Department of Justice (DOJ) 2002	<i>Memorandum to Director, FBI, Assistant Attorney General, Criminal Division, Counsel for Intelligence Policy, United States Attorneys; From: The Attorney General (John Ashcroft), Subject: Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI, March 6, 2002.</i>
Department of Justice (DOJ) 2002a	<i>Fact Sheet, Attorney General Guidelines for Information Sharing, September 23, 2002, WWW.USDOJ.GOV</i>
Department of Justice (DOJ) 2002b	<i>Fact Sheet, Overview of Information Sharing Initiatives in the War on Terrorism, September 19, 2002, WWW.USDOJ.GOV.</i>
Department of Justice (DOJ) 2002c	<i>Memorandum for the Deputy Attorney General, et al., From: The Attorney General, Subject: Coordination of Information Relating to Terrorism, April 11, 2002.</i>
Department of Treasury (DOT) 2001	<i>Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, F.R. 66, No. 22, February 1, 2001.</i>
Director of Central Intelligence (DCI) 1998	<i>Intelligence Disclosure Policy, Director of Central Intelligence Directive DCID 6/7, June 30, 1998.</i>
Director of Central Intelligence (DCI) 1998a	<i>Security Controls on the Dissemination of Intelligence Information, Director of Central Intelligence Directive DCID 1/7, June 30, 1998.</i>
Director of Central Intelligence (DCI) 1998b	<i>Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, Director of Central Intelligence Directive DCID 6/4, July 2, 1998.</i>
Director of Central Intelligence (DCI) 2004	<i>Intelligence Community Policy on Intelligence Information Sharing, Director of Central Intelligence Directive DCID 8/1, June 6, 2004.</i>
Executive Office of the President (EOP)	<i>Homeland Security Presidential Directive HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors.</i>
Executive Office of the President (EOP) 1981	<i>Executive Order 12333, United States Intelligence Activities, 4 December 1981.</i>
Executive Office of the President (EOP) 1995	<i>Executive Order 12958, Classified National Security Information, 17 April 1995.</i>
Executive Office of the President (EOP) 1996	<i>Executive Order 13010, Critical Infrastructure Protection, 15 July 1996.</i>

Executive Office of the President (EOP) 1998	Presidential Decision Directive (PDD) /NSC-63, <i>Protecting America's Critical Infrastructures</i> , 22 May 1998.
Executive Office of the President (EOP) 2001	Executive Order 13231, <i>Critical Infrastructure Protection in the Information Age</i> , 16 October 2001.
Executive Office of the President (EOP) 2001a	Executive Order 13228, <i>Establishing the Office of Homeland Security and the Homeland Security Council</i> , , 8 October 2001.
Executive Office of the President (EOP) 2003	Executive Order 13311 , <i>Homeland Security Information Sharing</i> , 29 July 2003.
Executive Office of the President (EOP) 2003a	Executive Order 13292, <i>Further Amendment to Executive Order 12958, as Amended, Classified National Security Information</i> , 25 March 2003.
Executive Office of the President (EOP) 2003a	Homeland Security Presidential Directive/ HSPD-7, <i>Critical Infrastructure Identification, Prioritization, and Protection</i> , 17 December 2003.
Executive Office of the President (EOP) 2003b	Homeland Security Presidential Directive/ HSPD-6, <i>Integration and Use of Screening Information</i> , 16 September 2003.
Executive Office of the President (EOP) 2004	Executive Order 13356, <i>Strengthening the Sharing of Terrorism Information to Protect Americans</i> , 27 August 2004.
Executive Office of the President (EOP) 2004a	Homeland Security Presidential Directive/HSPD-11, <i>Comprehensive Terrorist-Related Screening Procedures</i> , 27 August 2004.
Frank, F., & Soller, A. 2005	Collaboration and Knowledge Sharing across the Intelligence Community. <i>The Faces of Intelligence Reform: Perspectives on Direction and Form</i> . The Council for Emerging National Security Affairs (CENSA), Summer 2005.
Freedom of Information Act (FOIA)	<i>Explanation of FOIA Exemptions</i> , http://www.dtic.mil/dpmo/general_info/exemptions.htm
Gallagher, Sean and Neugebauer, Michael	<i>Critical Infrastructure Information Sharing</i> , NEED CITATION
Government Accountability Office (GAO) 2000	<i>Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination</i> , GAO/T-AIMD-00-268, 26 July 2000.

Government Accountability Office (GAO) 2001	<i>Information Sharing: Practices that Can Benefit Critical Infrastructure Protection</i> GAO Report GAO-02-24, October 2001.
Government Accountability Office (GAO) 2001a	<i>Homeland Security: Key Elements of a Risk Management Approach</i> , GAO-02-150T, 12 October 2001
Government Accountability Office (GAO) 2001b	<i>Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts</i> , GAO-02-208T, 31 October 2001
Government Accountability Office (GAO) 2002	<i>National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy</i> , GAO-02-811T, 7 June 2002.
Government Accountability Office (GAO) 2002a	GAO letter, Subj: <i>National Preparedness: Technology and Information Sharing Challenges</i> , dtd 30 August 2002.
Government Accountability Office (GAO) 2002b	<i>Homeland Security: Information Sharing Activities Face Continued Management Challenges</i> , GAO-02-1122T, 1 October 2002.
Government Accountability Office (GAO) 2002c	GAO Letter, Subj: <i>IRS and Terrorist-Related Information Sharing</i> , dtd 21 Oct 2002
Government Accountability Office (GAO) 2003	<i>Homeland Security Efforts to Improve Information Sharing Need to Be Strengthened</i> , GAO Report to the Secretary of Homeland Security, August 2003.
Government Accountability Office (GAO) 2003a	<i>Homeland Security Information Sharing Responsibilities, Challenges, and Key Management Issues</i> , GAO Testimony Before the Subcommittee on Cybersecurity, et al., September 17, 2003.
Government Accountability Office (GAO) 2003b	Report to Congressional Requesters, <i>Information Technology Terrorist Watch Lists Should be Consolidated to Promote Better Integration and Sharing</i> , April 2003.
Government Accountability Office (GAO) 2004	<i>Critical Infrastructure Protection Improving Information Sharing with Infrastructure Sectors</i> , GAO Report to Congressional Requesters, July 2004.
Government Accountability Office (GAO) 2004a	Testimony Before the Committee on Government Reform, House of Representatives, <i>9/11 Commission Report Reorganization, Transformation, and Information Sharing</i> , August 3, 2004.
Government Accountability Office (GAO) 2004b	<i>Homeland Security: Communication Protocols and Risk Communications Principles Can Assist In Refining the Advisory System</i> , GAO-04-682, June 2004

Government Accountability Office (GAO) 2004c *9/11 Commission Report: Reorganization, Transformation, and Information Sharing*, GAO-04-1033T, 3 August 2004

Government Accountability Office (GAO) 2004d *GAO Report, Data Mining: Federal Efforts Cover Wide Range of Uses*, May 2004. <http://www.gao.gov/new.items/d04548.pdf>

Information Sharing and Collaboration Office (ISCO) 2004 *DHS ISC Blueprint (Initial Draft)* 15 December 2004.

Information Sharing and Collaboration Office (ISCO) 2005 *DHS As-Is Report (Progress Report)*, Internal Draft, 15 January 2005.

Information Sharing and Collaboration Office (ISCO) 2005a *ISCP Background and the New Information Sharing Environment*, 12 January 2005.

Information Systems Council (ISC) 2004 *Initial Plan for the Interoperable Terrorism Information Sharing Environment*, prepared by the Information Systems Council in response to EO 13356, 20 December 2004.

Information Technology Information Sharing and Analysis Center, Inc. *Inter-ISAC Information Exchange Policy and Procedures Memorandum of Understanding*, January 2002, <https://www.it-isac.org/documents/Inter-ISAC-info-exch-MOU.pdf>.

Information Technology Information Sharing and Analysis Center, Inc. *Membership Agreement*, <https://www.it-isac.org/documents/membershipagreement.pdf>

Information Technology Information Sharing and Analysis Center, Inc. *NIPC and information Technology (IT-ISAC) Information Exchange Program Memorandum of Understanding (MOU)*, <https://www.it-isac.org/documents/IT--NIPC-MOU-01-14-02.pdf>

Lave & Wenger 1991 *Situated Learning: Legitimate Peripheral Participation*. Cambridge: Cambridge University Press.

Lavery, T., Franz, T., Winquist, J., & Larson, J. 1999 *The role of information exchange in predicting group accuracy on a multiple judgment task*. Basic and Applied Social Psychology, 2(4), 281-289.

Legal Subgroup,
Information Sharing
Working Group,
Intelligence
Community 2004 *Review of Laws, Regulations, and Policies for Legal Impediments Related to Information Sharing Vol I, Part I (U/FOUO)*, December 2004,
SECRET//NOFORN//20291213.

Lowenthal, Mark M. Open Source Intelligence: New Myths, New Realities, Mark M. Lowenthal ,
President, OSS USA.

Mantovani, G. 1996 *Social context in HCI: A new framework for mental models, cooperation, and communication.* Cognitive Science, 20, 237-269.

Markle Foundation
2002 *Protecting America's Freedom in The Information Age*, A Report of The
Markle Foundation Task Force, October 2002.

Markle Foundation
2003 *Creating a Trusted Network for Homeland Security*, Second Report of the
Markle Foundation Task Force, 2003.

Memorandum 88-05
1999 Memorandum 99-05, *Instructions on Complying with President's
Memorandum of May 14, 1998, Privacy and Personal Information in Federal
Records*, January 7, 1999.

Mennecke, B. 1997 *Using group support systems to discover hidden profiles: An examination of
the influence of group size and meeting structures on information sharing
and decision quality.* International Journal of Human-Computer Studies, 47,
387-405.

Murphy, M. Maureen
2001 *Privacy Protection for Customer Financial Information*, CRS Report for
Congress, RS20185, January 5, 2001.

NASIRE *National Information Architecture, Toward National Sharing of
Governmental Information*,
<https://www.nascio.org/hotIssues/EA/Fullrept.pdf>.

National Association
of State Chief
Information Officers
(NASCIO) 2003 *Concept of Operations for Integrated Justice Information Sharing*, July 2003.

National Association
of State Chief
Information Officers
(NASCIO) 2003a *Federal Privacy Law Compendium*, NASCIO Privacy Committee, April 2003

National Association
of State Chief
Information Officers
(NASCIO) 2005 *Government Information Sharing Calls to Action, Vol. 1: Justice*, March
2005.

National Association
of State Chief
Information Officers
(NASCIO) 2005a *Government Information Sharing Calls to Action, Vol. 2: Government*,
March 2005

National Defense Industrial Association (NDIA) 2003	<i>Homeland Security Information Sharing Architecture</i> , National Defense Industrial Association Interoperability and Systems Integration Conference, April 2, 2003.
National Institute for Standards and Technology (NIST) 1998	NIST Special Publication 800-18., <i>Guide for Developing Security Plans for Information Technology Systems</i> , December 1998
National Institute for Standards and Technology (NIST) 1999	NIST Special Publication 800-21, <i>Guideline for Implementing Cryptography in the Federal Government</i> , November 1999
National Institute for Standards and Technology (NIST) 2001	NIST Special Publication 800-26, <i>Security Self-Assessment Guide for Information Technology Systems</i> , November 2001.
National Institute for Standards and Technology (NIST) 2002	NIST Special Publication 800-34, <i>Contingency Guide for Information Technology Systems</i> , June 2002.
National Institute for Standards and Technology (NIST) 2002b	NIST Special Publication 800-41, <i>An Introduction to Firewalls and Firewall Policy</i> , January 2002.
National Institute for Standards and Technology (NIST) 2002c	NIST Special Publication 800-47, <i>Security Guide for Interconnecting Information Technology Systems</i> , August 2002.
National Institute for Standards and Technology (NIST) 2003	NIST Special Publication 800-59, <i>Guideline for Identifying an Information System as a National Security System</i> , August 2003
National Institute for Standards and Technology (NIST), 2002a	NIST Special Publication 800-40, <i>Procedures for Handling Security Patches</i> , August 2002.
Office of Homeland Security (OHS) 2002	<i>National Strategy for Homeland Security</i> , 16 July 2002.
Office of Justice Programs (OJP) 2004	<i>The National Criminal Intelligence Sharing Plan</i> , U.S. Department of Justice, Revised April 2004.

Office of Management and Budget (OMB)	<i>Appendix I to OMB Circular No. A-130, Federal Agency Responsibilities for Maintaining Records About Individuals</i>
Office of Management and Budget (OMB)	<i>Appendix II to OMB Circular No. A-130, Implementation of the Government Paperwork Elimination Act</i>
Ridge, Tom 2004	DHS Memorandum to (Distribution List), From: Tom Ridge, <i>Information Sharing and Collaboration</i> , May 11, 2004.
Russell, Rich 2004	<i>Information Sharing and Collaboration, Brief for the House Appropriations Committee</i> , 24 June, 2004.
Science Applications International Corporation (SAIC) 2004	<i>DHS Business Model and Target Data Architecture Report</i> , prepared for DHS Office of the Chief Information Officer, 29 October 2004.
Science Applications International Corporation (SAIC) 2004a	<i>HLS EA AS-IS Characterization Report</i> , Version 2.0, prepared for DHS Office of the Chief Information Officer, October 12, 2004
Soller, A. 2004	Understanding knowledge sharing breakdowns: A meeting of the quantitative and qualitative minds. <i>Journal of Computer Assisted Learning</i> , 20, 212-223.
Thompson, Larry D. 2001	DOJ Memorandum to Criminal Division, Office of Intelligence Policy and Review, and FBI, From: Larry D. Thompson, <i>Intelligence Sharing</i> , August 6, 2001.
USC	<i>Criminal Intelligence Systems Operating Policies</i> , (28 C.F.R. Sec. 23.20)
USC	<i>Drivers Privacy Protection Act.</i>
USC	<i>E-Government Act of 2002</i> , H.R. 2458
USC	<i>Electronic Communications Privacy Act of 1974</i>
USC	<i>Fair Credit Reporting Act.</i>
USC	<i>Family Educational Right to Privacy Act.</i>
USC	<i>FERPA Regulations.</i>
USC	<i>Foreign Intelligence Surveillance Act</i> , (FISA), 50 U.S.C. Section 1801et seq., 1978.
USC	<i>Freedom of Information Act;</i>
USC	<i>Gramm-Leach-Bliley Act.</i>

USC	<i>HIPAA Regulations.</i>
USC	<i>Homeland Security Act of 2002, Title II—Information Analysis and Infrastructure Protection, November 19, 2002, H.R. 5005</i>
USC	<i>Homeland Security Act of 2002, Title VIII—Coordination with Non-Federal Entities; Inspector General; United States Secret Service; Coast Guard; General Provisions, H.R. 5005, November 19, 2002. 6 USC Sec. 482 (2004)</i>
USC	<i>Homeland Security Information Sharing Act.</i>
USC	<i>Intelligence Authorization Act for 2003, P.L. 107-306, Section 701-702 November 27, 2002.</i>
USC	<i>Intelligence Authorization Act of 1997. 50 U.S.C. 403-5(a) 1997</i>
USC	<i>Intelligence Reform and Terrorism Act of 2004, S. 2845, December 17, 2004.</i>
USC	<i>National Security Act of 1947. 50 U.S.C. Section 401 et seq., 1947</i>
USC	<i>Omnibus Crime Control and Safe Streets Act, 42 USC 3796h 2004</i>
USC	<i>Paperwork Reduction Act of 1995, PL 104-13, May 22, 1995.</i>
USC	<i>Privacy Act of 1974. 5 USC 552a(b)(7), 1974</i>
USC	<i>Records Disposal Act</i>
USC	<i>Records Management by the Archivist of the United States.</i>
USC	<i>USA PATRIOT Act of 2001, Sec. 203, PL 107-56, H.R. 3162, October 26, 2001.</i>
White, James R. 2002	GAO Memorandum to Max Baucus and Charles E. Grassley, From: James R. White, <i>IRS and Terrorist-Related Information Sharing</i> , October 21, 2002.
Yim, Randall 2002	GAO Memorandum to Tom Davis, From: Randall Yim, “National Preparedness: Technology and Information Sharing Challenges,” August 30, 2002

Annex B Acronyms

Acronym	Definition
ADNet	Anti-Drug Network
ADNETLEADS	Anti-Drug Network NETLEADS®
ANACI	Access National Agency Check and Inquiry
BFM	Business and Financial Management
BI	Background Investigation
BICE	Bureau of Immigration and Customs Enforcement
BTS	Border and Transportation Security
CADNet	Chemical Agent Detector Network
CAIS	Criminal Alien Investigation System
CAPPS	Computer Assisted Passenger Pre-Screening System
CBP	Customs and Border Protection
CDC	Center for Disease Control and Prevention
CDS	Cross Domain Solution
ICEPIC	Immigration & Customs Enforcement Pattern Analysis & Information Collection Tool
CFO	Chief Financial Officer
CII	Critical Infrastructure Information
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISA	Criminal Information Sharing Alliance
CISANet	Criminal Information Sharing Alliance Network
CJIS APB	Criminal Justice Information Services Advisory Board

Class-net	Department of State Classified Network
COE	Center of Excellence
COEA	Cost and Operational Effectiveness Analysis
COI	Community of Interest
COOP	Continuity of Operations Plan
COP	Common Operating Picture
CPM	Contractor Program Manager
CRS	Congressional Research Service
CSA	Cognizant Security Authority
CSSO	Contractor Special Security Officer
CWIN	Critical information Infrastructure Warning Network
DAA	Designated Acquisition Authority
DACS	Deportable Alien Control System
DARTT	Data Analysis for Trade Transparency System
DAU	Defense Acquisition University
DCI	Director, Central Intelligence
DDO	Departmental Disclosure Officer
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOB	Date of Birth
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DSA	Digital Signature Algorithm
EA	Enterprise Architecture
EABM	Enforcement Apprehension Booking Module

