



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Organizations and Authorities Capability

Version 1.1.1

The Organizations and Authorities Capability encompasses the definition, establishment, governance, and revocation of information assurance (IA) roles and responsibilities within the Enterprise and provides for their continued authorization. The Organizations and Authorities Capability also provides accountability for reporting and performing roles, defining Organizations, and making decisions. In addition, Organizations and Authorities facilitate the collaboration and coordination of operations across different authorities and organizational boundaries.

07/30/2012



CGS Organizations and Authorities 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	6
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations	6
7	Capability Interrelationships.....	8
7.1	Required Interrelationships	8
7.2	Core Interrelationships	8
7.3	Supporting Interrelationships.....	9
8	Security Controls	9
9	Directives, Policies, and Standards	10
10	Cost Considerations	14
11	Guidance Statements.....	15



CGS Organizations and Authorities 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 Organizations and Authorities 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.

The Organizations and Authorities Capability encompasses the definition, establishment, governance, and revocation of information assurance (IA) roles and responsibilities within the Enterprise and provides for their continued authorization. These roles and responsibilities include personnel, physical, environmental, and technology considerations. Roles are responsible for executing and enforcing the IA vision of the Organization and ensuring that the definition and execution of projects and programs are aligned with the Community Gold Standard (CGS) Framework.

The Organizations and Authorities Capability also provides accountability for reporting and performing roles, defining Organizations, and making decisions. In addition, Organizations and Authorities facilitate the collaboration and coordination of operations across different authorities and organizational boundaries.

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.

The Organizations and Authorities Capability has two primary goals: 1) establishing the Enterprise’s internal roles and authorities related to IA and 2) facilitating the goal of federated, Community-wide coordination of IA processes, which cross Enterprise boundaries. To reach these goals, the Capability shall establish roles and authorities in accordance with existing Enterprise IA Policies, Procedures, and Standards.

The Organizations and Authorities Capability shall define and document all roles and authorities along with their assigned responsibilities. Documentation shall include explicit statements detailing the scope, boundaries, and operation for that role or authority and the justification for its creation. Clearly defining each role and its responsibilities enables individuals executing the role to support the mission and



CGS Organizations and Authorities Capability



Version 1.1.1

perform their duties correctly. Both roles and authorities need to be specific enough to fit the environment and dynamic enough to handle any reasonable change that may occur.

The Organizations and Authorities Capability shall mandate that all personnel go through a training program specific to their role or authority, as provided by the IA Training Capability, to ensure that they have the necessary knowledge to perform their duties. Personnel shall be trained to understand the proper scope of their role and responsibilities. When an issue arises that is outside the scope of their role, personnel shall seek proper guidance and expertise from an appropriate authority or management to solve the issue rather than taking on responsibilities that may be unnecessary, unauthorized, or undefined. Support from management shall be consistently made available to subordinates and shall be used to resolve Enterprise issues.

The Organizations and Authorities Capability functions shall consider all Capabilities defined within the CGS Framework. The roles and authorities defined by the Organizations and Authorities Capability shall be tailored for each Enterprise that is implementing the CGS based on its individual mission, environment, and operational needs. Decisions made by the Organizations and Authorities Capability about the roles and authorities internal to the Enterprise shall be made with an understanding and consideration of the goal for federated coordination across Enterprise boundaries.

The Organizations and Authorities Capability shall examine the Enterprise's hierarchical decision-making needs and the needs of the programs that execute within the Enterprise. Based on this information, the Capability shall assign responsibilities and authorities to roles to fulfill all of the required needs. The information used to make these assignment decisions shall be vetted within the Enterprise to ensure accuracy. In addition, the Organizations and Authorities Capability shall ensure that roles, Enterprises, and personnel have been assigned authority over their domain. Authorities shall be defined and supported by senior officials or executive management to ensure that their authority is recognized and enforced. Without adequate authority, necessary tasks may not be completed, which could cause excess risk to the Enterprise.

