



National Security Agency/Central Support Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Capability Definitions

Version 1.1.1

The CGS Capability Definitions provide an understanding of the importance of each Capability to the Enterprise. They provide a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

07/30/2012



# CGS Capability Definitions

Version 1.1.1



## Table of Contents

|      |  |    |
|------|--|----|
| 1    | Revisions .....                        | 2  |
| 2    | Capability Definition .....            | 3  |
| 2.1  | Know the Enterprise .....              | 3  |
| 2.2  | Protect the Enterprise .....           | 5  |
| 2.3  | Protect Data and Enable Access.....    | 10 |
| 2.4  | Assess the Vulnerability .....         | 15 |
| 2.5  | Assess the Threat .....                | 16 |
| 2.6  | Detect Events.....                     | 17 |
| 2.7  | Respond to Incidents .....             | 19 |
| 2.8  | Manage Risk .....                      | 20 |
| 2.9  | Manage Investments and Portfolios..... | 21 |
| 2.10 | Manage the Lifecycle .....             | 22 |
| 2.11 | Manage Corporate Culture.....          | 23 |



# CGS Capability Definitions

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 Capability Definitions

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.

### 2.1 Know the Enterprise

| Capability                             | Definition   |
|--|--|
| <b>Network Mapping</b>                 | <p>The Network Mapping Capability helps visualize the network and understand relationships and connectivity between all devices and the communications that provide service. Network Mapping is conducting Enterprise-level mapping of all network components. This mapping should depict every network component's network connectivity, at the nodal, logical, and physical level.</p> <p>For this Capability, network components shall be defined as every network device connected to the network, whether it has an Internet Protocol (IP) address and whether it is physically connected (shall also include wireless devices).</p>  |
| <b>Network Boundary and Interfaces</b> | <p>The Network Boundary and Interfaces Capability for an Enterprise is essential; it provides for an understanding of the resources' interface to other networks or Enterprises, as well as all the interdependencies involved.</p> <p>A network boundary is typically the point at which the resources owned or controlled by an Enterprise stop, and a connection to resources controlled by other entities occurs. Network boundaries are key to ensuring the information assurance (IA) of an Enterprise. Anything inside the network boundary can be controlled, changed, or addressed by the Enterprise; anything outside the network boundary cannot be easily controlled, if it can be controlled at all.</p> <p>Networking services and protocols that use open ports or accept incoming connections are considered interfaces. If an interface is directly accessible by systems that are external to the network, that interface is considered an external interface. Directly accessible means this device is on the edge between owned and un-owned</p> |



# CGS Capability Definitions

Version 1.1.1



| Capability   | Definition   |
|--|--|
|  | <p>resources. Network Boundaries and Interfaces can also be internal to an Enterprise (e.g., the Enterprise can choose to structure its architecture into a set of distinct networks with defined interfaces among them). This can limit damage and risk, although it often has a negative impact on performance and sharing. If an Enterprise chooses to build internal network boundaries into its architecture, it must be able to identify each boundary and determine what is on each side of that boundary.</p> <p>For this Capability, Network Boundaries and Interface components shall be defined as applications, data, and devices connected to both sides of a network boundary (the boundary can be internal (i.e., between enclaves) or external to the Enterprise; however, they may not always be physically connected (e.g., a wireless network interface controller [WNIC] would be one such component).</p> |
| <p><b>Utilization and Performance Management</b></p> | <p>Utilization and Performance Management provides the capability to ensure availability and reliability of resources that directly or indirectly provide support to mission functionality such that they are accessible and usable on demand by an authorized entity. Operations must manage the system to target Utilization and Performance levels to ensure availability and reliability of resources. Specifically, Utilization Management is the directed action to control the use or consumption of organizational resources; Performance Management is the directed action to control and facilitate the accomplishment of a given task.</p>  |
| <p><b>Understand Mission Flows</b></p>               | <p>Understand Mission Flows encompasses the definition and articulation of the relationship and dependencies of the mission to the people, process, technology, and environment that directly fulfill or support the missions. Understand Mission Flows provides the capability for the following:</p> <ol style="list-style-type: none"> <li>1. Intelligent allocation of resources to establish and maintain functions that fulfill the mission</li> <li>2. Mission resiliency, i.e., fighting through the attack and service outage, among others</li> <li>3. Characterization of the mission by its operational status</li> </ol>  |