ECPA	Electronic Communications Privacy Act of 1986
EEO	Equal Employment Opportunity
EID	Enforcement Integrated Database
E-MAIL	Electronic Mail
ENFORCE	Enforcement Case Tracking System
EO	Executive Order
EOC	Emergency Operations Centers
EP&R	Emergency Preparedness and Response
EREM	Enforcement Removal Module
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FEAPMO	Federal Enterprise Architecture Management Office
FinCEN	Financial Crimes Enforcement Network
FISA	Foreign Intelligence Surveillance Act of 1978
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSO	Facility Security Officer
FTTTF	Foreign Terrorist Tracking Task Force
GAO	U.S. Congress Government Accountability Office
GEMS	General Counsel Management Systems
GIS	Geographical Information System
HAS	Homeland Security Advisors
HEAF	Homeland Enterprise Architecture Framework
HIPAA	Health Insurance Portability and Accountability Act of 1999
HQ	Headquarters
HS	Homeland Security
HSA	Homeland Security Act

HSDN	Homeland Secure Data Network
HSDN	Homeland Security Data Network
HSIN	Homeland Security Information Network
HSIPB	Homeland Security Information Policy Board
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive
HTML	Hyper Text Markup Language
HUMINT	Human-Source Intelligence
I&A	Identification and Authentication
I2F	Information and Intelligence Fusion
IA	Information Assurance; Information Analysis
IAIP	Information Analysis and Infrastructure Protection Directorate
IC	Intelligence Community
iCAV	Infrastructure Critical Asset Viewer
ICC	Information Coordination Center
ICD	Infrastructure Coordination Division
ICE	Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
IDS	Intrusion Detection System
IMINT	Imagery Intelligence
INS	Immigration and Naturalization Service
INTEL	Intelligence
IOC	Initial Operating Capability
IP	Infrastructure Protection
IPSO	Information Processing Services Organization
IR	Infrared
IRTPA	Intelligence Reform and Terrorism Prevention Act

IS	Information System
IS&C	Information Sharing and Collaboration
IS&CP	Information Sharing and Collaboration Program
ISA	Interconnection Security Agreement
ISAC	Information Sharing and Analysis Centers
ISC	Information Sharing Council
ISCE	Information Sharing and Collaboration Environment
ISCO	Information Sharing and Collaboration Office
ISCP	Information Sharing and Collaboration Program
ISE	Information Sharing Environment
ISIS	Integrated Surveillance Info System
ISM	Information Security Markings
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITO	Infrastructure Transformation Office
IWG	
JICC	Joint Intelligence Coordinating Council
JRIES	Joint Regional Information Exchange System
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
KDDM	Knowledge Discovery and Data Mining
LE	Law Enforcement
LEA	Law Enforcement Agency
LEISP	Law Enforcement Information Sharing Program
LEO	Law Enforcement On-line
LES	Law Enforcement Sensitive

LESC	Law Enforcement Support Center
LYNX	Worksite Enforcement Activity Reporting System
MASINT	Measurement and Signature Intelligence
MBI	Minimum Background Investigation
MD	Management Directive
MIL	Military
MLS	Multi-Level Security
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSL	Multiple Security Levels
NAC	National Agency Check
NACI	National Agency Check and Inquiries (NACI)
NAIS	Nationwide Automatic Identification System
NASCIO	National Association of State Chief Information Officers
NCIC	National Cartographic Information Center; National Crime Information Center
NCS	National Communications Service
NCSD	National Cyber Security Division
NCTC	National Counter Terrorism Center
NDEx	National Data Exchange
NICC	National Infrastructure Coordination Center
NIPP	National Infrastructure Protection Plans
NIPRNet	Non-Secure Internet Protocol Router Network
NIPS	Numerically Integrated Processing System
NLETS	National Law Enforcement Telecommunications System
NORTHCOM	Department of Defense Northern Command
NRC	Nuclear Regulatory Commission
NSA	National Security Agency

OCIO	Office of the Chief Information Officer
OE	Organizational Element
OGC	Office of General Counsel
OIM	Office of Infrastructure Management
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management and Budget
OSINT	Open Source Intelligence
OSIS	Open Source Information System
PCII	Protected Critical Infrastructure Information
PDA	Personal Digital Assistant
PED	Portable Electronic Device
PEO	Program Executive Office
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
PSD	Protective Security Division
R&D	Research and Development
RDSTF	Regional Domestic Security Task Force
RISS	Regional Information Sharing System
RM	Resource Metadata
RMP	Risk Management Plan
S&L	State and Local
S&T	Science and Technology Directorate
S/L/T	State/ local/tribal
SAFE	Security Architecture Framework Extension

SAIC	Science Applications International Corporation
SATURN	Statewide Anti-Terrorism Unified Response Network
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDS	Surveillance Detection System
SEVP	Student and Exchange Visitor Program Office
SEVIS	Student and Exchange Visitor Information System
SII	Security/Suitability Investigations Index
SIIR	Standing Intelligence/Information Requirement
SIPRNet	Secure Internet Protocol Router Network
SIPRNETLEADS	Secret NETLEADS®
SLA	Service Level Agreements
SMART	State Messaging and Archival Retrieval Toolset
SOIC	Senior Official of the Intelligence Community
SOW	Statement of Work
SSBI	Single Scope Background Investigation
SSI	Sensitive Security Information
SSO	Special Security Officer
SSP	Systems Security Plan
SSR	Special Security Representative
STAR	Strategic Threat Action Report
TAIS	Telecommunications and Automated Information Systems
TAVISS	Targeted Violence Information Sharing System
TLS	Telecommunications Linking System
TSC	Terrorist Screening Center
TSIS	TSA/Transportation Security Intelligence Service

TTIC	Terrorism Treat Integration Center
US-CERT	Computer Emergency Response Team
USCS	U.S. Customs Service
USSS	US Secret Service
VPN	Virtual Private Network
VTC	Video Teleconference
WBS	Work Break Down Structure
XML	Extensible Markup Language

Annex C Glossary

<u>Term</u>	<u>Definition</u>
Access	means the ability or opportunity to gain knowledge of classified information.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(a)</u> : “A determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Access National Agency Check and Inquiry (ANACI)	Consists of a National Agency Check (NAC), employment checks, education checks, residence checks, reference checks, and law enforcement agency checks.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program</u>
Accreditation	technical, and personnel security standards.” <u>Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management.</u>
Actionable Information	Information that can be immediately used to help an operator carry out a physical action such as intercepting a hostile freighter, arresting an individual or defusing a bomb, e.g. Who, What, Where, and When.
Adjudication	Evaluation of pertinent data contained in a background investigation, and/or any other available relevant reports, to determine whether an individual is eligible for access to classified information and for Federal employment.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Affected Persons	“People who may benefit or be harmed by the disseminated information. This includes persons who are seeking to address information about themselves as well as persons who use information. <u>DHS Management Directive Number: 8200.1, Information Quality; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies.</u>

<u>Term</u>	<u>Definition</u>
Agency	<p>“Any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.” <u>Freedom of Information Act</u>.</p> <p>“[A]ny executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Federal government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only OMB and the Office of Administration.” <u>OMB Circular A-130, Management of Federal Information Resources</u>.</p>
Agent of a Foreign Power	<p>“means— “(1) any person other than a United States person, who— (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (2) any person who— (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power; (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).” <u>Foreign Intelligence Surveillance Act</u>.</p>
Aggrieved Person	<p>“means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” <u>Foreign Intelligence Surveillance Act</u>; “A person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.” <u>Electronic Communications Privacy Act</u>.</p>
Anonymization of Data	<p>“refers to techniques used to allow data to be shared or searched without disclosing identity.”</p> <p>http://www.heritage.org/Research/HomelandDefense/lm11.cfm</p>

<u>Term</u>	<u>Definition</u>
Asset	“A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.” <u>NIST Special Publication 800-26</u> ; “Information resources that support an organization’s mission.” <u>NIST Special Publication 800-12</u> .
Assets	includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel). <u>The Homeland Security Act.</u> ” 6 U.S.C. section 101(3).
Audiovisual, cartographic and architectural records	designated as permanent will be scheduled for transfer to National Archives as soon as they become inactive or whenever DHS cannot provide the proper care and handling of the materials to guarantee their preservation. Guidelines on special handling, storage and preservation problems can be found in 36 C.F.R. Part 1232.” <u>DHS Records Management Handbook</u> .
Audit Trail	“[A]record showing who has accessed an IT system and what operations the user has performed during a given period.” <u>NIST Special Publication 800-47</u> .
Authentication	Security measures designed to establish the validity of a transmission, message, originator, device (or network node), or a means of verifying an individual’s authorization to receive specific categories of information.
Authentication	“The broadest definition of authentication within computing systems encompasses identity verification, message origin authentication, and message content authentication.” <u>NIST Special Publication 800-21</u> ; “The process of verifying the authorization of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.” <u>NIST Special Publication 800-47</u> .
Authority to Process Information	“Occurs when management authorizes a system based on an assessment of management, operational and technical controls. By authorizing processing in a system the management official accepts the risk associated with it.” <u>NIST Special Publication 800-18</u> .
Authorization	The rights granted to a user to access, read, modify, insert, or delete certain data, or to execute certain programs.
Authorized	“when used with respect to access to classified information, means having authority, right or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.” <u>National Security Act</u> .

<u>Term</u>	<u>Definition</u>
Authorized Person	A person who has a need-to-know for access to classified information in the performance of official duties and who has been granted a personnel clearance or authorized access at the required level. The responsibility for determining whether a prospective recipient is an authorized person rests with the person who has possession, knowledge, or control of the classified information involved, and not with the prospective recipient.” <u>DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage.</u>
Automated information system	means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(c).</u>
Automatic declassification	means the declassification of information based solely upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under this order.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(d)</u>
Awareness, Training and Education	“Includes (1) awareness programs set the stage for training by changing organizational attitudes toward realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in automated information security.” <u>NIST Special Publication 800-18.</u>
Background Investigation (BI)	Consists of a National Agency Check (NAC), personal interviews with the individual and other sources, credit checks, law enforcement agency checks, residences checks, and employment checks.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Biometric Identifier	“means a technology that enables the automated identification, or verification of the identity, of an individual based on biometric information.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>
Biometric Identifier Information	“means the distinct physical or behavioral characteristics of an individual that are used for unique identification, or verification of the identity, of an individual.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>
Bluetooth Technology	A specification for low-cost, wireless communication and networking between PCs, mobile phones, PDAs, and other portable devices.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.</u>
Category	The classification assigned to a requester for fee purposes determined by the projected use of the records. The categories are: (a) commercial; (b) educational; (c) non-commercial scientific institutions; (d) representative of the news media; and (e) all other requesters.” <u>DHS Management Directive Number: 0460.1, Freedom of Information Act Compliance.</u>

<u>Term</u>	<u>Definition</u>
Certification and Accreditation	A term that is “synonymous with the term authorize processing. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements.” <u>NIST Special Publication 800-18</u> ; “Certification involves the testing and evaluation of the technical and non-technical security features of an IT system to determine its compliance with a set of specified security requirements. Accreditation is a process whereby a Designated Approval Authority (DAA) or other authorizing management official authorizes an IT system to operate for a specific purpose using a defined set of safeguards at an acceptable level of risk.” <u>NIST Special Publication 800-47</u> .
Chief Information Officer	“Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.” <u>Clinger-Cohen</u> .
Civil Liberties	Fundamental individual rights, such as freedom of speech, privacy and religion, protected by law against unwarranted governmental or other interference.
Classification	means the act or process by which information is determined to be classified information.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(f); DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage</u> .
Classification guidance	means any instruction or source that prescribes the classification of specific information.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(f)</u> .
Classification guide	means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(g)</u> .
Classified Information	“Classified information or classified national security information means information that has been determined pursuant to E. O. 12958 as amended by E.O. 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.” <u>NIST Special Publication 800-59</u> .

<u>Term</u>	<u>Definition</u>
Classified National Security Information (Classified Information)	<p>“means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(h)</u>; Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.” <u>DHS Management Directive Number: 11041, Protection of Classified National Security Information Program Management; DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage</u>; “[I]nformation or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.” <u>National Security Act</u>; “[A]ny information that has been determined pursuant to Executive Order No. 12356 of April 2, 1982, or successor orders, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure and that is so designated.” <u>National Security Act, 50 U.S.C. 438.</u></p>
Coalition Partners	<p>Countries that compose a temporary alliance to prosecute an adversary.</p>
Cognizant Security Authority (CSA)	<p>is the individual designated by a Senior Official of the Intelligence Community (SOIC) to serve as the responsible official for all aspects of security program management with respect to protection of intelligence sources and methods under SOIC responsibility. The CSA for DHS is the Chief Security Officer.” <u>Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management</u>; “The single principal designated by a SOIC to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods, under SOIC responsibility.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.</u></p>
Collaboration	<p>Two or more people actively sharing information to solve a common problem or task.</p>
Collaboration Tools	<p>Information technology applications that enable the sharing of mission-specific applications and data, such as chat and instant messaging, shared whiteboards, and audio/video teleconferencing.</p>
Collateral	<p>In general, national security information (including imagery), classified Top Secret, Secret or Confidential not in the Sensitive Compartmented Information category.</p>

<u>Term</u>	<u>Definition</u>
Collection of Information	<p>“means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either— (i) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States; or (ii) answers to questions posed to agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes; and (B) shall not include a collection of information described under section 3518 (c)(1).” <u>Paperwork Reduction Act</u>. “Section 3518 (c)(1) states that a particular subchapter in the PRA does not apply to the collection of information-- (A) during the conduct of a Federal criminal investigation or prosecution, or during the disposition of a particular criminal matter; (B) during the conduct of-- (i) a civil action to which the United States or any official or agency thereof is a party; or (ii) an administrative action or investigation involving an agency against specific individuals or entities; (C) by compulsory process pursuant to the Antitrust Civil Process Act and section 13 of the Federal Trade Commission Improvements Act of 1980; or (D) during the conduct of intelligence activities as defined in section 3.4(e) of Executive Order No. 12333, issued December 4, 1981, or successor orders, or during the conduct of cryptologic activities that are communications security activities. (2) This subchapter applies to the collection of information during the conduct of general investigations (other than information collected in an antitrust investigation to the extent provided in subparagraph (C) of paragraph (1)) undertaken with reference to a category of individuals or entities such as a class of licensees or an entire industry.” <u>Paperwork Reduction Act</u>.</p>
Communities of Interest	A collection of personnel who share knowledge about a discipline and learn from each other over an extended period of time.
Compilation	“means an aggregation of pre-existing unclassified items of information.” <u>Executive Order 13292, Classified National Security Information, Section 1.7(e)</u> .
Compromise	“The unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other critical security parameters).” <u>NIST Special Publication 800-21</u> .
Computer Trespasser	“(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and (B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.” <u>Electronic Communications Privacy Act</u> .

<u>Term</u>	<u>Definition</u>
COMSEC	The communications security systems, services, and concepts that constitute protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of any /such communications.” <u>DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage.</u>
Confidential	shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.” Executive Order 13292, Section 1.2(3); “A level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.” <u>DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage.</u>
Confidential information	Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security of
Confidential source	“means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(i).</u>
Confidentiality	A process by which “sensitive information is not disclosed to unauthorized individuals, entities or processes.” <u>NIST Special Publication 800-21</u> ; “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.” <u>44 U.S.C. Sec. 3542</u> ; “[T]he property that data or information is not made available or disclosed to unauthorized persons or processes.” <u>HIPAA Regulations.</u>
Confidentiality Protection	“Requires access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary, trade secrets, internal agency, investigations, other federal agency, national resources, national security, and high or new technology under Executive Order or Act of Congress.” <u>NIST Special Publication 800-18.</u>
Congressional Intelligence Committees	“means— (1) the Select Committee on Intelligence of the Senate; and (2) the Permanent Select Committee on Intelligence of the House of Representatives.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>

<u>Term</u>	<u>Definition</u>
Consumer Report	<p>“Any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for: (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604 [§ 1681b]. (2) Exclusions. The term "consumer report" does not include: (A) any (i) report containing information solely as to transactions or experiences between the consumer and the person making the report; (ii) communication of that information among persons related by common ownership or affiliated by corporate control; or (iii) communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons; (B) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device; (C) any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his or her decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made, and such person makes the disclosures to the consumer required under section 615 [§ 1681m]; or (D) a communication described in subsection (o).” <u>Fair Credit Reporting Act.</u></p>
Consumer Reporting Agency	<p>“Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.” <u>Fair Credit Reporting Act.</u></p>
Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis	<p>“[A] consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide: (1) Public record information. (2) Credit account information from persons who furnish that information regularly and in the ordinary course of business.” <u>Fair Credit Reporting Act.</u></p>
Contents,	<p>“when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.” <u>Foreign Intelligence Surveillance Act and the Electronic Communications Privacy Act.</u></p>

<u>Term</u>	<u>Definition</u>
Contingency Plan	“Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.” <u>NIST Special Publication 800-34.</u>
Continuity of Operations Plan (COOP)	“A predetermined set of instructions or procedures that describe how an organization’s essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.” <u>NIST Special Publication 800-34.</u>
Contractor Program Manager (CPM)	Responsible for DHS activity on behalf of a contracting company in a contractor facility.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.</u>
Contractor Records	“Records created or received and maintained for the Government by contractors. (a) Contractors performing program functions are likely to create or receive records necessary to provide adequate and proper documentation of these programs and to manage them effectively. DHS contracts shall specify the delivery to the Government of all records including data needed for the adequate and proper documentation of contractor-operated programs in accordance with requirements of the Federal Acquisition Regulation (FAR) (b) When contracts involve the creation of data for the Government's use, in addition to specifying a final product, DHS officials may need to specify the delivery of background data that may have reuse value to the Government. Before specifying the background data that contractors must deliver to the agency, program and contracting officials shall consult with DHS records and information managers and historians and, when appropriate, with other Government agencies to ensure that all agency and Government needs are met, especially when the data deliverables support a new agency mission or a new Government program. (c) Deferred ordering and delivery-of-data clauses and rights-in-data clauses shall be included in contracts whenever necessary to ensure adequate and proper documentation or because the data have reuse value to the Government. (d) When data deliverables include electronic records, DHS shall require the contractor to deliver sufficient technical documentation to permit DHS or other Government agencies to use the data. (e) All data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records and shall be managed in accordance with records management legislation as codified at 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (5 U.S.C. 552), and the Privacy Act (5 U.S.C. 552a), and shall be scheduled for disposition in accordance with 36 C.F.R. part 1228.” <u>DHS Records Management Handbook.</u>
Contractor Special Security Officer (CSSO)	administers the receipt, control, and accountability of SCI materials and the SCI security functions for contractor facilities.” <u>Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management</u>

