



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Understand Data Flows Capability

Version 1.1.1

Understand Data Flows is the identification and articulation of how the data supports the missions, including identification of the source, destination, and path of the data. It is essential to understand what types of data are being transmitted, processed, or stored and who the end user is of the data. The knowledge provided by Understand Data Flows is important in establishing security policy and protecting data.

07/30/2012



CGS Understand Data Flows Capability



Version 1.1.1

Table of Contents

1	Revisions	2
2	Capability Definition	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions	5
5	Capability Post-Conditions.....	5
6	Organizational Implementation Considerations	5
7	Capability Interrelationships.....	6
7.1	Required Interrelationships	7
7.2	Core Interrelationships	7
7.3	Supporting Interrelationships.....	8
8	Security Controls	8
9	Directives, Policies, and Standards	10
10	Cost Considerations	12
11	Guidance Statements.....	13



CGS Understand Data Flows Capability



Version 1.1.1

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1



CGS Understand Data Flows Capability



Version 1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Understand Data Flows is the identification and articulation of how the data supports the missions, including identification of the source, destination, and path of the data. It is essential to understand what types of data are being transmitted, processed, or stored and who the end user is of the data. The knowledge provided by Understand Data Flows is important in establishing security policy and protecting data.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Any type of data flow can change the risk posture of the Enterprise. The Understand Data Flows Capability shall enable other capabilities to make informed mission assurance decisions by enabling them to understand the flow of data across the network. For example, the Incident Response and Risk Analysis Capabilities will use the documented information to determine how to respond or what the risk is to the security posture of the environment.

To provide mission assurance, it is important to understand and document the end-to-end path(s) that data may follow. The Understand Data Flows Capability shall provide insight into the physical and environmental factors, communication mediums, and users, which are necessary to define the protection requirements for the data flows. In addition to protection requirements, knowledge of the data path is important and shall be useful for planning contingencies. For example, Understand Data Flows shall provide information about the data to make rerouting decisions in the event that a flow is no longer available or there is a mission or constraint change.

The Enterprise shall establish trust relationships through the Network Boundaries and Interfaces, Network Boundary Protection, and Network Mapping Capabilities to



CGS Understand Data Flows Capability



Version 1.1.1

understand the full path of a data flow(s). These trust relationships shall be used to determine the risk posture for the specific data flows within the Enterprise. The Capability shall provide the Enterprise officials and authorities with the knowledge to determine data protection needs.

The Understand Data Flows Capability shall provide information about data flows associated with the Enterprise, such as bandwidth, throughput, mission priority, content, type, and routing paths. The Enterprise shall decide which factors to provide information on based on the attributes of the data flow. Information shall be shared with the Utilization and Performance Management Capability so that it can perform analysis against the defined baseline.

The Understand Data Flows Capability shall monitor network activity in coordination with other Capabilities, such as Network Enterprise Monitoring and Utilization and Performance Management, to examine the data flows. Monitoring data flows shall be useful for detecting and investigating data flows that do not align with the mission flows.

The Understand Data Flows Capability shall evaluate two types of data flows: 1) data flows that directly support the mission of the Enterprise and 2) data flows that provide the overhead support to the Enterprise. The evaluation of two data flow types is necessary to observe modifications in the system processing, even if the mission does not change. Understand Data Flows uses data flow trending information, which is provided from Network Enterprise Monitoring and Utilization and Performance Management, in conjunction with information captured by the Capability to anticipate emerging data flow problems. In addition, data flows shall be characterized by trend data (e.g., volume of data) passing through pathways over time.

The Understand Data Flows Capability shall assess the data flows within the Enterprise so that the Enterprise can evaluate the impact and security considerations of establishing additional data flows, in conjunction with the Utilization and Performance Management Capability. The Understand Data Flows Capability shall know the access control decisions that have been made by officials to ensure data flows are established in accordance with access control.

Data flows shall be reevaluated based on changes in the mission, consumer need changes, and system design changes. The Enterprise shall define periodic reevaluation in accordance with the Enterprise's policy and procedures to ensure that all data flows are known to the Enterprise authorities.