# CGS Capability Definitions

Version 1.1.1



| Capability                                 | Definition  |
|--|---|
| <b>Understand Data Flows</b>               | 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.      |
| <b>Hardware Device Inventory</b>           | Hardware Device Inventory provides the Enterprise with the methods and schemas necessary to identify and track its classified and unclassified hardware assets, including operational assets and spares. Maintaining a Hardware Device Inventory means to identify the hardware as well as its components. Hardware shall include components such as network interface cards (NICs), telecom devices, network devices, and hard drives. |
| <b>Software Inventory</b>                  | The Software Inventory Capability provides the Enterprise with the methods and schemas necessary to identify and track its software assets. Software may include operating systems, applications, plug-ins, firmware, drivers, and patches.   |
| <b>Understand the Physical Environment</b> | Understand the Physical Environment provides knowledge of the facilities and physical resources being used and provides Enterprise personnel, designated staff, and visitor entry and exit information as well as any interdependencies. Physical Environment includes people, facilities, geographic location, and climate, among other physical considerations.   |

## 2.2 Protect the Enterprise

| Capability               | Definition   |
|--------------------------|--|
| <b>System Protection</b> | System Protection is a broader security capability that is focused on hardware and software (including applications) hardening and enforcement of related protection policies. The goal is to harden devices and software appropriately for the operating environment. System Protection provides enforcement of policies and practices as established in multiple Community Gold Standard (CGS) |



# CGS Capability Definitions

Version 1.1.1



| Capability                                    | Definition   |
|---|--|
|   | capabilities such as Digital Policy Management, Configuration Management, Access Management, and Port Security. In addition, System Protection is responsible for employing malware defenses.  |
| <b>Communication Protection</b>               | Communication Protection is a broad security Capability that is focused on protecting links and routes used for communication and enforcement of related protection policies. The goal is to protect communication channels appropriately for the operating environment. Communication Protection provides enforcement of policies and practices as established in multiple Community Gold Standard (CGS) Capabilities such as Port Security, Network Boundary Protection, Key Management, and Access Management.  |
| <b>Physical and Environmental Protections</b> | Physical and Environmental Protection consists of security in-depth measures (i.e., access controls, cameras, fencing, lighting) that prevent unauthorized access to facilities or resources (i.e., hardware, software); protects resources from natural/unnatural disasters, hazards, and physical and environmental attacks; and encompasses environmental protection, which prevents loss or compromise of facilities, resources, or information resulting from environmental impacts such as temperature, fire, or flood. This Capability allows only people with the proper authorization access to the facilities or information and provides protections for resources even when they are not inside a protected facility (i.e., in the field). |
| <b>Personnel Security</b>                     | Personnel Security programs are the first line of defense in protecting personnel, the environment, physical assets, and technology. The Personnel Security Capability provides the security measures necessary to ensure all affiliates are screened prior to being granted access to facilities, systems, and information. For the purpose of this document, affiliates include employees, contractors, military, second parties, and visitors.  |
| <b>Network Access Control</b>                 | Network Access Control is the capability of the system/network to ensure that each endpoint meets security policies when it connects to the network. The intent of Network Access Control is to provide technical controls to ensure that only authorized computing  |



# CGS Capability Definitions

Version 1.1.1



| Capability                             | Definition  |
|--|---|
|  | <p>platforms gain access to network resources. The Network Access the following:</p> <ul style="list-style-type: none"> <li>• Platform Authentication—Verifies the identity of a platform requesting access to a network</li> <li>• Access Policy Compliance—Determines that a platform requesting network access complies with policy for such access</li> <li>• Endpoint Policy Compliance—Establishes an endpoint's compliance with applicable configuration, patching, and approved software policy</li> <li>• Assessment, Isolation, and Remediation—Isolates platforms not meeting requirements for access from the network and provides for configuration remediation to bring a platform into compliance</li> </ul>   |
| <p><b>Configuration Management</b></p> | <p>The Configuration Management Capability comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configuration of those products and systems. In addition, Configuration Management starts with the establishment of a baseline and provides management of security features and assurances through control of changes made to hardware, firmware, software, and documentation to protect the information system against improper modifications during the system development lifecycle. Continuous monitoring, remediation, and reporting of system configurations are necessary for a successful Configuration Management program. Configuration Management focuses on Secure Configuration Management and Patch Management to provide assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. Configuration Management provides the following focus and capabilities:</p> <ol style="list-style-type: none"> <li>1. Secure Configuration Management is the management and control of configurations for an information system with the goal of enabling security and managing risk. Secure Configuration Management applies the general concepts,</li> </ol> |