<u>Term</u>	<u>Definition</u>
Counterintelligence	“means information gathered, and activities conducted ¹ to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or inter national terrorist activities.” <u>National Security Act and NIST Special Publication 800-59.</u>
Countermeasure	An appropriate and legally authorized action, such as training and awareness or other recommended measures that effectively negates or reduces the risk from an adversary’s ability to identify and exploit Vulnerabilities.” <u>DHS Management Directive Number: 11060, Operations Security Program.</u>
Covert Action	means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include - (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities; (2) traditional diplomatic or military activities or routine support to such activities; (3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or 4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad. (f) No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.” <u>National Security Act.</u>
Covert Agent	"means - (A) a present or retired officer or employee of an intelligence agency or a present or retired member of the Armed Forces assigned to duty with an intelligence agency - (i) whose identity as such an officer, employee, or member is classified information, and (ii) who is serving outside the United States or has within the last five years served outside the United States; or (B) a United States citizen whose intelligence relationship to the United States is classified information, and - (i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, an intelligence agency, or (ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or (C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.” <u>National Security Act.</u>
Credential	Identification showing that an individual is entitled to represent, or exercise official power as, part of a United States Government agency.” <u>DHS Management Directive Number: 11010.1, Issuance and Control of Credentials.</u>

<u>Term</u>	<u>Definition</u>
Critical Information	Specific facts about U.S. intentions, capabilities, or activities needed by adversaries to guarantee failure or unacceptable consequences detrimental to the interests of the United States Government.” <u>DHS Management Directive Number: 11060, Operations Security Program.</u>
Critical Infrastructure	has the same definition as described in section 2 of the Homeland Security Act of 2002, and means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof.” <u>DHS Procedures for Handling Critical Infrastructure Information, 6 CFR Sec. 29.2 (a).</u>
Critical Infrastructure Information	or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records or information concerning: (1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety; (2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or (3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.” <u>DHS Procedures for Handling Critical Infrastructure Information, 6 CFR Sec. 29.2 (b).</u>
Critical Infrastructure Information Program	or ‘CII Program’ means the maintenance, management, and review of these procedures and of the information provided to DHS in expectation of the protections provided by the CII Act of 2002.” <u>DHS Procedures for Handling Critical Infrastructure Information, 6 CFR Sec. 29.2 (c).</u>
Critical Sensitive	Critical Sensitive positions have the potential for exceptionally grave damage to the national security. These positions may include access up to, and including, TOP SECRET national security information or materials; or other positions related to national security, regardless of duties, that require the same degree of trust.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Cross Domain Solutions	A combination of procedures and tools that provide for the secure dissemination of information between different security domains.

<u>Term</u>	<u>Definition</u>
Cryptographic Key	“A parameter used in conjunction with a cryptographic algorithm that determines: (1) the transformation of plaintext data into ciphertext data, (2) the transformation of ciphertext data into plaintext data, (3) a digital signature computed from data, (4) the verification of a digital signature computed from data, or (5) a data authentication code (DAC) computed from data.” <u>NIST Special Publication 800-21</u> .
Cryptography	“The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof.” “Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption.” <u>NIST Special Publication 800-21</u> .
Damage to the national security	means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.” <u>Executive Order 13292, Classified National Security Information</u> , Section 6.1(j).
Data Aggregation	“With respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.” <u>HIPAA Regulations</u> .
Data Element	“A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location.” <u>NIST Special Publication 800-47</u> .
Data Exploitation	Part of a larger knowledge discovery process that enables users to analyze large amounts of data to find previously unknown patterns, associations, relationships, and anomalies. It uses computational techniques from statistics, natural language processing, machine learning, and pattern recognition to support this discovery process.
Data Integrity	“The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.” <u>NIST Special Publication 800-21</u> .

<u>Term</u>	<u>Definition</u>
Data Mining	“Although the use and sophistication of data mining have increased in both the government and the private sector, data mining remains an ambiguous term. According to some experts, data mining overlaps a wide range of analytical activities, including data profiling, data warehousing, online analytical processing, and enterprise analytical applications. ³ Some of the terms used to describe data mining or similar analytical activities include “factual data analysis” and “predictive analytics.” We surveyed technical literature and developed a definition of data mining based on the most commonly used terms found in this literature. Based on this search, we define data mining as the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.” <u>GAO Report, Data Mining: Federal Efforts Cover Wide Range of Uses</u> , May 2004. http://www.gao.gov/new.items/d04548.pdf (emphasis added).
Data Owner	The organization that has the final statutory and operational authority for specified information.
<u>Data Trail</u>	is a collection of information that reveals the places where an individual has actually been or things he has done.
Declassification	“means the authorized change in the status of information from classified information to unclassified information.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(k)</u> .
Declassification authority	“means: (1) the official who authorized the original classification, if that official is still serving in the same position; (2) the originators current successor in function; (3) a supervisory official of either; or (4) officials delegated declassification authority in writing by the agency head or the senior agency official.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(l)</u> .
Declassification guide	means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(m)</u> .
Decryption	The process of changing ciphertext into plaintext.” <u>NIST Special Publication 800-21</u> .
Defensive Activities	Activities relating to personnel, physical, document, and communications security, such as training and awareness, foreign travel/contact briefings and debriefings, foreign visitor management, threat analysis, coordination with appropriate Intelligence Community members and Law Enforcement Agencies, internal security incident/indicator reporting, security issue reviews as coordinated with proper authorities, and assistance to adjudications and security disciplines.” <u>DHS Management Directive Number: 11052, INTERNAL SECURITY -PROGRAM</u> .

<u>Term</u>	<u>Definition</u>
Departmental Disclosure Officer (DDO)	An individual reporting to the Under Secretary for Management who serves as the Department of the Homeland Security's principal point of contact and agency representative on FOIA -related matters. <u>DHS Management Directive Number: 0460.1, Freedom of Information Act Compliance</u> . See also, FOIA Officer.
Departmental E-mail Directory	“The e-mail list that contains all DHS e-mail user entries, distribution lists, and special user accounts.” <u>DHS Management Directive Number: 4500.1, DHS E-MAIL USAGE</u> .
Derivative classification	means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(n); DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage</u> .
Designated Accrediting Authority (DAA)	The official with the authority to assume formal responsibility for operating information systems at an acceptable level of risk.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities</u> .
Designated Approving Authority (DAA)	“The senior management official who has the authority to authorize processing (accredit) an automated information (major application) or (general support system) and accept the risk associated with the system.” <u>NIST Special Publication 800-18</u> .
Designated DHS Official	Senior DHS officials as designated by the Secretary, Deputy Secretary or Under Secretaries.” <u>DHS Management Directive Number: 0460.1, Freedom of Information Act Compliance</u> and “ <u>DHS Management Directive Number: 0470.1, Privacy Act Compliance</u> and <u>DHS Interim Management Directive Number: 0450.1, Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA)</u>).
DHS Headquarters (HQ) Offices	This term includes the Office of the Secretary, Office of the Deputy Secretary, Office of the Director of Shared Services, Office of Small and Disadvantaged Business, Office of General Counsel, Office for State and Local Government Coordination and Preparedness, Office of International Affairs, Office for National Capital Region Coordination, Office for Civil Rights and Civil Liberties, Privacy Office, Office of the Chief of Staff, Office of the Executive Secretariat, Office of Public Affairs, Office of Legislative Affairs, Office of the Inspector General, Office for Private Sector Liaison, Counter Narcotics Office, Homeland Security Advisory Council, and other similar offices within DHS HQ. For purposes of this directive, DHS HQ Offices do not include the DHS Directorates.” <u>DHS Management Directive Number: 11052, Internal Security Program</u> .

<u>Term</u>	<u>Definition</u>
DHS Organizational Elements	As used in this Directive, this term shall have the meaning given to the term in DHS Management Directive (MD) 0010.1, Management Directives System and DHS Announcements.” <u>DHS Management Directive Number: 11052, INTERNAL SECURITY -PROGRAM.</u> See also, Organizational Element.
DHS SCI Facility (SCIF)	Any facility that has been approved and accredited to process, store, and/or develop Sensitive Compartmented Information (SCI) for the Department of Homeland Security.” <u>DHS Management Directive Number: 11051, Department of Homeland Security SCIF Escort Procedures.</u> See also, <u>Sensitive Compartmented Information (SCI) Facility.</u>
DHS Users	“Individuals authorized to use E-mail as part of their assigned official duties. This includes DHS employees, contractor personnel, and authorized guests using DHS supplied resources.” <u>DHS Management Directive Number: 4500.1, DHS E-Mail Usage.</u>
Digital Signature	“The result of a cryptographic transformation of data which, when properly implemented, provides the services of: (1) origin authentication, (2) data integrity, and (3) signer non-repudiation. The digital signature is computed using a set of rules (e.g., the Digital Signature Algorithm (DSA)) and a set of parameters such that the identity of the signatory and integrity of the data can be verified. [. . .]. A data unit that allows a recipient of a message to verify the identity of the signatory and integrity of the message. [. . .]. A nonforgeable transformation of data that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data.” <u>NIST Special Publication 800-21).</u>
Disclose	means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.” <u>National Security Act.</u>
Disclosure	“To permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means.” FERPA Regulations; “[T]he release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.” <u>HIPAA Regulations.</u>
Disposal	“Removal of records from DHS control and authority by their physical destruction, sale as waste material, or other forms of savage or transfer; includes erasure of information captured or maintained on electronic media.” <u>DHS Records Management Handbook.</u>
Disposal Authority	“The legal authorization obtained only from the Archivist of the United States, NARA, for the disposal of records and recorded information.” <u>DHS Records Management Handbook.</u>

<u>Term</u>	<u>Definition</u>
Disposition	“An interim or final placement of records and recorded information; the actions taken with regard to records and recorded information to maintain them in a proper place following their appraisal, including the actions of a. retaining; b. transferring to a records center; c. transferring to an archival agency; and d. destruction.” <u>DHS Records Management Handbook</u> .
Dissemination	“The government initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency use or sharing of government information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act.” <u>OMB Circular A-130, Management of Federal Information Resources</u> ; “Means agency initiated or sponsored distribution of information to the public (see 5 C.F.R. 1320.3(d) (definition of "Conduct or Sponsor"). Dissemination does not include distribution intended to be limited to: government employees or agency contractors or grantees; intra- or inter-agency use or sharing of government information; and responses to requests for agency records under the Freedom of Information Act, the Privacy Act, the Federal Advisory Committee Act or other similar law. This definition also does not include distribution intended to be limited to: correspondence with individuals or persons, press releases, archival records, public filings, subpoenas or adjudicative processes.” <u>DHS Management Directive Number: 8200.1, Information Quality; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies</u> .
Document	means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(o)</u> .
Downgrading	means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(p)</u> .

<u>Term</u>	<u>Definition</u>
Education Records	<p>“Those records, files, documents, and other materials which: contain information directly related to a student; and are maintained by an educational agency or institution or by a person acting for such agency or institution. The term “education records” does not include: records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute; records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement; in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person’s capacity as an employee and are not available for use for any other purpose; or records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student’s choice.” <u>Family Educational Right to Privacy Act.</u></p>
Electronic Communication	<p>“Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce, but does not include: (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.” <u>Electronic Communications Privacy Act.</u></p>
Electronic Communications Service	<p>“Any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” <u>Electronic Communications Privacy Act.</u></p>
Electronic Communications System	<p>“Any service which provides to users thereof the ability to send or receive wire or electronic communications. <u>Electronic Communications Privacy Act.</u></p>
Electronic mail (E-mail)	<p>“Information created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, that may be transmitted with the message.” <u>DHS Management Directive Number: 4500.1, DHS E-Mail Usage.</u></p>

<u>Term</u>	<u>Definition</u>
Electronic mail (E-mail) system	“A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on computers, and word processing documents not transmitted on an e-mail system.” DHS Management Directive Number: 4500.1, DHS E- Mail Usage.
Electronic Signature	“A method of signing an electronic message that -- (A) Identifies and authenticates a particular person as the source of the electronic message; and Implementing Cryptography 123 (B) Indicates such person's approval of the information contained in the electronic message. [GPEA].” NIST Special Publication 800-21.
Electronic Storage	“(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” Electronic Communications Privacy Act.
Electronic Surveillance	means— (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511 (2)(i) of title 18 ; (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.” Foreign Intelligence Surveillance Act.

<u>Term</u>	<u>Definition</u>
Electronic, Mechanical or Other Device	“Any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than— (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal. <u>Electronic Communications Privacy Act.</u>
Emergency response provider	includes Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.” <u>The Homeland Security Act, 6 U.S.C. section 101(6).</u>
Employee	A person other than the President and Vice President, employed by, detailed, or assigned to an agency, including members of the Armed Forces; other categories of persons who act for or on behalf of an agency, as determined by the appropriate agency head.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Employment Position Sensitivity Categories	Defined by the Office of Personnel Management.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Employment Purposes	“When used in connection with a consumer report means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.” <u>Fair Credit Reporting Act.</u>
Encrypted Key (Ciphertext Key)	“A cryptographic key that has been encrypted with a key encrypting key, a PIN or a password to disguise the value of the underlying plaintext key.” <u>NIST Special Publication 800-21.</u>
Encryption	“The process of changing plaintext into ciphertext for the purpose of security or privacy.” <u>NIST Special Publication 800-21</u>); “The translation of data into a form that is unintelligible without a deciphering mechanism.” <u>NIST Special Publication 800-47.</u>
Enterprise	An entire organization including local and remote offices; a mixture of many departments and their computer systems. Enterprise wide computing encompasses the breadth and diversity of a large organization's computer needs.
Enterprise Architecture	“(i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing new technologies in response to changing mission needs; and (B) includes-- (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan.” <u>E-Government Act of 2002.</u>

<u>Term</u>	<u>Definition</u>
Facility Security Officer (FSO)	Under the authority of the Special Security Officer (see below), is responsible for the day-to-day management and implementation of DHS SCI security and administrative instructions for a designated DHS SCIF.” <u>DHS Management Directive Number: 11051, Department of Homeland Security SCIF Escort Procedures.</u>
False Match	“means the incorrect matching of one individual’s biometric identifier information to another individual’s biometric identifier information by a biometric identifier system.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>
False Non-Match	“means the rejection of a valid identity by a biometric identifier system.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>
Federal Benefit Program	“Any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.” <u>Privacy Act of 1974.</u>
Federal Information System	“An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.” <u>NIST Special Publication 800-59.</u>
Federal Personnel	“Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).” <u>Privacy Act of 1974.</u>
Federal Record	“All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.(Federal Records Act, 44 U.S.C. 3101 et seq.)” <u>DHS Management Directive Number: 4500.1, DHS E-Mail Usage.</u>
Federated Governance Authority	A management organization in which multiple organizations equally share responsibility. Decisions are generally based on consensus and implementation is normally decentralized and voluntary.
File	“When used in connection with information on any consumer, means all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.” <u>Fair Credit Reporting Act.</u>

<u>Term</u>	<u>Definition</u>
File series	cause they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(q).</u>
Financial Institution	“Any institution the business which is engaging in financial activities as described in section 1843(k) of title 12.” <u>Gramm-Leach-Bliley Act.</u> The term "financial institution" does not include: (1) any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.); (2) the Federal Agricultural Mortgage Corporation; or (3) any entity chartered and operating under the Farm Credit Act of or institutions chartered by Congress specifically to engage in transactions described in section 6802(e)(1)(C) of this title, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.” <u>Gramm-Leach-Bliley.</u>
Firewall	“A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.” <u>NIST Special Publication 800-47.</u>
FOIA Officer	FOIA Officer refers to an employee selected by an Under Secretary or a Designated DHS official to receive FOIA requests assigned to their area by the Departmental Disclosure Officer and to provide assistance in administrative matters pertaining to FOIA request processing. For other offices, FOIA Officer refers to the head of each disclosure office.” <u>DHS Management Directive Number: 0460.1, Freedom of Information Act Compliance. See also, Departmental Disclosure Officer.</u>
For Official Use Only (FOUO)	“The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, “Classified National Security Information,” as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.” This includes the following types of information: “(a) Information of the type that may be exempt from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments. Designation of information as FOUO does not infer that the information is already exempt from disclosure under FOIA. Requests under FOIA, for information designated as FOUO, will be reviewed and processed in the same manner as any other FOIA request; (b) Information exempt from disclosure per 5 U.S.C. 552a, Privacy Act; (c) Information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements; (d) Other international and domestic information protected by statute, treaty, regulation or other agreements; (e) Information that could be sold for profit; (f) Information that could result in physical risk to personnel; (g) DHS

Term

Definition

information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 12958, as amended, will be classified as appropriate; (h) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation; (i) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended; (j) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security; (k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.” DHS Management Directive, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.

Foreign government information

means: (1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; (2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or (3) information received and treated as ‘foreign government information’ under the terms of a predecessor order.” Executive Order 13292, Classified National Security Information, Section 6.1(r).

Foreign Intelligence

“means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities” National Security Act.

<u>Term</u>	<u>Definition</u>
Foreign Intelligence Information	means— (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against— (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to— (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States.” <u>Foreign Intelligence Surveillance Act</u> ; “[F]or purposes of section 2517 (6) [of the ECPA], means: (A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against: (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to— (i) the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States. <u>Electronic Communications Privacy Act</u> .
Foreign Power	“means— (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments.” <u>Foreign Intelligence Surveillance Act</u> .
Foreign Power and Agent of a Foreign Power	“have the same meanings as set forth in sections 101 (a) and (b) respectively, of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).” <u>National Security Act</u> .
Fusion Center	A physical location that provides the capability to integrate multiple sources of information into a comprehensive assessment.
General Support System	“[A]n interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.” <u>NIST Special Publication 800-18</u> .