CGS Understand Data Flows Capability



Version 1.1.1

The Enterprise shall document all of its mission supporting data flows. Data flows shall be documented to correlate with the related mission flows. Documented information shall include source, destination, data type, and full path of the data flow. The documents and reports of data flows shall be stored in an intermediate repository, which shall be in standard format to trace back to the source of data that relates to the mission asset(s) and then shared with Enterprise authorities for a top-down analysis for determining the source of data.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Data flows and mission flows can have a one-to-many correlation.
2. Accurate network maps exist.
3. Network boundary and interfaces are known and documented.
4. An accurate mission map exists.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability is able to identify and document data flows entering and leaving the Enterprise.
2. The Capability is able to identify and document critical data flows inside the Enterprise.
3. The Capability supports mission assurance decisions.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).



CGS Understand Data Flows Capability



Version 1.1.1

When Understand Data Flows is employed correctly, the Organization will possess the ability to understand and protect data flows for the environmental elements and technologies. This ability to understand and protect data flows will align with the mission assurance needs.

An Organization will characterize data flows based on the data volume (e.g., bandwidth, throughput, mission priority, content, type, and routing path) that is monitored and documented. This information will ensure the Organization's officials and authorities are able to determine a baseline for data protection needs.

An Organization will need to coordinate with other Capabilities once data flows are established. An Organization will make this Capability responsible for documenting data flows along with the missions they support (as provided by Understand Mission Flows) and will monitor their data flow network activity (see Capability Interrelationships). Reports about network activity related to data flows generated by those Capabilities will assist in monitoring the operational status of data and aid in future decisions regarding mission sustainment and realignment of data flows.

An Organization will document and report data flows to determine the source of the data. An Organization will make the processed information available via aggregation, storage, standard format, and analysis to minimize redundancy and keep a record of traceability to the data source.

An Organization will leverage the Understand Data Flows Capability to make decisions in other Capabilities, such as Utilization and Performance Management to manage quality of service and make load balancing decisions. For example, some applications have stricter latency requirements than others, such as Voice over Internet Protocol (VoIP). By identifying the latency requirements of each type of traffic, latency sensitive packets can be prioritized over ones that are not. For load balancing, if periods of heavy traffic lead to bottlenecks on a network with redundant links, the knowledge of the traffic source, destination, and path can be used to reroute traffic over different links and make more efficient use of the available bandwidth.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary



CGS Understand Data Flows Capability



Version 1.1.1

relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping—The Understand Data Flows relies on the Network Mapping Capability to provide a visualization of the network components so they can all be related to data flows.
- Network Boundary and Interfaces—The Understand Data Flows Capability relies on the Network Boundary and Interfaces Capability to provide information about the Enterprise network boundaries and interfaces (e.g., internal, external, physical, logical).
- Understand Mission Flows—The Understand Data Flows Capability relies on the Understand Mission Flows Capability to provide mission maps and mission requirements of the data flows.
- Hardware Device Inventory—The Understand Data Flows Capability relies on the Hardware Device Inventory Capability to provide information used to better understand hardware-generated data flows.
- Software Inventory—The Understand Data Flows Capability relies on the Software Inventory Capability to provide information used to better understand software-generated data flows.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management—The Understand Data Flows Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards—The Understand Data Flows Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness—The Understand Data Flows Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.



CGS Understand Data Flows Capability



Version 1.1.1

- IA Training–The Understand Data Flows Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Understand Data Flows Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Network Security Evaluations–The Understand Data Flows Capability relies on the Network Security Evaluations Capability to provide information that is used to fill any gaps that may have been overlooked when enumerating data flows.
- Risk Mitigation–The Understand Data Flows Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	
CM-2 <i>BASELINE CONFIGURATION</i>	Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Enhancement/s: (1) The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades. (2) The organization employs automated mechanisms to



CGS Understand Data Flows Capability



Version 1.1.1

	<p>maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.</p>
<p>PL-2 SYSTEM SECURITY PLAN</p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Develops a security plan for the information system that: <ul style="list-style-type: none"> - Is consistent with the organization’s enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [Assignment: organization-defined frequency]; <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The organization: <ul style="list-style-type: none"> (a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and (b) Reviews and updates the CONOPS [Assignment: organization-defined frequency]. <p>Enhancement Supplemental Guidance: The security CONOPS may be included in the security plan for the information system.</p> <ul style="list-style-type: none"> (2) The organization develops a functional architecture for the information system that identifies and maintains: <ul style="list-style-type: none"> (d) Types of information processed, stored, or transmitted by