# CGS Capability Definitions

Version 1.1.1



| Capability                                | Definition  |
|---|---|
|   | <p>processes, and activities of Configuration Management but with a focus on the outcomes that affect the security posture of the information system.</p> <p>2. Patch Management employs a process to maintain systematic notification, identification, deployment, installation, and verification of operating system (OS) and application software code revisions as well as hardware and firmware. The revisions are known by terms such as updates, patches, hot fixes, and service packs.</p>  |
| <p><b>Port Security</b></p>               | <p>Port Security helps to control access to logical and physical ports, protocols, and services. This includes all Enterprise devices such as network appliances, servers, workstations, and network boundary devices.</p> <p>The Port Security Capability provides the management of logical and physical ports. Port Security management includes deciding which ports, protocols, and services should be available and controlling which services or information may pass to, from, and through the system. This includes making decisions regarding the protection of physical ports and how to lock down services. This Capability also includes an auditing and monitoring function of Enterprise devices to ensure compliance with Port Security policies.</p>   |
| <p><b>Network Boundary Protection</b></p> | <p>Network Boundary Protection is the Capability to protect and control access to Enterprise resources across a security boundary. A security boundary exists when there is a separation of entities (systems, networks, enclaves, or Enterprises), which are governed by differing security policies or operate in a different threat environment. Network Boundary Protection is carried out by placing information assurance (IA) mechanisms between the internal system and the systems external to the security boundary. Examples of such IA mechanisms include, but are not limited to, Cross-Domain Solutions (CDSs), Controlled Interfaces, Demilitarized Zones (DMZs), Virtual Private Networks (VPNs), and encryption devices at the boundary, or interface. Because of the differing nature of boundary protection devices, a brief explanation</p> |



# CGS Capability Definitions

Version 1.1.1



| Capability | Definition  |
|------------|---|
|            | <p>of the example technologies is provided here for completeness.</p> <p>The purpose of a CDS is to provide a manual or automated means for transferring data between two or more differing security domains. The CDS is responsible for ensuring that unauthorized information cannot leak from a domain with information controlled at a higher level (e.g., classified information) to a domain that is controlled at a lower level (e.g., unclassified information). The CDS is also responsible for protecting the network from malicious content that may be passed from the less controlled network. CDSs enable the transfer of information among security domains, which is normally prohibited by automated policies, but is required for successful completion of a mission.</p> <p>The purpose of a Controlled Interface is to control access and information flow into and out of the domain. A Controlled Interface is used when the security policy between interconnected domains is fairly similar. In this instance, the networks are at the same classification level and the risk of contamination or attack by another domain is considered to be sufficiently low.</p> <p>The purpose of a DMZ is to provide an additional layer of security to an Organization's network when some of its services must be exposed to a larger community. A DMZ can be a physical or logical subnetwork. With a DMZ, the Organization can provide an external face and external services, while controlling interactions with the internal network and ensuring that an external attacker is restricted to the equipment in the DMZ, rather than having access to any part of the internal network.</p> <p>The purpose of a secure VPN (not a traffic engineering VPN) is to provide a connection into the network from a remote point, either for a user to gain access or to establish a connection between two networks. To perform this function, the VPN establishes a relationship between the endpoints (through authentication mechanisms) and then encrypts traffic between those endpoints such that traffic is protected from the underlying network.</p> |



# CGS Capability Definitions

Version 1.1.1



## 2.3 Protect Data and Enable Access

| Capability                        | Definition  |
|-----------------------------------|---|
| <p><b>Identity Management</b></p> | <p>Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID. A user ID is a unique identifier, such as a character string, used by an information system to identify a specific user. An identifier is a representation of a person (or non-person entities) on a network. A person or non-person entity can have more than one identifier.</p> <p>Identity Management is the function that unambiguously associates identifiers with entities such as individuals, Organizations, Communities of Interest (COIs), automated processes, and devices—anyone or anything that can perform an action anywhere in the Enterprise system. Identity Management is the underpinning for building trust in a need-to-share Enterprise model, where entities in any environment (stable to austere), and from any location within an Enterprise system, will be able to access information, services, and communications resources based in large part on an authenticated identity. The Identity Management function provides the Enterprise with the ability to create, issue, distribute, maintain, archive, and manage the lifecycle of globally unique identifiers, as well as to serve as an authoritative source of identity information.</p> |
| <p><b>Access Management</b></p>   | <p>Access management enforces the policies that define the actions that an entity may or may not perform against a resource. The Access Management Capability provides criteria that are used to make an access decision and the rules that will be used to assess those criteria. Specifically, Access Management will validate access through these fundamental steps:</p> <ol style="list-style-type: none"> <li>1. Authentication—Validating the identity of an entity within the system.</li> <li>2. Authorization—Determining the rights of the entity with respect to a resource.</li> <li>3. Enforcement—Ensuring that an entity can access only the</li> </ol>   |