<u>Term</u>	<u>Definition</u>
Geospatial Information	means graphical or digital data depicting natural or manmade physical features, phenomena, or boundaries of the earth and any information related thereto, including surveys, maps, charts, remote sensing data, and images.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>
Geospatial Intelligence	”This is the analysis and visual representation of security related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information.” http://www.intelligence.gov/2-business_cycle2.shtml
Geospatial Technology	“The term ‘geospatial technology’ means any technology utilized by analysts, specialists, surveyors, photogrammetrists, hydrographers, geodesists, cartographers, architects, or engineers for the collection, storage, retrieval, or dissemination of geospatial information, including -- (i) global satellite surveillance systems; (ii) global position systems; (iii) geographic information systems; (iv) mapping equipment; (v) geocoding technology; and (vi) remote sensing devices.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>
Governance	The decision processes, authorities, roles and responsibilities, and mechanisms used to define, approve, establish, change, review, and enforce policy, standards, budgets, and performance, of new and existing information systems and programs.
Government Information	“[I]nformation created, collected, processed, disseminated, or disposed of by or for the Federal Government.” <u>OMB Circular A-130, Management of Federal Information Resources.</u>
Government information	means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.” <u>DHS Management Directive Number: 8200.1, Information Quality; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies.</u>
Government-Furnished PED	PEDs that are owned or leased by the U.S. Government.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.</u>
Health Information	“Any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.” <u>HIPAA Regulations.</u>
High Risk	High-Risk positions have the potential for exceptionally serious impact on the integrity and efficiency of the service. These positions involve duties that are especially critical to the agency or program mission with a broad scope of responsibility and authority.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>

<u>Term</u>	<u>Definition</u>
Highly Sensitive Program	“means— (A) a government program designated as a Special Access Program (as that term is defined in section 4.1(h) of Executive Order 12958 or any successor Executive order); or (B) a government program that applies restrictions required for— (i) restricted data (as that term is defined in section 11 y. of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)); or (ii) other information commonly referred to as “sensitive compartmented information.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>
Homeland Security Information	“means any information possessed by a Federal, State, or local agency that— (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act.” <u>Homeland Security Information Sharing Act.</u>
Human-Source Intelligence (HUMINT)	“Human intelligence is derived from human sources. To the public, HUMINT remains synonymous with espionage and clandestine activities, yet, in reality, most HUMINT collection is performed by overt collectors such as diplomats and military attaches. HUMINT is the oldest method for collecting information, and until the technical revolution of the mid to late twentieth century, it was the primary source of intelligence. HUMINT is used mainly by the CIA , the Department of State , the DoD, and the FBI . Collection includes clandestine acquisition of photography, documents, and other material; overt collection by personnel in diplomatic and consular posts; debriefing of foreign nationals and US citizens who travel abroad; and official contacts with foreign governments. The National HUMINT Requirements Tasking Center is responsible for providing guidance for HUMINT activities, which are reflected in the National HUMINT Collection Directive. As part of this national effort, all HUMINT collection within the DoD is managed by the Defense HUMINT Service, under the direction of DIA’s Directorate for Operations.” http://www.intelligence.gov/2-business-cycle2.shtml
Identifiable Form	[A]ny representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.” <u>E-Government Act of 2002 and the Privacy Act of 1974 and OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.</u>
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.” <u>NIST Special Publication 800-47.</u>
Imagery Intelligence (IMINT)	“Imagery Intelligence includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. NGA is the manager for all imagery intelligence activities, both classified and unclassified, within the government, including requirements, collection, processing, exploitation, dissemination, archiving, and retrieval.” http://www.intelligence.gov/2-business-cycle2.shtml

<u>Term</u>	<u>Definition</u>
Immutable Audits	“Audit trails that cannot be disabled or changed. Immutable Audits ensure that (1) “everyone is subject to an audit”; (2) “produce cross-organizational audits”; (3) “measure accuracy of auditors by cross-validation;” and (4) “produce user logs that are tamper resistant.” http://www.heritage.org/Research/HomelandDefense/lm11.cfm
Indicators	Any detectable activity and/or information that, when looked at by itself or in conjunction with something else, allows an adversary to obtain critical or sensitive information.” <u>DHS Management Directive Number: 11060, Operations Security Program.</u>
Individual	A citizen of the United States or an alien lawfully admitted for permanent residence.” <u>Privacy Act of 1974 and DHS Management Directive Number: 0470.1, Privacy Act Compliance;</u> “[A] citizen of the United States or an alien lawfully admitted for permanent residence.” <u>Privacy Act and the OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002;</u> “[T]he person who is the subject of protected health information.” <u>HIPAA Regulations.</u>
Individual Accountability	“Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.” <u>NIST Special Publication 800-26.</u>
Individually Identifiable Health Information	“[I]nformation that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.” <u>HIPAA Regulations.</u>
Influential	When used in the phrase "influential scientific, financial, or statistical information", means that the agency can reasonably determine that dissemination of the information will have or does have a clear and substantial impact on important public policies or important private sector decisions. Each agency is authorized to define "influential" in ways appropriate for it given the nature and multiplicity of issues for which the agency is responsible.” <u>DHS Management Directive Number: 8200.1, Information Quality; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies.</u>
Informant	means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.” <u>National Security Act.</u>

<u>Term</u>	<u>Definition</u>
Information	<p>means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information." <u>Executive Order 13292, Classified National Security Information, Classified National Security Information, Section 6.1(s)</u>: "For purposes of the data quality law, Section 515, means any communication or representation of knowledge such as facts or data, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. This definition includes information that an agency disseminates from a web page, but does not include the provision of hyperlinks to information that others disseminate. Unlike the OMB Circular A-130 definition, this definition does not include opinions, where the agency's presentation makes it clear that what is being offered is someone's opinion rather than fact or the agency's views." <u>DHS Management Directive Number: 8200.1, Information Quality: OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies</u>; "[A]ny communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms." <u>OMB Circular A-130, Management of Federal Information Resources</u>; "Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates the information, or its successor in function, to regulate access to the information." <u>DHS Management Directive Number: 11041, Protection Of Classified National Security Information Program Management: DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage</u>.</p>
Information Dissemination	<p>"Product means any book, paper, map, machine readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, an agency disseminates to the public. This definition includes any electronic document, CD-ROM, or web page." <u>DHS Management Directive Number: 8200.1, Information Quality: OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies</u>.</p>
Information Dissemination Product	<p>"[A]ny book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public." <u>OMB Circular A-130, Management of Federal Information Resources</u>.</p>

<u>Term</u>	<u>Definition</u>
Information in Identifiable Form	“Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).” <u>OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.</u>
Information Life Cycle	“The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.” <u>OMB Circular A-130, Management of Federal Information Resources.</u>
Information Management	“The planning, budgeting, manipulating, and controlling of information throughout its life cycle.” <u>OMB Circular A-130, Management of Federal Information Resources.</u>
Information Owner	“Is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the data/information are shared with other organizations.” <u>NIST Special Publication 800-26.</u>
Information Processing Services Organization (IPSO)	“A discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis.” <u>OMB Circular A-130, Management of Federal Information Resources.</u>
Information Resources	“Information and related resources, such as personnel, equipment, funds, and information technology.” <u>NIST Special Publication 800-59</u> and the <u>Paperwork Reduction Act</u> ; “[I]ncludes both government information and information technology.” <u>OMB Circular A-130, Management of Federal Information Resources.</u>
Information Resources Management	“The process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.” <u>OMB Circular A-130, Management of Federal Information Resources</u> and the <u>Paperwork Reduction Act.</u>

<u>Term</u>	<u>Definition</u>
Information Security	As used in this directive, Information Security is the system of policies, procedures, and requirements established under the authority of Executive Order 12958, as amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.” <u>DHS Management Directive Number: 11041, Protection Of Classified National Security Information Program Management; DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage</u> ; “Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.” <u>NIST Special Publication 800-59</u> .
Information Sharing	The exchange of information between individuals working on related problems.
Information Sharing and Analysis Organization or ISAO	means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of: (1) Gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems to ensure the availability, integrity, and reliability thereof; (2) Communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems; and (3) Voluntarily disseminating critical infrastructure information to its members, Federal, State, and local governments, or any other entities that may be of assistance in carrying out the purposes specified in paragraphs (d)(1) and (d)(2) of this section.” <u>DHS Procedures for Handling Critical Infrastructure Information</u> , 6 CFR Sec. 29.2 (d).
Information Sharing Council	“means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection (g).” <u>Intelligence Reform and Terrorism Prevention Act of 2004</u> .
Information Sharing Environment (ISE)	“mean an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section.” <u>Intelligence Reform and Terrorism Prevention Act of 2004</u> .
Information System	Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog), and includes software, firmware, and hardware.

<u>Term</u>	<u>Definition</u>
Information System (IS)	Any telecommunications and/or computer-related equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog), including software, firmware, and hardware <u>DHS Management Directive Number 11021, Portable Electronic Devices in SCI Facilities</u> ; A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual <u>OMB Circular A-130, Management of Federal Information Resources</u> ; [A] discrete set of information [44 USC 3502 (8)] resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information <u>NIST Special Publication 800-59</u> ; [A]n interconnected set of information resources under the same direct management control that shares common functionality A system normally includes hardware, software, information, data, applications, communications, and people <u>HIPAA Regulations</u>
Information System Life Cycle	“[T]he phases through which an information system passes, typically characterized as initiation, development, operation, and termination.” <u>OMB Circular A-130, Management of Federal Information Resources</u> .
Information System Security Manager (ISSM)	The security official responsible for the IS security program for a specific Directorate, Office, or contractor facility.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities and DHS Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management</u> .
Information System Security Officer (ISSO)	The security official, either government or contractor, responsible for the security posture of a specific Information System.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities and DHS Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management</u> .

<u>Term</u>	<u>Definition</u>
Information Technology	<p>“[A]ny equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.” <u>OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002</u>; “[A]ny equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).” <u>OMB Circular A-130, Management of Federal Information Resources, and Clinger-Cohen.</u></p>
Integrity	<p>Refers to the security of information -- protection of the information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification.” <u>DHS Management Directive Number: 8200.1, Information Quality; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies</u>; “The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. . . . Integrity refers to assurance that a message was not modified accidentally or deliberately in transit, by replacement, insertion or deletion.” <u>NIST Special Publication 800-21</u>; “The property that data or information have not been altered or destroyed in an unauthorized manner.” <u>HIPAA Regulations.</u></p>
Integrity	<p>means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.” Executive Order 13292, Section 6.1(v).</p>
Intelink	<p>A web connecting nearly all the national security community at both the SECRET and TOP SECRET levels. As with the proposed environment, Intelink is not a single web, but instead it is a web connected seamlessly with other web environments.</p>
Intelligence	<p>Information and knowledge about a hostile individual or group obtained through observation, investigation, analysis, or understanding.</p>

<u>Term</u>	<u>Definition</u>
Intelligence	“(1) the product resulting from the [. . .] collection, processing, integration, analysis, evaluation, and [50 USC Ch 15] interpretation of available information concerning foreign countries or areas; or (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence.” <u>NIST Special Publication 800-59.</u>
Intelligence	ncludes foreign intelligence and counterintelligence. <u>National Security Act.</u>
Intelligence Activities	“The term 'intelligence activities' includes all activities that agencies within the Intelligence Community are authorized to conduct pursuant to <u>Executive Order 12333, United States Intelligence Activities.</u>
Intelligence Agency	“means any department, agency, or other entity of the United States involved in intelligence or intelligence-related activities.” <u>National Security Act</u> , Section 414(e)(1); “[I]ntelligence agency” means the Central Intelligence Agency, a foreign intelligence component of the Department of Defense, or the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation.” <u>National Security Act</u> , 50 U.S.C. Section 606(5).
Intelligence Community	“includes the following:(A) The Office of the Director of National Intelligence; (B) The Central Intelligence Agency; (C) The National Security Agency; (D) The Defense Intelligence Agency; (E) The National Geospatial-Intelligence Agency; (F) The National Reconnaissance Office; (G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; (H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy; (I) The Bureau of Intelligence and Research of the Department of State; (J) The Office of Intelligence and Analysis of the Department of the Treasury; (K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard; (L) Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.” <u>National Security Act</u> (as amended by the Intelligence Reform and Terrorism Prevention Act); “Intelligence Community” and “agency within the Intelligence Community” have the meanings set forth for those terms in section 3.4(f) of Executive Order 12333 of December 4, 1981, as amended.” <u>Executive Order 13356, Strengthening the Sharing of Terrorism Information To Protect Americans and the Homeland Security Information Sharing Act</u> ; “Intelligence Community includes United States Government agencies and organizations and activities identified in the National Security Act of 1947.” <u>Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management.</u>

<u>Term</u>	<u>Definition</u>
Intelligence Community (IC)	(1). United States Government agencies and organizations and activities identified in Section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and Section 3.4(f)(1 through 6) of Executive Order 12333. (2). Group of 15 government agencies and organizations that execute the intelligence activities of the U.S. Government. (Members are CIA, DIA, NSA, NGA, NRO, FBI, DOS [INR], DOE, DHS, Treasury, and the Intelligence components of the armed services.
Intelligence Program,	with respect to the acquisition of a major system, means a program that—(i) is carried out to acquire such major system for an element of the intelligence community; and (ii) is funded in whole out of amounts available for the National Intelligence Program.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>
Intercept	“[T]he aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” <u>Electronic Communications Privacy Act.</u>
Interconnection Security Agreement (ISA)	“In this guide, an agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.” <u>NIST Special Publication 800-47.</u>
Internal Security Training and Awareness Program	Required training for all DHS employees on topics such as foreign intelligence service elicitation and recruitment techniques, potential espionage indicators, terrorist modus operandi, espionage case studies, and internal security reporting requirements and processes. Also includes mandatory training for Internal Security Program Coordinators which familiarizes them with internal security issues and appropriate resolutions.” <u>DHS Management Directive Number: 11052, Internal Security -Program.</u>
International Terrorism	“means activities that— (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended— (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.” <u>Foreign Intelligence Surveillance Act.</u>
Interoperable	An overall environment that enables information systems and networks to function together as an automated sharing mechanism complementary with organizational policies, procedures, and regulations to facilitate the effective and expeditious dissemination of information.

<u>Term</u>	<u>Definition</u>
Intrusion Detection System (IDS)	A software application that can be implemented on host operating systems or as network devices to monitor activity that is associated with intrusions or insider misuse, or both.” <u>NIST Special Publication 800-47</u> ; “[A] software application that can be implemented on host operating systems or as network devices to monitor for signs of intruder activity and attacks.” <u>NIST Special Publication 800-41</u> .
Investigative Consumer Report	[A] consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information. However, such information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.” <u>Fair Credit Reporting Act</u> .
Investigative or Law Enforcement Officer	[A]ny officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.” <u>Electronic Communications Privacy Act</u> .
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, counters) during the entire life cycle of the keys, including the generation, storage, distribution, entry and use, deletion or destruction, and archiving. [. . .] The generation, storage, secure distribution and application of keying material in accordance with a security policy that prevents its modification, unauthorized use, or a combination thereof.” <u>NIST Special Publication 800-21</u> .
Key resources	means publicly or privately controlled resources essential to the minimal operations of the economy and government.” <u>The Homeland Security Act</u> , 6 U.S.C. section 101(9).
Knowledge Discovery and Data Mining (KDDM)	– an “umbrella term describing several activities and techniques for extracting information from data and suggesting patterns in very large databases.” http://www.cit.gu.edu.au/~s2130677/teaching/KDD.d/readings.d/AICE99.pdf
Laptop	A type of PED, usually a traditional notebook computer with a folding screen, with features similar to a standard desktop computer such as internal hard drive, standard communications and peripheral data ports, and larger in size than other PEDs <u>DHS Management Directive Number 11021, Portable Electronic Devices in SCI Facilities</u>

<u>Term</u>	<u>Definition</u>
Law Enforcement	The activities of the U. S. Government to investigate or enforce civil, criminal, or international law and, when lives are endangered, the activities of state or local law enforcement agencies. The term includes, but is not limited to, activities that are likely to result in court or administrative proceedings. The term does not include the activities of foreign governments except through the activities of the U.S. Government.
Law Enforcement Agency (LEA)	Any of a number of agencies (outside DoD) chartered and empowered to enforce laws in the following jurisdictions the U.S., a state (or political subdivision) of the U.S., a territory or possession (or political subdivision) of the U.S., or to enforce U.S. laws within the borders of a host nation.
Local Government	has the same meaning as established in section 2 of the Homeland Security Act of 2002, and means: (1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; (2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (3) A rural community, unincorporated town or village, or other public entity.” <u>DHS Procedures for Handling Critical Infrastructure Information</u> , 6 CFR Sec. 29.2 (e).
Maintain	Includes maintain, collect, use or disseminate.” <u>Privacy Act of 1974</u> .
Major Application	[A]n application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.” <u>NIST Special Publication 800-18</u> ;
Major Information System	embraces “large” and “sensitive” information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency’s programs, finances, property or other resources.” <u>OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002</u> .
Major System	has the meaning given such term in section 4(9) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 403(9)).” <u>Intelligence Reform and Terrorism Prevention Act</u> .