CGS Understand Data Flows Capability



Version 1.1.1

	the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and (e) Restoration priority of information or information system services.
--	--

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Understand Data Flows Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDI 8410.02 NetOps for the Global Information Grid (GIG), 19 December 2008, Unclassified	Summary: This instruction identifies a purpose: "Establishes policy and assigns responsibilities for implementing and executing NetOps, the DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG." It sets policy, "4. d. As information systems capabilities mature, they shall be capable of reporting their system status to include fault, configuration, performance, and security to facilitate GIG health and mission readiness assessments. 4. f. A common set of NetOps mission-driven metrics, measurements, and reporting criteria shall be used to assess GIG operating performance and to determine the



CGS Understand Data Flows Capability



Version 1.1.1

	mission impact of service degradations or outages.”
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Understand Data Flows Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February	Summary: This special publication (SP) provides the following information: (i) defining the core missions and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations); (ii) prioritizing missions and business processes with respect to the goals



CGS Understand Data Flows Capability



Version 1.1.1

2010, Unclassified	and objectives of the organization; (iii) defining the types of information that the organization needs to successfully execute the stated missions and business processes and the information flows or data flow both internal and external to the organization; (iv) developing an organization-wide information protection strategy and incorporating high-level information security requirements into the core missions and business processes.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:



CGS Understand Data Flows Capability



Version 1.1.1

1. Number of data flows—As the number of data flows to monitor increases so will the cost of monitoring those data flows.
2. Data flows incompatibility—The Enterprise will need to prioritize data and flows when data flows are incompatible.
3. Scope of work—The number of devices and breadth of hardware/software will contribute to the complexity of understanding data flows.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Understand Data Flows Capability.

- The Enterprise shall identify and articulate how the data supports the missions, including identification of the source, destination, and path of the data and understand what types of data are being transmitted, processed, or stored and who is the end user of the data.
- The Enterprise shall make informed mission assurance decisions by understanding the flow of data across the network.
- The Enterprise shall provide insight into the physical and environmental factors, communication mediums, and users that are necessary to define the protection requirements for the data flows.
- The Enterprise shall provide information regarding data paths of the network for planning contingencies. For example, the Enterprise shall provide information about the data to make rerouting decisions in the event that a flow is no longer available or there is a mission or constraint change.
- The Enterprise shall establish trust relationships through other systems to understand the full path of a data flow and use these relationships to determine the risk posture for the specific data flows within the Enterprise.
- The Enterprise shall provide information to Enterprise officials and authorities to determine data protection needs.
- The Enterprise shall provide information about data flows associated with the Enterprise, such as bandwidth, throughput, mission priority, content, type, and routing paths. The Enterprise shall decide which factors to provide information on based on the attributes of the data flow.



CGS Understand Data Flows Capability



Version 1.1.1

- The Enterprise shall monitor network activity in coordination with other systems to examine the data flows to detect and investigate data flows that do not align with the mission flows.
- The Enterprise shall evaluate data flows that directly support the mission of the Enterprise, and data flows that provide the overhead support to the Enterprise to observe modifications in the system processing, even if the mission does not change.
- Data flows shall be characterized by trend data (e.g., volume of data) passing through pathways over time.
- The Enterprise shall evaluate, in conjunction with other systems within the Enterprise, the impact and security considerations of establishing additional data flows.
- The Enterprise shall be provided with access control information that has been decided by officials to ensure data flows are established in accordance with access control.
- Data flows shall be reevaluated based on mission changes, consumer need changes, and system design changes. These reevaluations shall occur in concurrence with Enterprise changes.
- The Enterprise shall document all of its mission supporting data flows.
- Documented information on the data flows shall include source, destination, data type, and full path of the data flow.
- The documents and reports of data flows shall be stored in an intermediate repository.
- The Enterprise documents and reports of data flows shall be in standard format to trace back to the source of data that relates to the mission asset.
- The Enterprise documents and reports shall be shared with Enterprise authorities for a top-down analysis for determining the source of data.