# CGS Capability Definitions

Version 1.1.1



| Capability                       | Definition  |
|----------------------------------|---|
|                                  | <p>resources for which it is authorized based on authorization and resource access policies.</p> <p>Access management includes controlling access to physical spaces in addition to access to technology and electronic systems.</p>  |
| <b>Key Management</b>            | <p>Key Management is a service and process that provides, controls, and maintains the cryptographic keys, key material, and certificates required to support a wide range of operational missions. This Capability governs the key lifecycle, which includes key registration, ordering, generation, distribution, usage, expiration, revocation, and destruction. In addition, Key Management includes the functions of compromise management, accounting, handling, audit, and storage.</p>   |
| <b>Digital Policy Management</b> | <p>Digital Policy Management consists of a set of functions used to generate, convert, deconflict, validate, assess effectiveness, provision for distribution and deployment, and execute machine-readable policies used to enforce how resources are managed, used, and protected. These policies may include rules for authentication (e.g., trusted authorities, criteria for determining authenticity), system configurations, access rules, authorized sources of record or sources of reference, transport connectivity, bandwidth allocation and priority, audit event collection, and computer network defense monitoring and response (e.g., course of action).</p> <p>The Digital Policy Management Capability refers to digital policy as expressed in machine-executable form so that it can be directly implemented in systems without human intervention. Non-digital policy is policy that is encapsulated in human language (even if the policy is captured in a "digital form"). Non-digital policy is covered in the IA Policies, Procedures, and Standards Capability.</p> |
| <b>Metadata Management</b>       | <p>Metadata is data about data. It is used to describe characteristics of data assets to enhance their value and usability. There are many different types of metadata. Some of these types include the following:</p>  |



# CGS Capability Definitions

Version 1.1.1



| Capability | Definition   |
|------------|--|
|            | <ol style="list-style-type: none"> <li>1. Discovery metadata—Helps entities find data assets</li> <li>2. Mission metadata—Describes data assets in their mission context</li> <li>3. Information assurance (IA) metadata—Encompasses any metadata associated with the protection of a data asset. This can include metadata describing a data asset’s security properties, protection requirements, applied protections, and provenance (source of an entity). IA metadata enables data consumers to assess the trustworthiness of the data, while allowing providers to specify controls for their data.</li> </ol> <p>IA Metadata Management is the maintenance of IA metadata schemas and the generation, validation, association, and maintenance of IA metadata. The management of IA metadata specifically is the focus of this Capability.</p> <p>IA metadata is needed to realize information sharing objectives. Assured information discovery and retrieval hinges on resource attributes that can be conveyed in IA metadata and are sharable across domains. IA metadata supports interoperability for human understanding of data assets and for processing by automated systems, such as discovery services and access control functions. To fully realize interoperable secure information exchange, Enterprises must adhere to the following: a common and consistent Community-approved controlled IA vocabulary (i.e., standard meaning and vocabulary for security or sensitivity markings, specification of format for IA metadata, specification of subject roles and attributes), a robust information sharing infrastructure to protect both data assets and IA metadata, and a set of tools and protocols that facilitates the adoption of IA metadata standards (e.g., cryptographic binding, IA metadata validation) within and across Enterprise boundaries.</p> <p>IA metadata supports the assessment of the authoritativeness and trustworthiness of data assets that are used by mission supporting entities. This provides the information needed for continuing protection of those data assets. Trustworthiness assessment</p> |



# CGS Capability Definitions

Version 1.1.1



| Capability                          | Definition  |
|-------------------------------------|---|
|                                     | <p>includes identifying the extent to which the data asset should be protected from unauthorized disclosure and from unauthorized or unintentional modification while being processed, stored, or exchanged. The IA metadata and the use of IA for metadata and data assets can be afforded the same authoritativeness and trustworthiness as the data asset, and thereby be relied on to formulate decisions.</p> <p>Like all data, IA metadata needs to be protected using appropriate data protection techniques. IA metadata can be embedded within a data asset, stored alongside a data asset, or stored separately from its associated data asset (e.g., in a repository). Regardless of where IA metadata is stored, all security protections must still apply, such as those provided under the System Protection, Data Protection, and Communications Protection Capabilities, among others.</p>  |
| <p><b>Credential Management</b></p> | <p>A credential is means of providing evidence that supports a claim of identity, assertion, or association. Credential Management encompasses the functions to manage the creation, issuance, maintenance, revocation, reissuance, and status of each credential.</p> <p>Credentials are used as part of the authentication process, and authentication focuses on confirming a person’s (or non-person’s) identity, based on the reliability of his or her credential.</p> <p>There are two types of individual authentication:</p> <ul style="list-style-type: none"> <li>a) Identity authentication—Confirming a person’s unique identity.</li> <li>b) Attribute authentication—Confirming that the person belongs to a particular group or function (such as military veterans or U.S. citizens).</li> </ul> <p>For purposes of this Capability, Credential Management refers to identity credentials only. For information on management of attributes (and application of attribute credentials), see the Attribute Management Capability.</p> <p>Identity authentication can be conducted using credentials such as</p> |