<u>Term</u>	<u>Definition</u>
Mandatory declassification review	“means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.” <u>Executive Order 13292, Classified National Security Information, Classified National Security Information, Section 6.1(w).</u>
Matching Program	Any computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or recouping payments or delinquent debts under such Federal benefit programs, or two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records. The term does not include: (1) matches performed to produce aggregate statistical data without any personal identifiers; (2) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals; (3) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons; (4) matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act; (5) matches using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or conducted by an agency using only records from systems of records maintained by that agency if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; (6) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel; (7) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986; or (8) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. § 402(x)(3), § 1382(e)(1).” <u>The Privacy Act of 1974.</u>

<u>Term</u>	<u>Definition</u>
Material Weakness or significant weakness	A term “used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. ‘Material weakness’ is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.” <u>NIST Special Publication 800-26.</u>
Measurement and Signature Intelligence (MASINT)	“Measurement and Signature Intelligence is technically derived intelligence data other than imagery and SIGINT. The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. Examples of this might be the distinctive radar signatures of specific aircraft systems or the chemical composition of air and water samples. The Central MASINT Organization, a component of <u>DIA</u> , is the focus for all national and DoD MASINT matters.” http://www.intelligence.gov/2-business_cycle2.shtml .
Medical Information	[I]nformation or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics, or other medical or medically related facilities.” <u>Fair Credit Reporting Act.</u>
Memorandum of Agreement (MOA)	A document describing in detail the specific responsibilities of, and actions to be taken by, each of the parties so that their
Memorandum of Understanding (MOU)	A document that describes very broad concepts of mutual understanding, goals and plans shared by goals may be accomplished. A MOA may also indicate the goals of the parties, to help explain their actions and responsibilities. DHS <u>Interim Management Directive Number: 0450.1, Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA),</u> the parties. DHS <u>Interim Management Directive Number: 0450.1, Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA).</u>
Memorandum of Understanding/Agreement (MOU/A)	“A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide [NIST SP 800-47], an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.” <u>NIST Special Publication 800-47.</u>
Metadata	Data, usually structured, describing a self-contained set of information such as a document, photograph or database. Metadata can be used to describe general characteristics of the set of information such as the title, author and date of publication, and it can describe aspects of the content such as individuals referenced in a document.
Microform records	“Microform records must meet the filming, storage and use standards in 36 C.F.R. part 1230.” <u>DHS Records Management Handbook.</u>

<u>Term</u>	<u>Definition</u>
Minimization Procedures,	with respect to electronic surveillance, means— (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand foreign intelligence information or assess its importance; (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802 (a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.” Foreign Intelligence Surveillance Act.
Minimum Background Investigation (MBI)	Consists of a National Agency Check (NAC), personal interview with the individual, reference checks, credit checks, law enforcement agency checks, residence checks, and employment checks. Other than the personal interview, there are no source interviews conducted during this investigation.” DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.
Mission Creep (aka Task Accretion and Mission Leap)	Generally involves the collection of personal information for a particular purpose and subsequently discovering additional, more invasive secondary uses to which the information can be put.
Mission Critical System	[A]ny telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that: (A) is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);(B) is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy; or (C) processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.” Paperwork Reduction Act.
Mission Essential PEDs	PEDs that the DHS Program Manager approves as being required for a DHS employee or contractor.” DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.

<u>Term</u>	<u>Definition</u>
Misuse of E-mail	Any unauthorized, illegal, improper, or inappropriate use of DHS E-mail systems, or any violations of the policies listed herein.” <u>DHS Management Directive Number: 4500.1, DHS E-Mail Usage.</u>
Moderate Risk	Moderate Risk positions have the potential for moderate to serious impact on the integrity and efficiency of the service. These positions involve duties that considerably important to the agency or program mission with significant program responsibility or delivery of service.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Motor Vehicle Record	“[A]ny record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.” <u>Drivers Privacy Protection Act.</u>
Multi-Function PED	A single device that has the capability to perform multiple functions such as voice and video/photo recording, Infra-red (IR), and video/photo or text storage and wireless transmissions.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.</u>
Multi-Level Security (MLS)	The concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.
Multiple Security Levels (MSL)	The ability to disseminate intelligence information and products, and transfer data, information and intelligence between different and separate classification environments (e.g., TOP SECRET SCI, SECRET, and CONFIDENTIAL). While the different security environments do not coexist within one information space, the information within each is aided in its ability to move from one to another.
Multiple sources	means two or more source documents, classification guides, or a combination of both.” <u>Executive Order 13292, Classified National Security Information, Classified National Security Information, Section 6.1(x).</u>
National Agency Check (NAC)	Consists of records searches in the Office of Personnel Management (OPM) Security/Suitability Investigations Index (SII); FBI Identification Division/Headquarters investigation files; FBI National Criminal History Fingerprint File; Defense Clearance and Investigations Index (DCII); and other sources, as necessary, to cover specific areas of a subject’s background.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
National Agency Check and Inquiries (NACI)	Consists of a NAC, employment checks, education checks, law enforcement agency checks, and personal reference checks.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
National Crime Information Center (NCIC) Check	Consists of a check of the computerized index of criminal justice information (e.g., criminal record history information, fugitives, stolen properties, missing persons).” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>

<u>Term</u>	<u>Definition</u>
National Foreign Intelligence Board	is chaired by the Director of Central Intelligence and is comprised of Intelligence Community members and distinguished civilians appointed by the President.” <u>Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management</u>
National Foreign Intelligence Program	refers to all programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of Central Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.” <u>Intelligence Reform and Terrorism Prevention Act of 2004.</u>
National Intelligence and Intelligence-Related to the National Security	(A) each refer to intelligence which pertains to the interests of more than one department or agency of the Government; and (B) do not refer to counterintelligence or law enforcement activities conducted by the Federal Bureau of Investigation except to the extent provided for in procedures agreed to by the Director of Central Intelligence and the Attorney General, or otherwise as expressly provided for in this title.” <u>National Security Act.</u>
National security	means the national defense or foreign relations of the United States.” <u>Executive Order 13292, Classified National Security Information, Classified National Security Information, Section 6.1(y).</u>
National Security Positions	Positions defined under Executive Orders 10450 and 12968 that involve activities of the U.S. Government concerned with the protection of the nation from foreign aggression or espionage. These include positions involved with developing defense plans or policies; intelligence or counterintelligence activities; foreign relations, and related activities concerned with preserving the military strength of the United States; and positions that require regular use of, or access to, classified information.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
National Security Systems	[A]s defined in the Clinger-Cohen Act ⁴ , an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.” <u>OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 and the Clinger-Cohen Act;</u> “[A]ny telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be administrative

<u>Term</u>	<u>Definition</u>
	and business applications (including payroll, finance, logistics, and personnel management applications). The policies and procedures established in this Circular will apply to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in Section 5141 of the Clinger-Cohen Act (Pub. L. 104-106, 40 U.S.C. 1451). Applicability of Clinger-Cohen Act to national security systems shall include budget with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2)).” <u>OMB Circular A-130, Management of Federal Information Resources.</u>
Native Desktop	Standard workstation used in the daily performance of ones job.
Need-to-know	means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.” <u>Executive Order 13292, Classified National Security Information, Classified National Security Information, Section 6.1(z) and Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management; DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program;</u> “The determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties.” <u>DHS Management Directive, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.</u> “A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.” <u>DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage.</u>
Network	means a system of two or more computers that can exchange data or information.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(aa).</u>
Networks	Include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.” <u>NIST Special Publication 800-18.</u>
Non-Critical Sensitive	Non-Critical Sensitive positions have the potential for serious damage to the national security. These positions involve either access to SECRET or CONFIDENTIAL national security information materials, or duties that may adversely affect, directly or indirectly, the national security operations of the Department.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>

<u>Term</u>	<u>Definition</u>
Nonpublic Personal Information	Personally identifiable financial information - (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. The term personally identifiable financial information does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of GRAMM-LEACH BLILELY ACT. The term also shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information. The term shall include, however, any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information.” <u>Gramm-Leach Blilely Act.</u>
Non-repudiation	This service provides proof of the integrity and origin of data that can be verified by a third party. [. . .] Non-repudiation of origin is protection against a sender of a message later denying transmission.” <u>NIST Special Publication 800-21.</u>
Non-Sensitive/Low Risk	Non-Sensitive/Low Risk positions have the potential for limited impact on the integrity and efficiency of the service. These positions involve duties and responsibilities of limited relation to an agency or program mission.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Objectivity	<p>involves two distinct elements: presentation and substance. 1) "Objectivity" includes whether disseminated information is being presented in an accurate, clear, complete, and unbiased manner. This involves whether the information is presented within a proper context. Sometimes, in disseminating certain types of information to the public, other information must also be disseminated in order to ensure an accurate, clear, complete, and unbiased presentation. Also, the agency needs to identify the sources of the disseminated information (to the extent possible, consistent with confidentiality protections) and, in a scientific, financial, or statistical context, the supporting data and models, so that the public can assess for itself whether there may be some reason to question the objectivity of the sources. Where appropriate, data should have full, accurate, transparent documentation, and error sources affecting data quality should be identified and disclosed to users.</p> <p>In addition, "objectivity" involves a focus on ensuring accurate, reliable, and unbiased information. In a scientific, financial, or statistical context, the original and supporting data shall be generated, and the analytic results shall be developed, using sound statistical and research methods. a. If data and analytic results have been subjected to formal, independent, external peer review, the information may generally be presumed to be of acceptable objectivity. However, this presumption is rebuttable based on a persuasive showing by the petitioner in a particular instance. If agency sponsored peer review is employed to help satisfy the objectivity standard, the review process employed shall meet the general criteria for competent and credible peer review recommended by OMB-OIRA to the President's Management</p>

Term

Definition

Council (9/20/01) (http://www.whitehouse.gov/omb/inforeg/oira_review-process.html), namely, "that (a) peer reviewers be selected primarily on the basis of necessary technical expertise, (b) peer reviewers be expected to disclose to agencies prior technical/policy positions they may have taken on the issues at hand, (c) peer reviewers be expected to disclose to agencies their sources of personal and institutional funding (private or public sector), and (d) peer reviews be conducted in an open and rigorous manner." b. If an agency is responsible for disseminating influential scientific, financial, or statistical information, agency guidelines shall include a high degree of transparency about data and methods to facilitate the reproducibility of such information by qualified third parties. 3) With regard to analysis of risks to human health, safety and the environment maintained or disseminated by the agencies, agencies shall either adopt or adapt the quality principles applied by Congress to risk information used and disseminated pursuant to the Safe Drinking Water Act Amendments of 1996 (42 U.S.C. 300g-1(b)(3)(A) & (B)). Agencies responsible for dissemination of vital health and medical information shall interpret the reproducibility and peer-review standards in a manner appropriate to assuring the timely flow of vital information from agencies to medical providers, patients, health agencies, and the public. Information quality standards may be waived temporarily by agencies under urgent situations (e.g., imminent threats to public health or homeland security) in accordance with the latitude specified in agency-specific guidelines. 4) If, at the end of the public comment period, an agency is not prepared to identify what kinds of original and supporting data will be subject to the reproducibility standard, then the agency must include in its guidelines a statement to the effect that the agency shall assure reproducibility for those kinds of original and supporting data according to - commonly accepted scientific, financial, or statistical standards." DHS Management Directive Number: 8200.1, Information Quality: OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies.

Occupant Escort

A person whose work space resides within the SCIF and who has been authorized by the FSO to escort uncleared personnel within the facility. The "Occupant Escort" should be the first choice for escort duties." DHS Management Directive Number: 11051, Department of Homeland Security SCIF Escort Procedures.

Office of Information and Regulatory Affairs

"Is a Federal office that Congress established in the 1980 Paperwork Reduction Act. OIRA is an office within the Office of Management and Budget, which is an agency within the Executive Office of the President. [. . .] In addition to reviewing draft regulations under Executive Order 12866, OIRA reviews collections of information under the Paperwork Reduction Act, and also develops and oversees the implementation of government-wide policies in the areas of information technology, information policy, privacy, and statistical policy." http://www.whitehouse.gov/omb/inforeg/qa_2-25-02.pdf.

<u>Term</u>	<u>Definition</u>
Office of Information and Regulatory Affairs (OIRA)	Is a Federal office that Congress established in the 1980 Paperwork Reduction Act. OIRA is an office within the Office of Management and Budget, which is an agency within the Executive Office of the President. [. . .] In addition to reviewing draft regulations under Executive Order 12866, OIRA reviews collections of information under the Paperwork Reduction Act, and also develops and oversees the implementation of government-wide policies in the areas of information technology, information policy, privacy, and statistical policy.” http://www.whitehouse.gov/omb/inforeg/qa_2-25-02.pdf
Open Source Information	“means any all information that can be derived from overt collection: all types of media, government reports and other documents, scientific research and reports, commercial vendors of information, the Internet, etc. The main qualifiers to open source information are that it does not require any type of clandestine collection techniques to obtain it and that it must be obtained through means that entirely meet the copyright and commercial requirements of vendors where applicable.” <u>Open Source Intelligence: New Myths, New Realities, Mark M. Lowenthal, President, OSS USA).</u>
Open source intelligence (OSINT)	“applies the proven methods of the Intelligence Community to open source information, and transforms volumes of information into an unclassified intelligence product that represents judicious source discovery and validation, multi-source integration and subject-matter expertise.” <u>Open Source Intelligence: New Myths, New Realities, Mark M. Lowenthal, President, OSS USA.</u> The internet is only a tiny slice of OSINT. It includes internet searches and searches of commercially available databases.”
Operational Controls	“Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).” <u>NIST Special Publication 800-18.</u>
Oral Communication	“ Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication. ” <u>Electronic Communications Privacy Act.</u>
Organizational Element	As used in this directive, organizational element is as defined in DHS MD Number 0010.1, Management Directive System and DHS Announcements.” <u>DHS Management Directive Number: 11041, Protection of Classified National Security Information Program Management and DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage and DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u> See also, DHS Organizational Element.
Original classification	means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(bb).</u>

<u>Term</u>	<u>Definition</u>
Original classification authority	means an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(cc)</u> . “An individual authorized in writing, either by the President, or by agency heads, or other officials designated by the President, to classify information in the first instance.” <u>DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage</u> .
Parties	The parties to a MOU/MOA covered by this instruction are the DHS and one or more governmental or private entities.” <u>DHS Interim Management Directive Number: 0450.1, Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA)</u> .
Password	A string of characters used to authenticate an identity or to verify access authorization.” <u>NIST Special Publication 800-21</u> ; “[C]onfidential authentication information composed of a string of characters.” <u>HIPAA Regulations</u> .
Pattern of Activities	requires a series of acts with a common purpose or objective.” <u>National Security Act</u> .
Permanent records	Those records that NARA appraises as having sufficient value to warrant continued preservation by the Federal Government as part of the National Archives of the United States, because the records have continuing value as documentation of the organization and functions of DHS or because the records document the nation’s history by containing significant information on persons, things, problems, and conditions.” <u>DHS Management Directive Number: 0550.1, Records Management</u> . “DHS records determined by DHS and approved by NARA to be permanent must be available in a medium and format that conforms with the standards for permanent records. DHS permanent records will be transferred to the National Archives of the United States at the time designated on a NARA-approved Request for Records Disposition (SF115). When permanent records are transferred to National Archives, legal custody of the records is transferred to NARA at this time. NARA takes measures needed to preserve the records and also provides reference service, including service to the creating agency.” <u>DHS Records Management Handbook</u> .
Permissioning Systems	Building privacy rules into databases and search engines through digital rights management and using browsers to enforce privacy principles. These systems show the privacy status of information, highlight compliance requirements for accessing particular data, and support audit functions built into the system.” http://www.heritage.org/Research/HomelandDefense/lm11.cfm

<u>Term</u>	<u>Definition</u>
Person	means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.” <u>Foreign Intelligence Surveillance Act</u> ; “[A]ny employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.” <u>Electronic Communications Privacy Act of 1974</u> ; “[A]n individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision.” <u>The Paperwork Reduction Act</u> ; “[A]ny individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.” <u>Fair Credit Reporting Act</u> .
Personal Digital Assistant (PDA)	A hand-held device that is a type of PED used for computing and information storage and retrieval capabilities such as calendars and address books. Some examples include Palm Pilots, Black Berries, and MP3 players.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities</u> .
Personal Identification Number	A 4 to 12 character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.” <u>NIST Special Publication 800-21</u> .
Personal Information	Information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.” <u>Drivers Privacy Protection Act</u> .
Personal Papers	Documentary materials of a private or nonpublic character that do not relate to, or have an effect upon, the conduct of agency business. Personal papers are excluded from the definition of Federal records and are not owned by the Government.” <u>DHS Management Directive Number: 0550.1, Records Management</u> .
Personally Identifiable Information	[I]ncludes, but is not limited to: (a) The student's name; (b) The name of the student's parent or other family member; (c) The address of the student or student's family; (d) A personal identifier, such as the student's social security number or student number; (e) A list of personal characteristics that would make the student's identity easily traceable or (f) Other information that would make the student's identity easily traceable. <u>FERPA Regulations</u> .
Personally Owned Equipment	Equipment not owned or leased by the U.S. Government.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities</u> .

<u>Term</u>	<u>Definition</u>
Physical Safeguards	Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.” <u>HIPAA Regulations</u> .
Plaintext	“Unencrypted (unenciphered) data.” <u>NIST Special Publication 800-21</u> .
Policy-Based Authorization	The rights granted to a user to access, read, modify, insert, or delete certain data, or to execute certain programs based on policy or role as opposed to based on an individual’s user name.
Portable Electronic Device (PED)	Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, processing, and/or transmitting data, video/photo images, and/or voice emanations. This definition generally includes, but is not limited to, laptops, PDAs, pocket PCs, palmtops, Media Players (MP3s), memory sticks (thumb drives), cellular telephones, PEDs with cellular phone capability, and pagers.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities</u>
Practical Utility	means the ability of an agency to use information, particularly the capability to process such information in a timely and useful fashion.” <u>Paperwork Reduction Act</u> .
Privacy Act of 1974	This federal statute controls the collection and dissemination of personal information by the federal government. It guarantees that U.S. citizens and Lawful Permanent Residents have: (1) the right to see records about themselves that are maintained by the federal government (provided that information is not subject to one or more of the Privacy Act's exemptions); (2) the right to amend inaccurate, irrelevant, untimely, or incomplete records; and (3) the right to sue the government for failure to comply with its requirements. It also contains fair information practices that: (1) require that information about a person be collected from that person to the greatest extent practicable; (2) require agencies to ensure that their records are relevant, accurate, timely, and complete; and (3) prohibit agencies from maintaining information describing how an individual exercises his or her First Amendment rights (unless the individual consents to it, it is permitted by statute, or is within the scope of an authorized law enforcement investigation).
Privacy Act Record	Any item, collection, or grouping of information about an individual that is maintained by DHS in a system of records, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.” <u>DHS Management Directive Number: 0470.1, Privacy Act Compliance</u> . <u>See also, System of Records</u> .