The roles established by the Organizations and Authorities Capability shall provide separation of responsibility and authority, as determined by IA Policies, Procedures, and Standards. This separation is to prevent conflicts of interest and to provide management and compliance checks. In addition to establishing new roles, the Capability shall review existing roles and authorities to determine what needs exist for supervision and how extensive those needs may be. Existing roles shall be changed accordingly to provide a



CGS Organizations and Authorities Capability



Version 1.1.1

sufficient amount of supervision without degrading the mission. Supervision is also a way to enforce accountability. Accountability shall be enforced at all levels of the Enterprise because IA responsibilities encompass every person in the Enterprise. Enforcement shall take the form of consequences for not having a role or authority defined or for not measuring the effectiveness of a role. Based on the determined supervision needs, the Capability shall define verification and validation mechanisms to enforce the necessary supervision and measure its effectiveness.

The Organizations and Authorities capability shall establish procedures for the revocation of roles, responsibilities, or authorities. Revocation can occur for a variety of reasons, and procedures shall be in place for each likely eventuality. Some of the reasons for revocation can include a reorganization of responsibilities among different roles or functional positions being created, adjusted, or eliminated.

The Organizations and Authorities Capability shall establish a centralized awareness of the Enterprise's roles and authorities, which encompasses all technical, personnel, physical, and environmental factors. Centralized awareness facilitates the goal of shared responsibility between cooperating roles and responsibilities in execution of the Enterprise's functions. For example, system owners and data owners may be independent of each other but need to work together to achieve their mission objectives. In addition, coordination between differing functional roles requires a comprehensive understanding of how mission flows and data flows interoperate. This Capability cooperates with the Understand Mission Flows and Understand Data Flows Capabilities to collect this information.

The governance established by the Organizations and Authorities Capability specifies the coordinated authorities for federated operations that cross Enterprise boundaries. These coordinated authorities span all agency, partner, and contractor capabilities that operate within the Enterprise, minimizing unacknowledged risks. The Organizations and Authorities Capability considers the broader Enterprise requirements when making changes within a program to ensure that the Enterprise vision and scope are properly accounted for. In addition, as part of the Organizations and Authorities Capability, the reporting requirements and mechanisms for each Organization or authority need to be clearly defined.



CGS Organizations and Authorities Capability



Version 1.1.1

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. The budget is allocated and available to establish the necessary roles and Organizations.
2. Policy exists that defines the need for the designated roles and Organizations.
3. An analysis of the CGS has occurred and will be used to determine the necessary roles.

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 makes sure reporting requirements and mechanisms are clearly defined.
2. For each CGS Capability implemented within the Enterprise, the roles have been defined to include the authority, responsibility, and accountability.
3. The overseeing Organization mandates and ensures compliance with appropriate IA standards.

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).

The Organization will decide how to implement the CGS across its Enterprise prior to being able to implement the Organizations and Authorities Capability. Based on this decision, implementation of the Organizations and Authorities Capability will establish the necessary roles and authorities required by the other CGS Capabilities to fulfill their functions. These roles will be assigned the responsibilities that are relevant to their functional tasks. Each role will be assigned the appropriate level of authority necessary to perform its mission objectives. Roles will be thoroughly documented at the time of their creation with specifications of their scope, boundaries, and operation and the



CGS Organizations and Authorities Capability



Version 1.1.1

justification for their existence. This documentation and any reports that may be required will be stored so they are available for future reference. Roles, responsibilities, and authorities will be revoked when they are no longer necessary. The Organization will establish a centralized mechanism by which to build awareness of roles and authorities. This centralized mechanism will enable cooperation among the various functional roles.

The Organization will collect information about mission and organizational needs prior to defining roles, responsibilities, and authorities. Mission and operational needs are the basis for defining these items. A proper understanding of these needs is critical to defining roles properly. Therefore, to effectively implement Organizations and Authorities, the Organization will define and use a vetting process to ensure that it has an accurate understanding of its needs before defining any roles, responsibilities, and authorities.