# CGS Capability Definitions

Version 1.1.1



| Capability                         | Definition  |
|------------------------------------|---|
|                                    | <p>certificates and passwords. Certificates are digitally signed representations of an identity that are issued by a trusted authoritative source. For certificate-based credentials, the certificate is presented to support authentication. For non-certificates, such as passwords, authentication is completed by confirming that the credential applies to the user (the credential itself is the linkage between the account and the password).</p>   |
| <p><b>Attribute Management</b></p> | <p>The Attribute Management Capability is responsible for managing the properties associated with entities in the Enterprise; these properties are referred to as attributes. An attribute represents the basic properties or characteristics of an entity that are used to enable the implementation of access control and configuration management policies. Examples of some possible attributes are contact attributes (email address, phone number), demographic attributes (organization, affiliation), and device attributes (physical location, logical addresses, installed software, and patch level).</p> <p>Attribute Management encompasses the functions that manage the identification, maintenance, and publication of each attribute. In addition, Attribute Management identifies the attributes that are needed and an authoritative source from which to retrieve the attribute values.</p> <p>A given attribute may be dynamic or static, which is determined by the authoritative source. Attribute Management provides for a capability in which all attributes stored by any system on a network are controlled by a set of policies to restrict or enable access based on functional need.</p> |
| <p><b>Data Protection</b></p>      | <p>Data protection is protecting all data so that it is available when requested and only authorized users may access, modify, destroy, or disclose the data. Data protection is enforced in all data states including in use, at rest, and in transit. Data in use refers to data that is being acted upon. Data at rest refers to data that is being stored. Data in transit refers to data being transferred between systems.</p>  |



# CGS Capability Definitions

Version 1.1.1



## 2.4 Assess the Vulnerability

| Capability                                 | Definition   |
|--|--|
| <p><b>Network Security Evaluations</b></p> | <p>Network Security Evaluations are comprehensive examinations of a network, its architecture, and its defenses. They are used to identify strengths and weaknesses in a given network and provide recommendations for correcting the problems that are identified.</p> <p>Network Security Evaluations are used by Organizations to accomplish several objectives:</p> <ul style="list-style-type: none"> <li>• Identify vulnerabilities in operational systems</li> <li>• Measure the effectiveness of security policy and effect changes</li> <li>• Demonstrate the impact of network vulnerabilities when attacked</li> </ul> <p>Network Security Evaluations are commonly conducted in two parts, where each part takes a different approach to assessing the network. One approach is to attempt to infiltrate the system by emulating an adversary. The other approach is to conduct the evaluation in cooperation with the local network and system administrators to review the security policies, protections, and network architecture. Network Security Evaluations identify vulnerabilities that exist within a network and provide feedback to the network owners, identifying those vulnerabilities, making recommendations for mitigation, and stating their mission impact.</p> |
| <p><b>Architecture Reviews</b></p>         | <p>The Architecture Reviews Capability establishes Architecture Reviews, which are requirements-based reviews to determine whether the requirements were satisfied by the architecture. Security Architecture Reviews focus specifically on determining whether the security requirements for a system, application, or service were included in the architecture (sometimes called security architecture). The reviews demonstrate security requirement satisfaction as well as potential vulnerabilities as a result of missing requirements. The review may be conducted on logical (e.g., data</p>   |



# CGS Capability Definitions

Version 1.1.1



| Capability                      | Definition  |
|---------------------------------|---|
|                                 | flows) or physical (e.g., physical connections) architectures.  |
| <b>Vulnerability Assessment</b> | A vulnerability is a weakness that has the potential to reduce an Enterprise's ability to fulfill its mission. Vulnerability Assessment is the systematic examination of an Enterprise to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Vulnerability alerts are released to initiate follow-on functions. |

## 2.5 Assess the Threat

| Capability               | Definition   |
|--------------------------|--|
| <b>Threat Assessment</b> | <p>The Threat Assessment Capability identifies, analyzes, and prioritizes threat information by identifying threats and threat sources, understanding the threat's capability, and determining the likelihood of the threat occurring.</p> <p>A threat is the potential for a particular threat source (or set of threat sources) to successfully exploit a particular vulnerability (or set of vulnerabilities) that has the potential to adversely impact agency, agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.</p> <p>A threat source is either 1) the intent and method targeted to intentionally exploit a particular vulnerability (or set of vulnerabilities) or 2) a situation and method that may accidentally overwhelm a vulnerability (or set of vulnerabilities). Common threat sources include, but are not limited to, natural threats such as floods, earthquakes, and tornadoes; human threats such as terrorists, computer criminals, and insiders; and environmental threats such as long-term power failure, chemicals, and pollution.</p> <p>A threat capability is the level of access, resources, knowledge, and skill that a threat source is capable of applying against</p> |