<u>Term</u>	<u>Definition</u>
Privacy Impact Assessment (PIA)	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.” <u>OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.</u>
Privacy Policy In Standardized Machine-Readable Format	[A] statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser.” <u>OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.</u>
Private Key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.” <u>NIST Special Publication 800-21.</u>
Private Sector	Commerce, academia, the media and non-governmental organizations.
<u>Profiling</u>	A technique by which information regarding past experiences with a class of persons is used to establish characteristics that are then used to search databases or other records for other persons who closely fit those characteristics. <u>See also, Racial Profiling.</u>
Program Manager (PM)	Government manager responsible for the overall conduct of a DHS program or activity and responsible for determining if a PED is mission essential.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.</u>
Protected Computer	include "a computer . . . which is used in interstate or foreign commerce or communication." <u>Electronic Communications Privacy Act.</u> 18 U.S.C. § 1030(e)(2)(B).
Protected Critical Infrastructure Information or Protected CII	means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in Sec. 29.5 of this chapter. This information maintains its protected status unless the CII Program Manager renders a final decision that the information is not Protected CII. <u>DHS Procedures for Handling Critical Infrastructure Information</u> , 6 CFR Sec. 29.2 (f); “Critical infrastructure information (CII) is defined in 6 U.S.C. 131(3) (Section 212(3) of the Homeland Security Act. Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.” <u>DHS Management Directive, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.</u>

<u>Term</u>	<u>Definition</u>
Protected Health Information (PHI)	Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv).” <u>HIPAA Regulations</u> .
Protected System	means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.” <u>DHS Procedures for Handling Critical Infrastructure Information</u> , 6 CFR Sec. 29.2 (g).
Public Information	Any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public.” <u>Paperwork Reduction Act</u> .
Public Key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public. [. . .] The public key is used to verify a digital signature. This key is mathematically linked with a corresponding private key.” <u>NIST Special Publication 800-21</u> .
Public Key Infrastructure (PKI)	An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys.” <u>NIST Special Publication 800-21</u> .
Public Trust Positions	Positions defined under 5 CFR 731 that may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust; positions involving access to, or operation of, or control of financial records, with a significant risk for causing damage or realizing personal gain.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program</u> .
Purpose	has the meaning as described in section 214(a)(1) of the CII Act of 2002, and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.” <u>DHS Procedures for Handling Critical Infrastructure Information</u> , 6 CFR Sec. 29.2 (h).

<u>Term</u>	<u>Definition</u>
Quality	n encompassing term comprising utility, objectivity, and integrity. Therefore, the guidelines sometimes refer to these three statutory terms, collectively, as "quality." <u>DHS Management Directive Number: 8200.1, Information Quality; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies.</u>
Racial Profiling	is "any police-initiated action that relies on the race, ethnicity, or national origin rather than the behavior of an individual or information that leads the police to a particular individual who has been identified as being, or having been, engaged in criminal activity." <u>DOJ Resource Guide on Racial Profiling Data Collection Systems, http://www.ncjrs.org/pdffiles1/bja/184768.pdf; "Racial profiling', at its core concerns the invidious use of race or ethnicity as a criterion in conducting stops, searches and other law enforcement investigative procedures. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity." <u>DOJ Guidance Regarding The Use Of Race By Federal Law Enforcement Agencies, http://www.usdoj.gov/crt/split/documents/guidance_on_race.htm</u></u>
Readily Accessible to the General Public	With respect to a radio communication, that such communication is not: (A) scrambled or encrypted; (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication; (C) carried on a subcarrier or other signal subsidiary to a radio transmission; (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio." <u>Electronic Communications Privacy Act.</u>
Receive-only Pager	One-way text pagers that can receive messages, but are not capable of user input for transmission." <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.</u>
Recipient Agency	Any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program." <u>Privacy Act of 1974.</u>
Recipient Agency	Any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program." <u>Privacy Act of 1974.</u>
Record	includes any writing, drawing, map, tape, film, photograph, or other means by which information is preserved, irrespective of format." <u>49 CFR Sec. 1520.1(b).</u>

<u>Term</u>	<u>Definition</u>
Recordkeeping Requirement	[A] requirement imposed by or for an agency on persons to maintain specified records, including a requirement to-- (A) retain such records; (B) notify third parties, the Federal Government, or the public of the existence of such records; (C) disclose such records to third parties, the Federal Government, or the public; or (D) report to third parties, the Federal Government, or the public regarding such records.” <u>Paperwork Reduction Act</u> .
Recordkeeping system	A system in which records are collected, organized, +and categorized to facilitate their preservation, retrieval, use, and disposition.” <u>DHS Management Directive Number: 4500.1, DHS E-Mail Usage</u> .
Records	means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant. <u>Executive Order 13292, Classified National Security Information, Section 6.1(dd)</u> ; “Any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.” <u>FERPA Regulations</u> ; “[A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.” <u>Privacy Act of 1974 and The Freedom of Information Act</u> ; “All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included.” <u>OMB Circular A-130, Management of Federal Information Resources</u> and <u>44 U.S.C. 3301</u> ; “All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.” <u>DHS Records Management Handbook</u> and <u>The Records Disposal Act</u> (the Records Disposal Act additionally states that “Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included.”); “All

<u>Term</u>	<u>Definition</u>
	recorded information, regardless of medium or format, made or received by DHS under Federal law or in connection with the transaction of public business, either preserved or appropriate for preservation because of their administrative, legal, fiscal or informational value. Records serve as organizational memory; they are of critical importance in ensuring that DHS continues to function effectively and efficiently.” <u>DHS Management Directive Number: 0550.1, Records Management.</u>
Records Creation	The production or reproduction of any record.” <u>Records Management by the Archivist of the United States.</u>
Records Disposition	Any activity with respect to-- (A) disposal of temporary records no longer necessary for the conduct of business by destruction or donation; (B) transfer of records to Federal agency storage facilities or records centers; (C) transfer to the National Archives of the United States of records determined to have sufficient historical or other value to warrant continued preservation; or (D) transfer of records from one Federal agency to any other Federal agency.” <u>Records Management by the Archivist of the United States.</u>
Records having permanent historical value	means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(ee).</u>
Records Maintenance and Use	Any activity involving-- (A) location of records of a Federal agency; (B) storage, retrieval, and handling of records kept at office file locations by or for a Federal agency; (C) processing of mail by a Federal agency; or (D) selection and utilization of equipment and supplies associated with records and copying.” <u>Records Management by the Archivist of the United States.</u>
Records Management	The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2)).” <u>OMB Circular A-130, Management of Federal Information Resources.</u>
Records management	means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(ff).</u>

<u>Term</u>	<u>Definition</u>
Records Series	File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access and use.” <u>DHS Records Management Handbook</u> .
Registration Label	A label or bar code attached to a PED indicating that it has been approved for entry into DHS SCI Facilities because all known risks have been mitigated or accepted.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities</u> .
Reproducibility	means that the information is capable of being substantially reproduced, subject to an acceptable degree of imprecision. For information judged to have more (less) important impacts, the degree of imprecision that is tolerated is reduced (increased). If agencies apply the reproducibility test to specific types of original or supporting data, the associated guidelines shall provide relevant definitions of reproducibility (e.g., standards for replication of laboratory data). With respect to analytic results, "capable of being substantially reproduced" means that independent analysis of the original or supporting data using identical methods would generate similar analytic results, subject to an acceptable degree of imprecision or error.” <u>DHS Management Directive Number: 8200.1, Information Quality and OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies</u> .
Responsible Official	The head of the organizational unit having immediate custody of the records requested or a designated official. The responsible official makes initial determinations to grant or deny requests for access to records and requests for fee waivers. The responsible official will also determine a requester's category for fee purposes.” DHS Management Directive Number: 0460.1, <u>Freedom of Information Act Compliance</u> ; The official having custody of the records requested, or a designated official, who makes initial determinations whether to grant or deny requests for notification, access to records, accounting of disclosures, and amendments of records.” <u>DHS Management Directive Number: 0470.1, Privacy Act Compliance</u> .
Risk	A measure of the potential inability to achieve overall program objectives within constraints. It has two components: the <i>probability/likelihood</i> of failing to achieve a particular outcome, and the <i>consequences/impacts</i> of failing to achieve that outcome.
Risk	The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.” <u>NIST Special Publication 800-18</u> ; “The net mission impact considering the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and the resulting impact if this should occur.” <u>NIST Special Publication 800-47</u> .

<u>Term</u>	<u>Definition</u>
Risk Management	“Is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.” <u>NIST Special Publication 800-34</u> .
Risk Assessment	The process of evaluating security risks based on analysis of threats to and/or vulnerabilities of a system or operation.” <u>DHS Management Directive Number: 11060, Operations Security Program</u> . The process of identifying and analyzing program areas and critical processes to increase the probability of meeting objectives. <i>Risk identification</i> is the process of examining the program areas and each critical process to identify and document the associated risk. <i>Risk analysis</i> is the process of examining each identified risk area or process to refine the description of the risk, isolating the cause, and determining the effects. It includes risk rating and prioritization in which risk events are defined in terms of their probability of occurrence, severity of consequence/impact, and relationship to other risk areas or processes.
Risk Documentation	is recording, maintaining, and reporting assessments, mitigation analysis and plans, and monitoring results.
Risk Management	The act or practice of dealing with risk including planning for risk, assessing (identifying and analyzing) risk areas, developing risk mitigation options, monitoring risks to determine how they have changed, and documenting the overall risk management program.
Risk Mitigation	The process that identifies, evaluates, selects and implements options to set risk at acceptable levels given constraints and objectives. This includes the specifics on what should be done, when it should be accomplished, who is responsible and associated cost and schedule.
Risk Monitoring	The process that systematically tracks and evaluates the performance of risk-mitigation activities against established metrics and develops further risk-mitigation options, as appropriate. It feeds information back into the other risk management activities of planning, assessment and mitigation as show in the figure.
Risk Planning	The process of developing and documenting an organized, comprehensive and interactive strategy and methods of identifying and tracking risk areas, developing risk mitigation plans, performing continuous risk assessments and assigning resources.
Routine Use	Means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.” <u>Privacy Act of 1974</u> .

<u>Term</u>	<u>Definition</u>
Rules of Behavior	The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability.” <u>NIST Special Publication 800-18.</u>
Sabotage	means activities that involve a violation of chapter 105 of title 18 , or that would involve such a violation if committed against the United States.” <u>Foreign Intelligence Surveillance Act.</u>
Safeguarding	means measures and controls that are prescribed to protect classified information.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(gg).</u>
SCI Facility (SCIF)	is an accredited area, room, group of rooms, buildings, or installation where SCI may be used, stored, discussed and/or processed.” <u>Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management.</u>
Secrecy	Refers to denial of access to information by unauthorized individuals.” <u>NIST Special Publication 800-21.</u>
Secret	shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.” <u>Executive Order 13292, Classified National Security Information, Section 1.2(1):</u> “Level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.” <u>DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage.</u>
Secret information	Information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security of the United States.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Secret Key	A cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall not be made public. The use of the term “secret” in this context does not imply a classification level, rather the term implies the need to protect the key from disclosure or substitution.” <u>NIST Special Publication 800-21.</u>
Sector	A large group of users linked to each other by related missions. For the purposed of this report, the sectors are Homeland Security; Law Enforcement; Defense; State, Local & Tribal authorities; Intelligence; Diplomatic Community; and the Private Sector.

<u>Term</u>	<u>Definition</u>
Secure and Reliable Forms of Identification,	for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).” <u>Homeland Security Presidential Directive/HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors.</u>
Security Clearance	is a formal authorization for an employee with a specific need-to-know to have access to information that is classified as Confidential, Secret, or Top Secret in the interest of national security or the defense of the United States.” <u>DHS Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management.</u>
Security Controls	<i>Protective measures used to meet the security requirements specified for IT resources.”</i> <u>NIST Special Publication 800-47.</u>
Security Escort	An SCI-cleared security officer or individual authorized by the FSO to provide escort duties within a SCIF.” <u>DHS Management Directive Number: 11051, Department of Homeland Security SCIF Escort Procedures.</u>
Security Incident	The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” <u>HIPAA Regulations.</u>
Security Issue Review Program	Program involves conducting preliminary actions to determine if an internal security incident or indicator should result in a referral to the Federal Bureau of Investigation, pursuant to Section 811 of the Intelligence Authorization Act of 1995.” <u>DHS Management Directive Number: 11052, Internal Security Program.</u>
Security Liaison	An official who is assigned responsibility for implementation and management of an organizational element’s security program as a secondary or additional duty.” <u>DHS Management Directive Number: 11041, Protection of Classified National Security Information Program Management;</u> “An official who is assigned responsibility for implementing and managing an organizational element’s security program as a secondary or additional duty.” <u>DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage.</u>
Security Officer	Authorized position within an organizational element whose primary duties are to serve as the lead official for the development, implementation, and management of security programs within the organizational element.” <u>DHS Management Directive Number: 11041, Protection Of Classified National Security Information Program Management and DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage.</u>

<u>Term</u>	<u>Definition</u>
Self-inspection	means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(hh).</u>
Senior Agency Official	is the official designated by the agency head under section 5.4(d) of E.O. 12958, as amended, who directs and administers the agency’s program under which information is classified, safeguarded, and declassified. The Senior Agency Official for DHS is the Chief Security Officer.” <u>DHS Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management and DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage.</u>
Senior Official of the Intelligence Community (SOIC)	is the head of an organization within the Intelligence Community, as defined by the National Security Act of 1947. Within DHS there are five SOICs: The Secretary, the Deputy Secretary, the Under Secretary for Information Analysis and Infrastructure Protection, the Assistant Secretary for Information Analysis, and the Assistant Commandant for Intelligence for the United States Coast Guard.” <u>Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management.</u> “The heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations. DHS SOICs are the Secretary, the Deputy Secretary, The Under Secretary for Information Analysis and Infrastructure Protection, and the Assistant Secretary for Information Analysis.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.</u>
Sensitive But Unclassified (SBU)	(1). A caveat used to elicit caution in handling information that is technically unclassified, but sensitive. (2). (<i>Network context</i>) An SBU network supports only unclassified processing, but is separated from the commercial Internet to protect the sensitive content information. (Sensitivities may relate to incomplete or unverified data sets, or cost, contractual, and proprietary data).
Sensitive Compartmented Information (SCI)	(1). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCID 1/19). (2). All information and materials bearing special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products for which Community systems of compartmentation have been or will be formally established.

<u>Term</u>	<u>Definition</u>
Sensitive Compartmented Information (SCI)	is classified information concerning, or derived from, intelligence sources, methods, or analytical processes requiring handling within formal access control systems established by the Director Central Intelligence (DCI). SCI is also referred to as "codeword" information. The sensitivity of this information requires that it be protected in a much more controlled environment than other classified information. Therefore, the DCI has established special policies and procedures for the protection of SCI. These policies and procedures are promulgated through Director of Central Intelligence Directives (DCIDs)." <u>Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management</u> ; "Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence." <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities</u> . "Classified information concerning, or derived from, intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the Director of Central Intelligence." <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program</u> .
Sensitive Compartmented Information (SCI) Facility	An accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed." <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities</u> . See also, <u>DHS SCIF Facility</u> .
Sensitive Information	Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act." <u>NIST Special Publication 800-18</u> ; "Any information, the loss, misuse, unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy." <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program</u> ; "Information, the compromise of which could adversely affect the national interest or the privacy to which individuals are entitled under the Privacy Act, but that has not been specifically authorized to be classified (commonly referred to as Sensitive But Unclassified (SBU) Information.) <u>DHS Management Directive Number: 11060, Operations Security Program</u> .

<u>Term</u>	<u>Definition</u>
Sensitive Security Information (SSI)	Sensitive security information (SSI) is defined in 49 C.F.R. Part 1520. SSI is a specific category of information that requires protection against disclosure. 49 U.S.C. 40119 limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.” <u>DHS Management Directive, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.</u>
Sensitivity	In an information technology environment consists of the system, data, and applications which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.” <u>NIST Special Publication 800-18.</u>
Service Recipient	An agency organizational unit, programmatic entity, or chargeable account that receives information processing services from an information processing service organization (IPSO). A service recipient may be either internal or external to the organization responsible for providing information resources services, but normally does not report either to the manager or director of the IPSO or to the same immediate supervisor.” <u>OMB Circular A-130, Management of Federal Information Resources.</u>
Single Scope Background Investigation (SSBI)	Consists of a National Agency Check (NAC)' a spouse or cohabitant NAC' a personal Subject Interview' and citizenship, education, employment, residence, law enforcement, and record searches covering the most recent ten (10) years of an individual's life, or since his or her 18th birthday, whichever is shorter.” <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.</u>
Source Agency	Any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program.” <u>Privacy Act of 1974.</u>
Source document	means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(jj).</u>
Special access program	means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(kk).</u>

<u>Term</u>	<u>Definition</u>
Special Security Officer (SSO)	works under the direction of the Chief, Special Security Programs Division and administers the receipt, control and accountability of SCI. The SSO oversees SCI security functions and reporting requirements for subordinate SCIFs.” <u>DHS Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management</u> : “Officer responsible for the overall security posture of a particular DHS program or facility on behalf of the government.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities</u> : “DHS Official who provides SCI advice and assistance and normally has day-to-day SCI security cognizance over all DHS security components and subordinate SCIFs.” <u>DHS Management Directive Number: 11051, Department of Homeland Security SCIF Escort Procedures</u> .
Special Security Representative (SSR)	works under the direction of the supporting SSO, and is responsible for the day-to-day management and implementation of SCI security and administrative instructions for a separate, subordinate DHS SCIF.” <u>Department Of Homeland Security Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management</u> .
Special Sensitive	Special Sensitive positions include any position designated at a level higher than Critical Sensitive that complement E.O. 10450 and E.O. 12968 (such as Director of Central Intelligence Directive 6/4 that sets investigative requirements and access to Sensitive Compartmented Information and other intelligence-related Special Sensitive information). <u>DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program</u> .
State	includes the District of Columbia and any commonwealth, territory, or possession of the United States.” <u>Homeland Security Information Sharing Act</u> .
State and Local Personnel	means any of the following persons involved in prevention, preparation, or response for terrorist attack: (A) State Governors, mayors, and other locally elected officials. (B) State and local law enforcement personnel and firefighters. (C) Public health and medical professionals. (D) Regional, State, and local emergency management agency personnel, including State adjutant generals. (E) Other appropriate emergency response agency personnel. (F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section.” <u>Homeland Security Information Sharing Act</u> .
Statistical Record	[A] record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of Title 13.” <u>Privacy Act of 1974</u> .
Student	Any person with respect to whom an educational agency or institution maintains education records or personally identifiable information, but does not include a person who has not been in attendance at such agency or institution. <u>Family Educational Right to Privacy Act</u> .