The Organization will design roles and authorities using a separation of responsibility so that they provide oversight for each other. Oversight is critical to IA because it prevents an individual or group of individuals from performing unauthorized or unintentional actions without being detected or given special authorization. Different roles and responsibilities require different levels of oversight, which is accounted for during role creation. If these requirements change over time, the definition and scope of roles will be adjusted by the Organization as necessary to ensure a sufficient level of oversight. In addition to oversight measures, the Organization will establish a mechanism by which to verify whether roles are being executed as they are intended. This will be accomplished by the built-in oversight measures, but these measures may not be effective. To ensure that roles are functioning as intended and are not being abused, the Organization will use a verification process that is separate from the oversight mechanisms. This verification process will assess operations and make recommendations about any changes that may need to occur. For example:

- A role may require additional oversight to ensure compliance with its scope.
- The scope of the role may need to change because of changes in the mission or environment.
- The scope of a role may need to change because the original scope was unrealistic.

The Organization will create roles that are specific to its own functional needs. One example of a role the Organization will establish is that of a Program Manager (PM). One part of a PM's job will be to ensure that programs are managed in accordance with



CGS Organizations and Authorities Capability



Version 1.1.1

the policies established in the IA Policies, Procedures, and Standards capability and are able to meet established objectives. Another example of a role the Organization will create is that of Systems Security Engineers (SSE). SSEs will be responsible for designing systems that satisfy all security policies required for operational use.

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 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.

- Understand Mission Flows—The Organizations and Authorities Capability relies on the Understand Mission Flows Capability to provide information about the flow of missions so that roles and authorities for the Enterprise can be effectively defined.
- Understand Data Flows—The Organizations and Authorities Capability relies on the Understand Data Flows Capability to provide information about the flow of data so that roles and authorities for the Enterprise can be effectively defined.
- Finance—The Organizations and Authorities Capability relies on the Finance Capability to ensure that the roles and authorities created for the Enterprise are appropriately budgeted for and that any necessary changes to those roles and authorities are also included in the budget.

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 Organizations and Authorities 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 Organizations and Authorities 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.



CGS Organizations and Authorities Capability



Version 1.1.1

- IA Awareness–The Organizations and Authorities Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Organizations and Authorities Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.

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.

- Risk Monitoring–The Organizations and Authorities Capability relies on the Risk Monitoring Capability to provide feedback on the effectiveness of roles and responsibilities defined for the Enterprise.

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>	
AC-5 SEPARATION OF DUTIES	Control: The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion; b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations. Enhancement/s: None Specified.
CM-9 CONFIGURATION MANAGEMENT PLAN	Control: The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; Enhancement/s: (1) The organization assigns responsibility for developing the



CGS Organizations and Authorities Capability



Version 1.1.1

	configuration management process to organizational personnel that are not directly involved in system development.
PM-2 <i>SENIOR INFORMATION SECURITY OFFICER</i>	Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. Enhancement/s: None Specified.
PM-10 <i>SECURITY AUTHORIZATION PROCESS</i>	Control: The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program. Enhancement/s: None Specified.
PS-8 <i>PERSONNEL SANCTIONS</i>	Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. Enhancement/s: None Specified.

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.

Organizations and Authorities Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 1, Policy Directive for Intelligence Community Leadership, 1 May 2006, Unclassified	Summary: This capstone Intelligence Community (IC) Directive (ICD) sets forth the overarching policy and framework for the Director of National Intelligence's (DNI) approach to national intelligence and delineates authorities and responsibilities of the DNI and the Office of the DNI.
ICD 500 Director of National Intelligence,	Summary: This directive establishes the roles and responsibilities of the Associate Director of National



CGS Organizations and Authorities Capability



Version 1.1.1

Chief Information Officer, August 2008, Unclassified	Intelligence (ADNI)/Chief Information Officer (CIO).
ICD 503 IC Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008, Unclassified	Summary: This policy implements strategic goals agreed upon in January 2007 by the IC CIO, the Chief Information Officers of the Department of Defense (DoD), the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). This ICD focuses on a more holistic and strategic process for the risk management of information technology (IT) systems, and on processes and procedures designed to develop trust across the IC IT Enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.
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)	
DoDD 5144.1 Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, 2 May 2005, Unclassified	Summary: This directive assigns responsibilities, functions, relationships, and authorities to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and network-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; information technology (IT), including National Security Systems (NSS); information resources management (IRM) (as defined by reference (b)); spectrum management; network operations; information systems; information assurance (IA); positioning, navigation, and timing (PNT) policy, including