# CGS Capability Definitions

Version 1.1.1



|                             |   |
|-----------------------------|---|
|                             | technical, personnel, physical, and environmental aspects of the Enterprise. The threat likelihood is the probability of a given threat source's attempt to exploit a given vulnerability.  |
| <b>Signature Repository</b> | A Signature Repository Capability provides a group of signatures for use by network security tools such as anti-virus applications, host or network sensors that require signatures (e.g., intrusion detection/prevention systems), and other monitoring and detection applications. For analysis, the Organization uses these signatures to understand the attack patterns and their relationship to specific threats or activities. |

## 2.6 Detect Events

| Capability                             | Definition  |
|--|---|
| <b>Network Enterprise Monitoring</b>   | The Network Enterprise Monitoring Capability employs active and passive monitoring of the network on an Enterprise level to detect security- or performance-relevant changes or events. This includes continuously monitoring the state of the network and networked devices across the Enterprise to share awareness of event changes. It also includes monitoring health and status, links between devices, and traffic flow. Enterprise-level monitoring is used to provide inputs to the overall situational awareness picture. |
| <b>Physical Enterprise Monitoring</b>  | Physical Enterprise Monitoring is the monitoring of the physical and environmental controls that prevent unauthorized physical access to facilities, systems, or other resources. This Capability includes the monitoring of the environment, systems, hazards, and other resources; it ensures that the physical and environment protection systems are still effective when changes occur.  |
| <b>Personnel Enterprise Monitoring</b> | Personnel Enterprise Monitoring is the monitoring of the personnel mechanisms and processes that prevent unauthorized access to facilities, systems, and information. The Personnel Enterprise Monitoring Capability provides assurance that the affiliates granted access to facilities, systems, and information have proper authorization and clearances and follow information assurance (IA) policies and practices. The Personnel Enterprise Monitoring   |



# CGS Capability Definitions

Version 1.1.1



| Capability                                | Definition   |
|---|--|
|   | <p>Capability establishes and executes the ongoing procedures that occur after the initial personnel security verifications, which provide a basis for granting access. For the purpose of this document, affiliates include employees, contractors, military, second parties, and visitors.</p>   |
| <p><b>Network Intrusion Detection</b></p> | <p>The Network Intrusion Detection Capability helps to detect malicious activity incoming to, outgoing from, and on the network. Network Intrusion Detection Systems are deployed to inspect all network traffic for malicious activity, including anomalies and incidents. The network traffic is examined by passive and in-line computer network defense sensors located within the network.</p>  |
| <p><b>Host Intrusion Detection</b></p>    | <p>The Host Intrusion Detection Capability helps to detect malicious activity by monitoring for anomalies within the system that indicate malicious activity. The Capability is deployed to monitor the internals of a system(s) for threats.</p>  |
| <p><b>Network Hunting</b></p>             | <p>The Network Hunting Capability is employed to proactively look for indicators of an active threat or exploitation of a vulnerability that was previously known or unknown. Network Hunting may involve signature detection and detection of changes in behaviors and normal usage, as well as the ability to detect incidents that are not known to be occurring.</p>   |
| <p><b>Physical Hunting</b></p>            | <p>Physical Hunting is employed to detect anomalies in the physical components, and vulnerabilities associated with those components, in the physical infrastructure of the Enterprise. Physical Hunting may involve detection of technical surveillance devices (e.g., keystroke taps, bugs). This Capability provides for hardware forensics and searching for vulnerabilities in the physical Enterprise, including intended emanations and changes to the environment.</p> |
| <p><b>Enterprise Audit Management</b></p> | <p>The Enterprise Audit Management Capability involves the identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring and maintenance of the Capability. An Enterprise Audit Management solution should be</p>   |



# CGS Capability Definitions

Version 1.1.1



| Capability | Definition   |
|------------|--|
|            | deployed to centralize audit collection and provide appropriate storage for and access to audit data. For each type of audit (specific to system/mission/data), auditable events are identified, auditing is conducted to properly capture and store that data, and analysis and reporting are performed. Certain high-profile events should trigger automated notification to individuals such as systems administrators. |