<u>Term</u>	<u>Definition</u>
Submission to DHS	“as referenced in these procedures means any transmittal of CII from any entity to DHS. The CII may be provided to DHS either directly or indirectly via another Federal agency, which, upon receipt of the CII, will forward it to DHS.” <u>DHS Procedures for Handling Critical Infrastructure Information</u> , 6 CFR Sec. 29.2 (i).
Suitability	A determination based on an individual's character or conduct that may have an impact on the integrity or efficiency of their employment. Determinations made under this category are distinct from determinations of eligibility for assignment to, or retention in, sensitive national security positions.” DHS Management Directive Number: 11050.2, Personnel Security and Suitability Program.
System	[A] generic term used for brevity to mean either a major application or a general support system.” <u>NIST Special Publication 800-18</u> .
System Administrator	A person who manages a multi-user computer system. Responsibilities are similar to that of a network administrator. A system administrator would perform systems programmer activities with regard to the operating system and other network control programs.” <u>NIST Special Publication 800-40</u> .
System Development Life Cycle	The scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.” <u>NIST Special Publication 800-34</u> .
System Interconnection	The direct connection of two or more IT systems for the purpose of sharing data and other information resources.” <u>NIST Special Publication 800-47</u> .
System Manager	The official identified in the system notice who is responsible for the operation and management of the system of records.” <u>DHS Management Directive Number: 0470.1, Privacy Act Compliance</u> .
System of Records	[A] group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” Privacy Act of 1974; DHS Management Directive Number: 4500.1, DHS E-Mail Usage; “A group of any records under the control of DHS from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” <u>DHS Management Directive Number: 0470.1, Privacy Act Compliance</u> . See also, <u>Privacy Act Records</u>
Systematic declassification review	means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(II)</u> .
Systems Security Plan (SSP)	The formal documentation of the security plan for a particular system.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities</u> .

<u>Term</u>	<u>Definition</u>
Tear Line	The place on an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the "need-to-know" principle.
Technical Controls	Hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications." <u>NIST Special Publication 800-18.</u>
Technical Safeguards	The technology and the policy and procedures for its use that protect electronic protected health information and control access to it." <u>HIPAA Regulations.</u>
Technical Surveillance Countermeasures	are techniques and measures used to detect and nullify a wide variety of technologies used to obtain unauthorized access to classified national security information, restricted data, and/or unclassified sensitive information." <u>DHS Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management.</u>
Telecommunications	means the preparation, transmission, or communication of information by electronic means." Executive Order 13292, Section 6.1(mm); "The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received." <u>NIST Special Publication 800-59 and 47 USC 5 153.</u>
Telecommunications and Automated Information Systems (TAIS)	is defined any telecommunications or computer related equipment, or interconnected system or subsystems of equipment, that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice or data (digital or analog), including software, firmware, and hardware." <u>DHS Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management.</u>
TEMPEST	is an information protection program to preclude inadvertent disclosure of national security information through poor design or installation practices." <u>DHS Management Directive System, MD Number: 11043, Sensitive Compartmented Information Program Management.</u>

<u>Term</u>	<u>Definition</u>
Temporary Records	Those records that are designated for either immediate disposal or for disposal after a specified period of time or an event, in accordance with a NARA-approved Request for Records Disposition (SF 115) or the General Records Schedule. Temporary records may document DHS business processes or document legal rights of the government or the public, document government accountability, or contain information of administrative or fiscal value. Depending on the type of record, the retention period may range from immediate destruction to as long as 100 years.” <u>DHS Management Directive Number: 0550.1, Records Management</u> ; “Temporary records will be maintained and disposed of only in accordance with an approved records control schedule. Records classified as temporary should not be retained beyond their authorized retention period; nor will they be destroyed or otherwise disposed of prior to the end of their authorized retention period.” <u>DHS Records Management Handbook</u> .
Terrorism	means any activity that-- (A) involves an act that-- (i) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and (ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (B) appears to be intended-- (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.” <u>The Homeland Security Act</u> , 6 U.S.C. section 101(15).
Terrorism Information	means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to— (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.” <u>Intelligence Reform and Terrorism Prevention Act and Executive Order 13356, Strengthening the Sharing of Terrorism Information to Protect Americans</u> .
Terrorist-Related Screening	means the collection, analysis, dissemination, and use of information related to people, cargo, conveyances, and other entities and objects that pose a threat to homeland security. Terrorist-related screening also includes risk assessment, inspection, and credentialing.” <u>Homeland Security Presidential Directive/HSPD-11, Comprehensive Terrorist-Related Screening Procedures</u> .
Threat	An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.” <u>NIST Special Publication 800-18</u> ; “An entity or event with the potential to harm a system.” <u>NIST Special Publication 800-21</u> ; “The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.” <u>NIST Special Publication 800-47</u> .

<u>Term</u>	<u>Definition</u>
Threat Analysis	An examination of an adversary’s technical and operational capabilities, motivation, and intentions to detect and exploit vulnerabilities.” <u>DHS Management Directive Number: 11060, Operations Security Program.</u>
Top Secret	shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.” <u>Executive Order 13292, Classified National Security Information, Section 1.2(1); “Information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security of the United States.” DHS Management Directive Number: 11050.2, PERSONNEL SECURITY AND SUITABILITY PROGRAM; “Level of classification applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.” DHS Management Directive Number: 11045, Protection of Classified National Security Information: Accountability, Control, and Storage.</u>
Transnational Threat	means the following: (A) Any transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime) that threatens the national security of the United States; (B) Any individual or group that engages in an activity referred to in subparagraph (A).” (Definition applies only the particular subsection in which it is found in the <u>National Security Act</u>).
Trojan Horse	<i>A computer program containing an apparent or actual useful function that also contains additional functions that permit the unauthorized collection, falsification, or destruction of data.” <u>NIST Special Publication 800-47.</u></i>
Unauthorized disclosure	means a communication or physical transfer of classified information to an unauthorized recipient.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(nn).</u>
United States Person	means the following: (A) A United States citizen; (B) An alien known by the intelligence agency concerned to be a permanent resident alien; (C) An unincorporated association substantially composed of United States citizens or permanent resident aliens; (D) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.” (Definition applies only the particular subsection in which it is found in the <u>National Security Act</u>); “means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section <u>1101 (a)(20)</u> of title <u>8</u>), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.” <u>Foreign Intelligence Surveillance Act.</u>

<u>Term</u>	<u>Definition</u>
Unscheduled Records	Those records whose final disposition has not been approved by NARA. Unscheduled records are potentially permanent and must be treated as if they are permanent.” <u>DHS Management Directive Number: 0550.1, Records Management.</u>
Unsolicited Communications	Unauthorized electronic, written, or telephonic requests for information or suspicious inquiries received by a DHS entity or individual from an external source.” <u>DHS Management Directive Number: 11052, Internal Security Program.</u>
Use	With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.” <u>HIPAA Regulations.</u>
Use	With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.” <u>HIPAA Regulations.</u>
User	Any person or entity who: (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use.” <u>Electronic Communications Privacy Act</u> ; “Any DHS employee, detailee, or contractor who wishes to introduce a PED into or use a PED within a SCI facility.” <u>DHS Management Directive Number: 11021, Portable Electronic Devices in SCI Facilities.</u> “[A] person or entity with authorized access.” <u>HIPAA Regulations.</u>
Utility	refers to the usefulness of the information to its intended users, including the public. In assessing the usefulness of information that the agency disseminates to the public, the agency needs to consider the uses of the information not only from the perspective of the agency but also from the perspective of the public. As a result, when transparency of information is relevant for assessing the information's usefulness from the public's perspective, the agency must take care to ensure that transparency has been addressed in its review of the information.” <u>DHS Management Directive Number: 8200.1, Information Quality; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies.</u>
Virtual Private Network (VPN)	“A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or “tunnel,” between them.” <u>NIST Special Publication 800-47.</u>

<u>Term</u>	<u>Definition</u>
Vital records	These types of records are essential to the continued function or reconstruction of an organization during and after an emergency. Refer to the NARA publication entitled “Vital Records and Records Disaster Mitigation and Recovery” for guidance on handling these types of records. The emergency preparedness needs of DHS will be met through the identification of vital records and pre-positioning copies of them at strategic locations for ready accessibility in the event of a national or local natural or technological disaster.” <u>DHS Records Management Handbook</u> .
Voluntary or Voluntarily,	when used in reference to any submission of CII to DHS, means submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information; such submission may be accomplished by (i.e. come from) a single entity or an ISAO on behalf of itself or its members. The term does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings. In the case of any action brought under the securities laws--as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47)) the term “voluntary” does not include information or statements contained in any documents or materials filed, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 78l(i)) with the Securities and Exchange Commission or with Federal banking regulators; and with respect to the submission of CII, it does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities.” <u>DHS Procedures for Handling Critical Infrastructure Information</u> , 6 CFR Sec. 29.2 (j).
Vulnerability	The susceptibility of information to exploitation by an adversary.” <u>DHS Management Directive Number: 11060, Operations Security Program</u> ; “A flaw or weakness that may allow harm to occur to an automated information system or activity.” <u>NIST Special Publication 800-18</u> ; A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat. <u>NIST Special Publication 800-21</u> ; A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy. <u>NIST Special Publication 800-47</u> ; “A security exposure or mis-configuration in an operating system or other system software or application software component that allows the security policy to be violated. A variety of organizations maintain publicly accessible databases of vulnerabilities based on version number of the software. Much vulnerability can potentially compromise the system or network if successfully exploited.” <u>NIST Special Publication 800-40</u> .
Vulnerability assessment	means any examination of a transportation system, vehicle, or facility to determine its vulnerability to unlawful interference.” <u>49 CFR Sec. 1520.1(b)</u> .
Weapons of Mass Destruction	“means chemical, biological, radiological, and nuclear weapons.” <u>Executive Order 13292, Classified National Security Information, Section 6.1(pp)</u> .

<u>Term</u>	<u>Definition</u>
Web Services	A group of closely related emerging technologies describing a service oriented, component based application architecture founded on an open Internet centric infrastructure. Web services represent a model where discrete e-business tasks are distributed widely across a value net. Web services components can be recombined by other organizations to meet their software applications and business needs.
Wire Communication	means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.” <u>Foreign Intelligence Surveillance Act</u> ; “Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.” <u>Electronic Communications Privacy Act</u> .
Worm	A computer program or algorithm that replicates itself over a computer network and usually performs malicious actions.” <u>NIST Special Publication 800-47</u> ; “A type of malicious code particular to networked computers. It is a self-replicating program (unlike a virus which needs a host program) which works its way through a computer network exploiting vulnerable hosts, replicating and causing whatever damage it was programmed to do.” <u>NIST Special Publication 800-40</u> .
Write to Release	A general approach where reports are written in such a way that references to sources and methods are disguised or eliminated so that the report can be distributed to customers or partners at lower security levels.

Annex D From Enabling Information Sharing to Facilitating Community Collaboration

Introduction

Enabling, encouraging, and facilitating information sharing and collaboration require different supportive mechanisms culturally and technologically. Enabling information sharing is the first step, involving cross-organizational access to information according to sharing policies and procedures. But access to information does not necessarily lead to effective knowledge sharing and collaboration. Mantovani (1996) explains that when people share knowledge, they are not just sharing information; they are also sharing cultural and social references. Likewise, when people seek knowledge, they are not just seeking information; they are seeking information grounded in, and carrying different meanings to different social communities. Information is viewed, perceived, and used differently by each community. When users from different communities share information, they interpret that knowledge in new contexts, transforming and creating new knowledge, while at the same time contributing toward the identity of the communities grounding that knowledge. The role of the computer environment, then, is to encourage, support, mediate, and guide these processes of community development through knowledge seeking, sharing, and joint understanding (Mennecke 1997).

The next section explains why special attention might be needed to encourage and ensure that the right information is shared in the right contexts. Section 3 describes a few different technological foundations for facilitating knowledge sharing and community development. Section 4 discusses mechanisms for evaluating and ensuring information sharing progress.

Knowledge sharing breakdowns

Tools and policies that help communities manage information security risks are essential to defining information sharing boundaries and channels; however, addressing security issues and establishing pathways to sharing is not enough. Tools, community training programs, and assessment and evaluation of community knowledge sharing processes are necessary for helping users understand *why* information uniquely possessed by one community of interest should be shared with others (Cho et al. 2002). Research in social science suggests that this does not happen naturally because individuals tend to share the information they have in common with others, not knowledge that they know they uniquely possess. Intuitively, this makes sense because people enjoy talking about their likenesses, and often refrain from discussing topics that will be of interest to only a minority of the participants.

Moreover, it has been shown that when collaborators do share their individual expertise in decision making situations, the quality of the overall group decision does not improve (Lave and Wenger 1991) (Mennecke 1997). There are several explanations for this. First, group members tend to rely on common knowledge for their final decisions, even though other knowledge may have surfaced during their interaction. Second, community members must cognitively process and seek to understand the meaning of the information they share, otherwise, even effective information sharing performance will not produce optimal decisions (Mennecke 1997). To this end, members of different communities of interest must be motivated to interpret, understand, and apply knowledge shared in different contexts.

Effective knowledge sharing across communities with different objectives and perspectives means sharing the right information, at the right level of detail, using the right language, at the right time, in the right context, with the right people. A failure related to any one of these factors can lead to a knowledge sharing breakdown. Some social psychology research has identified strategies that might encourage communities to share the information they uniquely possess. Such strategies include helping participants understand the nature and granularity of the knowledge held by each community of interest, and setting up interactive agendas specifically for information sharing so that gaps can be more readily identified. The next section further discusses tools and methodologies for facilitating knowledge sharing and community development

Facilitating knowledge sharing

Facilitating knowledge sharing across communities of interest that do not yet have established processes for information sharing involves creating the infrastructure, mindset, and tools needed to support a new culture of collaboration and sharing. A number of different factors influence community members' participation, involvement, and the eventual success of the collaboration. These include the degree to which users are aware of the various communities, information, and knowledge available in the environment (awareness), the ease of finding useful information in a timely manner (structure), and whether or they perceive an immediate benefit from collaborating with others (motivation).

Awareness

Although effective collaboration does require effective knowledge sharing and an understanding of others' perspectives, a single common operating picture (COP) and set of objectives may not be necessary. Each community of interest might have a different set of objectives, and may still collaborate effectively to share the information that others need, without necessarily aiming to attain the same goals.

Helping communities develop their own awareness and understanding of other communities' knowledge, problems, and goals may very well be one of the most difficult challenges. Rather than forcing users to agree on a common language and perspective, we might want to lean toward supporting awareness, tolerance, and understanding of how different perspectives differ, and meaningful analogies to facilitate this conceptual

translation. Supporting these processes might translate into knowledge seeking and searching tools that attempt to understand the user's core community perspective and guide him toward the most appropriate knowledge sources tailored to his needs. Other awareness tools might help communities frame their knowledge in terms and languages that are most useful to other known communities, developing implicit links between similar concepts and programs. Social awareness and social networking tools would be useful for connecting community members and enabling them to attach meaning to tacit knowledge that was developed in specific contexts.

Structuring and Regulating Collaboration

By connecting communities of interest and providing more information at users' fingertips, we increase the volume of data that a user must search through in order to finding the most relevant information. Guidelines, roadmaps, metadata, structures, and tools for finding relevant information in community-based contexts are essential, and must be constantly updated and maintained.

The moderator role is key, and several may be needed (e.g. at least one from each community). Questions should also be raised regarding the characteristics that are needed for effective moderation of DHS community based knowledge networks. For example, do some moderators need domain knowledge or experience in professional group facilitation? Do others need to personally know the collaborating partners and establish a level of trust with them?

Cross-community discussion groups that are linked to integrated data sources may help to give more context and meaning to the content. For example, users and groups could collaborate in online discussion forums that are directly linked to the imagery and reports they are sharing, commenting and explicitly making linkages (e.g. arrows, highlights) to sections of the shared items being discussed. Rating or voting tools might also help community members determine what information (discussion items, images, etc.) was helpful for what purposes.

Motivation

Communities are motivated to share quality, understandable information with other communities that do the same. The perceived and measured benefit of collaborating is predictive of the level to which community members continue to collaborate with each other over time. For example, Cho et al (2002) studied the online interaction of students using listservs and community discussion boards, and found that less information was shared and processed by the students as the term progressed. Central/prestigious actors shared more information at the beginning of the term, while less central/prestigious (more peripheral) actors were more likely to interact and share knowledge later in the term. This suggests that peripheral actors require time to enter community-based practices, and also makes sense in terms of Lave and Wenger's (1999) legitimate peripheral participation/situated learning theory.

Cho et al.(2002) also found that URLs posted to the class listservs (and consequently emailed to all the participants) were visited significantly ($p = 0.51$) more times than those posted on the discussion boards (in which students needed to access explicitly). The “push” technology was necessary to have the learners fully involved in the community-based activities. This concept may be particularly important for more established community members – the motivation for knowledge discovery may decrease over time as more accomplished members feel more like they already know what they need to know, and the need to use a system to discover things they think they already know decreases.