CGS Organizations and Authorities Capability



Version 1.1.1

	airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters. Pursuant to chapter 113, subchapter III of 40 U.S.C. (reference (j)), the ASD(NII)/DoD CIO has responsibilities for integrating information and related activities and services across the Department. The ASD(NII)/DoD CIO also serves as the DoD Enterprise-level strategist and business advisor from the information, IT, and IRM perspective; Information and IT architect for the DoD enterprise; and, DoD-wide IT and IRM executive.
DoDD 8000.01, Management of DoD Information Enterprise, 10 February 2009, Unclassified	Summary: This directive establishes policy that each DoD component shall have a CIO who reports directly to the head of the component. CIOs may also be designated at subordinate levels, but a reporting mechanism through the component CIO must be maintained to ensure continuity of purpose. This directive goes on to assign responsibilities throughout the DoD.
DoDD 8500.01E Information Assurance, 23 April 2007, Unclassified	Summary: This directive establishes policy and assigns responsibilities under reference (a) to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology and supports the evolution to network-centric warfare.
Committee for National Security Systems (CNSS)	
CNSSD 502 National Directive on Security of National Security Systems, 16 December 2004, Unclassified	Summary: This directive delineates and clarifies objectives, policies, procedures, standards, and terminologies as set forth in the “National Policy for the Security of National Security Telecommunications and Information Systems, (NSD-42)” dated July 5, 1990 (hereinafter referred to as “the national policy”). It established the ASD(NII)/DoD CIO as the committee chair and membership across the Federal Government.
Other Federal (OMB, NIST, ...)	
OMB Circular No. A-130, Management of Federal Information Resources,	Summary: This circular establishes policy applicable to all federal agencies, which states how responsibilities are to be assigned within the agency. Specifically, it shall be



CGS Organizations and Authorities Capability



Version 1.1.1

Unclassified	policy that the head of each agency must have primary responsibility for managing agency information resources; ensuring that the agency implements appropriately all of the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB; and appointing a CIO.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Executive Order 12333, United States Intelligence Activities, 30 July 2008, Unclassified	Summary: This order applies to all Organizations involved in intelligence activities for the United States. Each of these Organizations has a responsibility to work together to share information in a manner consistent with any applicable laws and presidential guidance. The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President regarding intelligence activities. The DNI shall act as the head of the IC. This policy also establishes the responsibilities of each Organization in the IC.
Legislative	
Nothing found	

Organizations and Authorities 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	



CGS Organizations and Authorities Capability



Version 1.1.1

Other Federal (OMB, NIST, ...)	
Nothing found	
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:

1. Lifecycle maintenance—The definitions of roles, responsibilities, and authorities need to be reviewed and updated over time based on changing needs and their varying degrees of effectiveness.
2. Gaining recognition—Authorities need to gain recognition both within the Enterprise and across Enterprise boundaries.



CGS Organizations and Authorities Capability



Version 1.1.1

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 Organizations and Authorities Capability.

- The Enterprise shall define, establish, and provide governance and revocation of IA roles and responsibilities within the Enterprise. These roles and responsibilities include personnel, physical, environmental, and technology considerations.
- The Enterprise shall establish and assign roles, authorities, and responsibilities in accordance with existing Enterprise IA policies, procedures, and standards.
- The Enterprise shall document all of the roles, authorities, and responsibilities within the Enterprise.
- The Enterprise shall provide necessary training to personnel assigned to each role in accordance with their assigned responsibilities.
- The Enterprise shall manage roles and responsibilities such that there is a separation of duties to prevent conflicts of interest.
- The Enterprise shall review existing roles and authorities and update them as necessary based on changing Enterprise needs.
- The Enterprise shall ensure proper accountability protocols are in place to enforce the established roles and responsibilities.
- The Enterprise shall establish procedures for the revocation of roles, responsibilities, or authorities.
- The Enterprise shall establish a centralized awareness of the Enterprise's roles and authorities, which encompasses all technical, personnel, physical, and environmental factors.
- The Enterprise shall identify or establish coordinated authorities for federated operations that cross Enterprise boundaries and define the reporting requirements and mechanisms for each involved Organization or authority.