## 2.7 Respond to Incidents

| Capability                          | Definition  |
|-------------------------------------|---|
| <b>Incident Response</b>            | Incident Response is a conscious plan of action given the stimulus of an assessed occurrence having actual or potentially adverse effects on an asset. It involves notification, triage, escalation, isolation, and restoration (when appropriate) of technical, personnel, physical, and environmental incidents. Incident Response provides the Capability to respond to any incident (both external to the network and information technology [IT] related). A formal Incident Response Team (IRT) provides the expertise to appropriately respond to the problem. |
| <b>Incident Analysis</b>            | Incident Analysis uses information gathered during Incident Response to determine the root cause of an incident. The Incident Analysis generated is used to develop, recommend, and coordinate Enterprise mitigation actions for technical, personnel, physical, and environmental incidents.   |
| <b>Network Intrusion Prevention</b> | Network Intrusion Prevention employs a response to perceived anomalous activity on the network. When this activity is perceived, Network Intrusion Prevention encompasses mechanisms to react to block, drop, redirect, and/or quarantine anomalous activities. Network Intrusion Prevention is enabled through network-based modules deployed throughout the network.  |
| <b>Host Intrusion Prevention</b>    | The Host Intrusion Prevention Capability employs a response to a perceived incident of interference on a host-based system and  |



# CGS Capability Definitions

Version 1.1.1



| Capability                         | Definition   |
|------------------------------------|--|
|                                    | <p>encompasses mechanisms that reside on a host to react in real-time to block, drop, redirect, and/or quarantine malicious activities. Host Intrusion Prevention is enabled through a host-based system rather than on a network appliance.</p>   |
| <p><b>Contingency Planning</b></p> | <p>Contingency Planning establishes policy, procedures, and technical measures designed to maintain or restore business operations. This includes computer operations (possibly at an alternate location) in the event of emergencies, system failures, or disasters. Contingency Planning occurs under all circumstances, including major disasters and events.</p> <p>The Contingency Planning Capability focuses on Information System Contingency Planning, which refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption (National Institute of Standards and Technology [NIST] Special Publication [SP] 800-34). The purpose of Information Systems Contingency Planning is to ensure the business and mission functions of an Organization under all circumstances.</p> |

## 2.8 Manage Risk

| Capability                        | Definition   |
|-----------------------------------|--|
| <p><b>Risk Identification</b></p> | <p>Risk Identification is the creation of a relationship between the results of the Threat Assessment and Vulnerability Assessment Capabilities. It establishes the influence that the threats and vulnerabilities are perceived to have on the Enterprise's risk.</p> <p>The risk-related data comprises known threats and vulnerabilities and their combined impact. With this in mind, a simple notional function that demonstrates the relative relationships between Risk, Threat, Vulnerability, and Impact is <math>R = f(T,V,I)</math> as represented by a portfolio of attacks. The impact portion of the relationship is determined in the Risk Analysis Capability.</p> |



# CGS Capability Definitions

Version 1.1.1



| Capability             | Definition  |
|------------------------|---|
| <b>Risk Analysis</b>   | The Risk Analysis Capability collects and analyzes risk-related data from the Risk Identification Capability for the broader purpose of providing decision-makers information on the benefits, costs, and uncertainty of alternative courses of action with respect to executing the assigned mission in multiple environments. The risk-related data comprises known threats and vulnerabilities and their combined impact. With this in mind, a simple notional function that demonstrates the relative notional relationships between Risk, Threat, Vulnerability, and Impact is $R = f(T,V,I)$ , as represented by a portfolio of attacks. The threat and vulnerability information is aggregated from the Threat and Vulnerability Assessment Capabilities during the risk identification process in the Risk Identification Capability. |
| <b>Risk Mitigation</b> | Risk Mitigation is the reduction of the likelihood and/or impact of Enterprise security risk. The Risk Mitigation Capability decides which mitigations will be applied to identified risks, implements those mitigations, and subsequently reduces the risk level.  |
| <b>Risk Monitoring</b> | Risk Monitoring assesses the effectiveness of the risk decisions that are made by the Enterprise. This Capability establishes the current security posture and then determines the gaps between the current security posture and the intended risk posture (see the Risk Analysis Capability). Risk Monitoring includes the monitoring of risks (as identified in the Risk Identification Capability) pertaining to people, operations, technology, and environments. Risk levels must be monitored based on changes in the risk posture.   |

## 2.9 Manage Investments and Portfolios

| Capability     | Definition   |
|----------------|--|
| <b>Finance</b> | Finance is an integral part of the Organization's process for obtaining funds for the procurement of information assurance (IA) services and products in line with the Organization's current budget. The Finance Capability ensures that Organizations have budgeted for IA programs, products, and services throughout the |