Assessment and Evaluation

One method for rewarding communities for their sharing efforts is to provide their members with summative feedback about their participation and collaboration. Augmenting participation and activity statistics with suggestions and comments may also help community participants understand what is working, and why or why not. Evaluation and assessment should be done at each phase of development and deployment with a high level of community involvement. For example, each organization should understand what knowledge was shared and how it was used by other organizations.

Annex E DHS Response to OMB Data Call

Bureau/ Office	System Name	Program(s) Supported	Type of Information	Identify Users
BTS	Automated Biometric Identification System [IDENT]	US-VISIT, Border Patrol, ICE Investigations, ICE D & R, Assylum, CBP Inspections	LE	US-VISIT, CBP Border Patrol, ICE Investigations, ICE D & R, Assylum, CBP Inspections
CBP	ACE/International Trade Data System	Facilitate trade	HS	CBP, Trade, Canadian & Mexican Customs..... DOT/FMCSA (ACE Release 4)
CBP	Advance Passenger Information System	Anti-terrorism, anti-drug	HS, LE	
CBP	America's Shield Initiative (formerly ISIS --Integrated Surveillance Info System)		HS, LE	
CBP	Arrival/Departure Information System	US-Visit	HS, LE	
CBP	Automated Commercial Environment	Modernization	HS	All of Customs and Trade community
CBP	Automated Commercial System	Trade Facilitation	HS	Bureau of Census Internal Revenue Service National Finance Center (Agriculture) National Marine Fisheries Service Fish and Wildlife Service Food and Drug Administration Department of Agriculture Department of Commerce Federal Communication Commission Bure
CBP	Automated Export System	Anti-terrorism & Trade facilitation	HS	CBP, Foreign Trade Division of the Bureau of Census (Commerce), the Bureau of Export Administration (Commerce), the Office of Defense Trade Controls (State), other Federal agencies, and the export trade community

CBP	Automated Targeting System	Anti-terrorism, anti-drug, anti-fraud, anti-smuggling	HS	Federal Bureau of Investigations FAST Data Warehouse , e-CAR, LBVTS, TECS -APIS Carrier (Air), Carrier (Passenger)
CBP	Biometric Verification System/Border Crossing Card		HS, LE	
CBP	Non-Immigrant Information Systems	Anti-terrorism, anti-drug	Immigration control, law enforcement (tracking persons arriving in/departing from U.S. as nonimmigrant visitors; assist INS/other government agencies in law enforcement, intelligence, and counter-terrorism activities).	Court, grand jury, administrative/regulatory body; federal, state, local, foreign, tribal agency/organization/task force; Congress; GSA, NARA; news media and public; federal government contractors; former Department employees.
CBP	Private Aircraft Enforcement System	Anti-terrorism, Anti-drug	HS, LE	CBP Inspectors and FAA
CBP	Treasury Enforcement Communications System	Anti-terrorist, anti-drug, US-Visit	Law Enforcement, Inspections, Seizures	National Crime Information Center, US Embassy, US Coast Guard, Federal Bureau of Investigations, Internal Revenue Service, Drug Enforcement Administration, El Paso Intelligence Center, Federal Aviation Administration, Bureau of Alcohol Tobacco and Firearm, Federal, state, local government, intl law enforcement/regulatory agencies, foreign governments, DOD, DOS, Dept of the Treasury, CIA, SSS, USCG, UN, INTERPOL, individuals/organization; attorney/rep of individual covered by system; news media and public; Congress, federal government contractors; former Department employees; parties in litigation; officials/employees of federal agency or entity.

DHS	Civil Rights and Civil Liberties Matters Tracking System	CRCL Equal Employment Opportunity (EEO) and Matters Investigations.	HS, LE	<p>With members of the CRCL staff who are directly responsible for CRCL Matters and EEO activities. With contractors who supplement the CRCL staff. With the DHS Inspector General.</p> <p>Information from the system is currently shared with the following DHS Internal government components: Customs and Border Patrol; the Transportation Security Administration; Immigration and Customs Enforcement; the United States Citizenship and Immigration Service, the United States Coast Guard, Emergency Preparedness and Response and Information Analysis and Infrastructure Protection. Sharing with additional DHS components may occur if and when Matters or EEO complaints are filed involving them.</p>
DHS	Homeland Secure Data Network	All DHS programs with collateral SECRET communications requirements	(LE, HS, MIL, INTEL) HSDN is a transport mechanism and will not own any of the data that is carried by it. That said, the program fully expects that law enforcement, homeland security, military and intel information will all be carried on it (with the predominant traffic being homeland security and law enforcement).	HSDN is a transport mechanism. The only person-identifiable data it will own will relate to holders of user accounts. (And) HSDN is, by its nature, a mechanism to share information. As noted previously, though, HSDN provides the transport and application services only, and is not a data owner.

IAIP	CERT - Vulnerability Research and Incident Identification	US-CERT	Homeland security (HS)	Other bureaus within agency with proper need to know
IAIP	Constellation - Automated Critical Asset Management System		Law Enforcement (LE) Homeland Security (HS)	Law Enforcement and first responders

IAIP	Critical infrastructure Warning Information Network (CWIN)	CWIN supports DHS as a whole and specifically the HSOC, HSIN, and JRIES. CWIN also directly supports the States' Homeland Security Advisors (HAS) and the States' Emergency Operations Centers (EOC)	homeland security (HS)	Dept. of Treasury, Financial Services ISAC, Internal Revenue Service, Federal Reserve Board, Chemical ISAC, Environmental Protection Agency, MWEAC, National Communications System COOP, White House Sit Rm, Multi-State ISAC, DHS Homeland Security Operations Center, Office of Management and Budget, Department of Defense (G Root), Boeing, Department of Veterans Affairs, Lockheed Martin, Northrop Grumman, Joint Task Force-Global Network Operations, Defense Information Systems Agency GNOSC, Army Research Lab (H Root), Federal Emergency Management Agency, Department of Energy, Electric ISAC, Oil & Gas ISAC, Akami, AOL, Arrowhead, Avici, Computer Emergency Response Team Coordination Center, Cisco, Cogent Communications, Computer Associates, Earthlink, EDS, Equinix, SysAdmin, Audit, Network, Security (SANS), Computer Sciences Corporation (CSC), ICANN (L-Root), Internet Security Services (ISS), Information Technology ISAC, ISC(F Root), Juniper Networks, Level3, Lucent, Microsoft, NASA (E Root), Nortel Networks, Sun Microsystems, Symantec, UMD (D Root), VeriSign (A&J Root), White House CIO, Assoc. of State Dam Safety Officials, Nuclear Regulatory Commission (NRC), CDC, AT&T, BellSouth, MCI, Telecom ISAC, Qwest, SBC, Sprint, Verizon, FCC, Department of Transportation, Surface Transportation ISAC, FAA CSIRC, Water ISAC & 50 states and the District of Columbia
IAIP	DHS Extended Briefing System	Information Analysis	INTEL	Federal Agency, DHS Federal Agency, DOJ NCTC

IAIP	Homeland Security Information Network	Homeland Security Operations Center	Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES), For Official Use Only (FOUO), HSIN-Secret, to select users)	IA, IP, HSOC, Federal, State and Local Law Enforcement, Other Federal, State, Local, Tribal Agencies, Critical Sectors, Private Sectors
IAIP	IA-R Contact DB	Information Analysis	INTEL	Federal Agency, DHS
IAIP	iMap Data	Operational support to IAIP	Homeland security (HS)	another bureau within agency with proper need to know
IAIP	Information and Intelligence Fusion (I2F)	Information Analysis	INTEL	Federal Agency, DHS Federal Agency, CIA Federal Agency, DOJ Federal Agency, DOD NCTC
IAIP	Infrastructure Critical Asset Viewer (iCAV)	Operational support to IAIP	Homeland security (HS) Infrastructure and Key Resource Geospatial Data and Information.	Users supporting operational, situational, and strategic awareness of the nation's infrastructure. Also users supporting geospatial-intelligence analysis, infrastructure analysis, and threat analysis. iCAV will align with and interface with the NADB, NTIDB, HSIN/JRIES GIS Portal, and DoD/NGA's Palanterra.
IAIP	National Asset Database	Operational support to IAIP	Homeland security (HS)	will be another bureau within agency with proper need to know
IAIP	National Threat and Incident Data Base	Information Analysis	INTEL	Federal Agency, DHS
IAIP	Pantheon	Information Analysis	INTEL	Federal Agency, DOD
IAIP	Prizm Infrastructure Assessment Tool	Operational support to the National Infrastructure Coordination Center (NICC)	Homeland Security (HS)	
IAIP	Protected Critical Infrastructure Information		Homeland security (HS)	
IAIP	Protective Security Advisors (VPN)	Operational support to IAIP	Homeland security (HS)	

IAIP	PSD - Chemical Site Monitoring Via Web Cameras	Operational support to IAIP	Homeland security (HS)	will be another bureau within agency with proper need to know
ICE	Consolidated Enforcement Environment	ICE, CBP, CIS, DOJ, DOS, FAA, DOC, Treas, Canadians, Interpol, OAG, ACE, US VISIT, HSDN, ISIS, emerge2, JRIES, IAIP, Targeting and Selectivity, TSA, USSS, USCG, FEMA	LE, INTEL, & HS	ICE, CBP, CIS, DOJ, DOS, FAA, DOC, Treas, Canadians, Interpol, OAG, ACE, US VISIT, HSDN, ISIS, emerge2, JRIES, IAIP, Targeting and Selectivity, TSA, USSS, USCG, FEMA
ICE	Criminal Alien Investigation System (CAIS)	ICE	LE	DRO IRP Officers, Clerks, and Supervisors; Enforcement Apprehension Booking Module (EABM).
ICE	Data Analysis for Trade Transparency (DARTT) System	ICE Investigations - Trade Transparency Unit	LE	ICE, DOS, DOT
ICE	Deportable Alien Control System (DACs)	ICE & CBP	LE	ICE, CIS, CBP, DOJ, FBI
ICE	Enforcement Case Tracking System (ENFORCE) Apprehension Booking Module (EABM)	ICE & CBP	LE, INTEL	IAFIS Automated Biometric Identification System (IDENT); Deportable Alien Control System (DACs) DHS/ICE/CBP/Inspections/Office of Investigations
ICE	Enforcement Removal Module (EREM)	ICE	LE	ICE, CIS, CBP, DOJ, FBI
ICE	General Counsel Management Systems (GEMS)	ICE / OPLA	LE	Attorneys and support staff involved in the Deportation/Removal process
ICE	ICE International Affairs Foreign Office Infrastructure Upgrades	ENFORCE, TECS, SEACATS	LE	ICE Special Agents assigned to selected DHS foreign offices
ICE	Immigration & Customs Enforcement Pattern Analysis & Information Collection Tool (ICEPIC)	ICE OI & INTEL	LE	ICE, CBP, DOJ, FBI, DOS
ICE	Lead Trac	ICE Investigations - Compliance Enforcement Unit	LE	Compliance Enforcement Unit personnel
ICE	NETLEADS®, includes Anti-Drug (ADNETLEADS) and Secret (SIPRNETLEADS)	Investigations, Intelligence	INTEL,HS	ICE, CBP, DHS, DOJ, FBI, DOS, DOD and classified use

ICE	Numerically Integrated Processing System (NIPS)	ICE Intelligence & Investigations	LE & INTEL	Federal agency, DHS-wide
ICE	Student and Exchange Visitor Information System (SEVIS)	SEVIS supports the ICE - Student and Exchange Visitor Program Office (SEVP)	LE	There are different types of users - depending upon needs of system. SEVIS users are: DHS - ICE/SEVP, ICE officers, CBP Officers at POEs, CIS-adjudicators in District Offices; FBI analysts; Dept. of State users - Consular Affairs; Primary/Designated School Officials at schools, universities, etc. and Alternate/Responsible Officers at exchange programs. SEVIS use was mandated as of Jan. 31, 2003, and for all initial and continuing students, SEVIS use was mandated as of August 2003; therefore, users are increasing daily.
ICE	Telecommunications Linking System (TLS)	ICE Criminal Investigations	LE	ICE -- Office of Investigations; ICE -- Office of Professional Responsibility; ICE -- Office of Intelligence; Drug Enforcement Administration
ICE	WinForce Software	ICE Investigations - Financial	LE	ICE, DOJ, AUSA
ICE	Worksite Enforcement Activity Reporting System (LYNX)	ICE Investigations	LE	ICE Investigations
ICE & CBP	Enforcement Integrated Database (EID)	ICE & CBP	INTEL,HS	CBP, Inspections, ICE - Office of Investigations, DHS-Intelligence group, Customs officers.
ICE/FAMS	Surveillance Detection System (SDS)	ICE FAMS	HS	FAMS
ICE/FPS	FPS WebRMS, Records Management System	Intel, Law Enforcement, Physical Security,	LE	ICE - FPS
ICE/FPS	FPS-Secure Portal	Intel, Law Enforcement, Physical Security,	LE	ICE - FPS
ODP	Terrorism Knowledge Base (http://www.tkb.org/Home.jsp)		HS	
S&T	Threat Vulnerability Mapper	Office of Information Analysis Strategic Operations	HS	DHS IAIP/OIA

S & T	Biowatch	NBACC National Bio- Forensics Analysis Center	HS	Homeland and National Security Communities
S & T	BioKnowledge Center	NBACC National Bio- Forensics Analysis Center	HS	DHS, FBI, IC, National Laboratories, DHS Centers of Excellence, HHS
TSA / TSOC	Crisis Management and Event Tracking	TSA Aviation Security and Intermodal Programs	HS, INTEL and LE	Department of Homeland Security
TSA / TSOC	TSOC Crisis Information Management System / WebEOC	TSA Aviation Security and Intermodal Programs	HS, INTEL and LE	Department of Homeland Security
TSA/Transportation Security Intelligence Service (TSIS)	TINMAN (Network)	Internal intelligence databases and JWICS connectivity	INTEL, HS, LE	FBI, DHS, NSA, CIA, FAA, FAMS, STATE
TSA/Transportation Security Intelligence Service (TSIS)	TINSEL (Network)	Internal intelligence databases, SIPRNet connectivity, and organizational messaging (Automated Message handling System-AMHS)	INTEL, HS, LE	FBI, DHS, NSA, CIA, FAA, FAMS, STATE
TSA/Transportation Security Intelligence Service (TSIS)	TRACE (Network)	Standalone classified network	INTEL, HS, LE	DHS, FAM
USCG	Coast Guard Data Network Plus	USCG Missions	MIL, LE, HS	Special liaison connections such as HSOC watchstanders, White House liaison, Hill liaison.
USCG	Defense Message System	USCG Missions	MIL, INTEL, LE, HS	All DOD services, Civilian Agencies with trusted SIPRNET DMS gateways (e.g. State, DEA, DHS)
USCG	Joint Maritime Information Element/Maritime Awareness Global Network	USCG Missions	INTEL, MIL, HS, LE	Other. Federal intelligence and national security agencies; federal and state numbering/titling officials, departments of labor, and transportation safety agencies; foreign entities; federal, state, and local law enforcement; entities in a formal relationship with the USCG.
USCG	Marine Information for Safety & Law Enforcement	USCG Missions	LE, HS, MIL	ICE, TSA, CBP, DHS

USCG	Merchant Mariner Licensing and Documentation System	USCG Missions	HS, LE	Coast Guard personnel, other federal and state government agencies, Financial institutions, other moneylenders and other persons with an interest in a vessel.
USCG	Nationwide Automatic Identification System (NAIS) for MDA . (formerly "National Automatic Identification System")	USCG Missions	HS	Ships, Shippers, Carriers, Worldwide Public
USCG	Port and Waterways Safety System	USCG Missions	HS	Authorized state/local entities in the port area
USCG	Ship Arrival and Notification System	CBP ACE, USCG Missions	HS, LE	CBP, DHC. Other.
USSS	Forensic Information System for Handwriting	Secret Service Protective Mission, Secret Service Investigative Mission	LE	USSS
USSS	Protective Research Information System Management	Secret Service Protective Mission	INTEL	USSS
	1. Data cells left blank indicate data could not be developed in the time available			
	2. Budget figures are in million dollars			
	3. "Type of information" codes: LE = Law Enforcement; HS = homeland-security; INTELL = intelligence; MIL = military			
	DATE PREPARED: 8 April 2005			
	Submitted by: Department of Homeland Security			
	Contact: DHS Office of the CIO			

REPORT DOCUMENTATION PAGE

*Form Approved
OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY) June 2005		2. REPORT TYPE Study		3. DATES COVERED (From – To)	
4. TITLE AND SUBTITLE Information Sharing and Collaboration Business Plan				5a. CONTRACT NUMBER DASW01-04-C-0003/W74V8H-05-C-0042	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBERS	
6. AUTHOR(S) Peter A. Kind, J. Katharine Burton				5d. PROJECT NUMBER	
				5e. TASK NUMBER ER-5-2370	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882				8. PERFORMING ORGANIZATION REPORT NUMBER IDA Document D-3206	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Department of Homeland Security 245 Murrury Lane, Bldg. 410 Washington, DC 20233				10. SPONSOR'S / MONITOR'S ACRONYM DHS	
				11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; unlimited distribution: 7 March 2005.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT IDA developed a draft Business Plan that addresses Information Sharing Vision, the "As-Is" status and analysis, the "To-Be" (desire end state) and an implementation plan (road map) including recommended near, mid and long term actions. Key concepts addressed include in depth development of advanced collaboration capabilities, inter-agency and coalition Information Sharing and Collaboration (ISC), detailed capability requirements, and requirements. Also, principal issues in governance, standards and policy, cultural resistance, resources, access and dissemination control, collaboration and architecture. A new Capability Maturity Model for ISC and an extensive ISC glossary are included.					
15. SUBJECT TERMS Information Sharing and Collaboration (ISC), Business Plan, Information Sharing Vision, Capability Maturity Model.					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mr. Richard Russell
Unclassified	Unclassified	Unclassified	Unlimited	199	19b. TELEPHONE NUMBER (Include Area Code) (202) 282-9415