# CGS Capability Definitions

Version 1.1.1



| Capability                  | Definition   |
|-----------------------------|--|
|                             | Enterprise. The budget includes funding for personnel, operational, environmental, and technical considerations, as well as funding for enabling supporting resources such as IA training and recruitment.   |
| <b>Acquisition</b>          | The Acquisition Capability provides supply chain risk management by determining an appropriate risk management approach for individual acquisitions of products and services. The Acquisition Capability provides research and analysis of suppliers and products and provides that information to the Risk Analysis Capability to make a risk decision regarding whether risks associated with a product or service can be properly managed by the Enterprise. These measures provide assurance against products having intentional security flaws, supplier personnel posing unknown vulnerabilities, or other risks that may be unacceptable to the Enterprise.                               |
| <b>Portfolio Management</b> | Portfolio Management is the process of analyzing, selecting, controlling, and evaluating Capability needs against current and planned investments within a Capability portfolio to better inform decision-makers and optimize resources. Portfolio Management involves the alignment of programs, initiatives, and activities with Enterprise priorities and requirements to maximize the return on investment. This Capability is specifically concerned with information assurance (IA) Portfolio Management, which is focused on the alignment of IA programs, initiatives, and activities. This information will feed into the Enterprise's overall Portfolio Management Capability efforts. |

## 2.10 Manage the Lifecycle

| Capability         | Definition   |
|--------------------|--|
| <b>Development</b> | Development is the creation of a solution based on an identified need. The development phase of the lifecycle comprises many activities that ensure that information assurance (IA) is included from concept up to the Deployment Capability. The Development Capability includes the incorporation of IA during architecture, |



# CGS Capability Definitions

Version 1.1.1



| Capability                        | Definition   |
|-----------------------------------|--|
|                                   | concept, design, implementation/build, integration, requirements, and test.  |
| <b>Deployment</b>                 | Deployment is the phase of the system development lifecycle in which solutions are placed into use to change or maintain the operational baseline. The Deployment Capability ensures that information assurance (IA) is employed while the processes for deployment are executed. When necessary, Deployment includes integration into the environment or other solutions and testing within that environment.   |
| <b>Operations and Maintenance</b> | The Operations and Maintenance Capability encompasses the activities of the Operations and Maintenance phases of the system development lifecycle. These activities include technical and administrative procedures that account for the use and maintenance of hardware, software, and data assets that support the mission. The Operations and Maintenance Capability shall employ an approved system development lifecycle process (established in accordance with the IA Policies, Procedures, and Standards Capability) that implements and maintains information assurance (IA) during Operations and Maintenance. |
| <b>Decommission</b>               | The Decommission Capability includes the execution of technical and administrative procedures prior to, during, and following removal and disposal of hardware, software, and data assets. During decommission, approved procedures are employed, which maintain information assurance (IA) and prevent the inadvertent compromise of data. This may include sanitization, declassification, and additional releasability procedures.  |

## 2.11 Manage Corporate Culture

| Capability                                    | Definition   |
|---|--|
| <b>IA Policies, Procedures, and Standards</b> | The Information Assurance (IA) Policies, Procedures, and Standards Capability encompasses existing policies, procedures, and standards and defines, distributes, stores, implements, |



# CGS Capability Definitions

Version 1.1.1



| Capability          | Definition  |
|---------------------|---|
|                     | <p>enforces, reviews, and maintains them, as needed. IA Policies, Procedures, and Standards are defined by an Organization in accordance with national, Department of Defense (DoD), and Intelligence Community (IC) policies. These policies, procedures, and standards may be used in identifying and establishing subsequent policies, procedures, and standards for IA. Organizations may use a variety of terminology in their internal structure to refer to policies, procedures, and standards.</p> <p>Policies regulate, direct, or control actions for the Organization. They generally provide broad statements, assign responsibilities and authorities, and identify the applicable policy source and references.</p> <p>Procedures provide specific implementations for the policy, which may assign further responsibility and implementation guidance. Procedures tend to be written at a lower level than policies and contain more specific information about what actions are required.</p> <p>Standards include establishment of the corporate vision and strategy, Enterprise operations, and governance. They define the mission statement and goals. At the lower level, standards also define corporate or technical best practices (a subset of policies and procedures). Standards that are defined based on the needs of the Organization can also be used to generate IA policy and procedures.</p> |
| <b>IA Awareness</b> | <p>The Information Assurance (IA) Awareness Capability promotes understanding of IA objectives, threats, risks, and actions, among other IA concerns. IA Awareness is intended to empower individuals to recognize IA or security concerns and respond accordingly.</p>   |
| <b>IA Training</b>  | <p>Information Assurance (IA) Training is the training of users and IA practitioners on IA policies, requirements, processes, and procedures. It also includes technical and operational IA Training to all personnel based on user and/or role. Within this Capability, an IA Training program is established, which includes identification,</p>  |



# CGS Capability Definitions

Version 1.1.1



| Capability                           | Definition   |
|--------------------------------------|--|
|                                      | administration, maintenance, and evaluation of the training activities and materials.  |
| <b>Organizations and Authorities</b> | <p>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.</p> <p>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.</p> |