



National Security Agency/Central Support Service



INFORMATION ASSURANCE DIRECTORATE

CGS IA Policies, Procedures, and Standards Capability

Version 1.1.1

The Information Assurance (IA) Policies, Procedures, and Standards Capability encompasses existing policies, procedures, and standards and defines, distributes, stores, implements, enforces, reviews, and maintains them, as needed.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

Table of Contents

- 1 Revisions2
- 2 Capability Definition3
- 3 Capability Gold Standard Guidance.....3
- 4 Environment Pre-Conditions7
- 5 Capability Post-Conditions.....7
- 6 Organizational Implementation Considerations8
- 7 Capability Interrelationships..... 11
 - 7.1 Required Interrelationships 11
 - 7.2 Core Interrelationships 13
 - 7.3 Supporting Interrelationships..... 14
- 8 Security Controls 14
- 9 Directives, Policies, and Standards20
- 10 Cost Considerations29
- 11 Guidance Statements.....30

1



CGS IA Policies, Procedures, and Standards Capability



Version 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 IA Policies, Procedures, and Standards 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 Information Assurance (IA) Policies, Procedures, and Standards Capability encompasses existing policies, procedures, and standards and defines, distributes, stores, implements, 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. The IA Policies, Procedures, and Standards Capability 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.

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.

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.

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.

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.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

The IA Policies, Procedures, and Standards Capability operates at different levels within an Enterprise. IA Policies, Procedures, and Standards are established at the Enterprise level, organizational level, and program level. At the highest level, standards define the Enterprise's vision, mission, and strategy. They shall be built from the top down to ensure achievement of the corporate vision. Enterprise level policies create an IA program for the Enterprise, establish its goals, and assign responsibilities. Policy decisions at any level will affect the entire Enterprise. Thus each subordinate policy, procedure, or standard shall not diminish the overarching policy and shall not negatively impact the mission of partnering Organizations. In addition subordinate policies shall ensure interoperability between partnering Organizations.

The IA Policy, Procedures, and Standards Capability shall identify existing policies, procedures, and standards. Based on the identified policies, procedures, and standards, the Capability shall define, distribute, store, implement, enforce, review, and maintain policies, procedures, and standards as applicable.

Identify:

This Capability shall provide the ability to identify higher-level, overarching policies (e.g., source and content) and analyze gaps. Multiple sources may exist for different types of policies, procedures, and standards based on the Enterprise and the policy, procedures, and standards being defined. This Capability shall determine if there are policies, procedures, and standards defined at a higher or peer level. Reuse of higher-level and peer-level policies shall occur, where possible.

Define:

The appropriate Enterprise authority shall exist to define policies, procedures, and standards; document the reason for defining the policy, procedure, or standard; document alignment with higher-level and peer standards and policies; and determine at what level they shall exist and be implemented. Each policy or standard shall include an outlook to the future and have complementary lower-level procedures and implementation guidance. Decision-makers shall rely on Enterprise subject matter experts to define the policy and include input from many different parties from within each Organization, such as the Chief Information Security Officer (CISO), the Enterprise's highest level decision-makers, and possibly department heads and major project managers. Review and coordination shall occur in a timely manner such that the policies and procedures can affect the change.

Distribute/Store:



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

Policies, procedures, and standards shall be centrally managed and shall be under configuration control. Policies, procedures, and standards shall be distributed only from the originating source. The IA Policies, Procedures, and Standards Capability shall provide a process for notifying interested parties of new policies, procedures, and standards, as well as ensuring old policies, procedures, and standards are archived based on Enterprise requirements.

Implement:

Once IA Policies, Procedures, and Standards have been established to ensure compliance, responsibility shall be delegated to relevant users and groups for implementation. The responsible Enterprise is the implementer with the necessary authorities and resources to implement and execute the policy and procedure. The implementation timeframe shall occur as dictated in the policies, procedures, and standards. If a timeframe is not dictated, the Enterprise authority shall define the timeframe.

Enforcement:

In addition to establishing IA Policies, Procedures, and Standards for the Enterprise to follow, this Capability also shall establish governance practices to ensure compliance. Accountability for implementation shall be provided. Enforcement mechanisms shall be defined, which may require the implementation of supplemental security controls to provide protections that enforce the policy or deter actions outside of the policy. Protections shall be provided by the Protect the Enterprise Capabilities, the Protect Data and Enable Access Capabilities, and policies and procedures defined within this Capability.

Review and Maintain:

All IA Policies, Procedures, and Standards shall undergo a periodic review process, which includes stakeholders, to address identified gaps and to ensure their continued effectiveness and applicability to technological advances. Changes shall be implemented in a timely manner and align with technology, when necessary, to ensure policies and procedures are useful. Standards and procedures shall be reviewed and updated any time policies or processes change. A standard shall be established that defines how often IA policies, procedures, and standards are reviewed. This standard may be dictated by a parent Organization.

An Enterprise's higher-level policies and standards shall:

- Create and Define an IA Policy—Policy shall be clear as to which resources the policy covers, including facilities, hardware and software, information, and personnel.
- Set Enterprise vision, mission, and strategy—This includes defining the goals of the Enterprise. For example, in an Enterprise responsible for maintaining large



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

mission-critical databases, reduction in errors, data loss, data corruption, and recovery might be specifically addressed.

- Assign Responsibilities—Responsibilities shall be assigned to the Computer Security Organization responsible for direct implementation and other responsibilities shall be assigned to related offices (such as the Information Resources Management Organization).
- Address Compliance Issues—Policy shall address two compliance issues and thereby, meet the requirements to establish: 1) the responsibilities assigned therein to various Enterprise components, and 2) the use of specified penalties and disciplinary actions.

An Enterprise's policies, procedures, and standards shall:

- Address Specific Areas—Topics of current relevance and concern to the Enterprise shall be addressed. Management may find it appropriate, for example, to issue a policy, procedure, or standard defining how the Enterprise will approach e-mail privacy or Internet connectivity.
- Be Updated Frequently—More frequent modification of technical standards and policies is required as changes in technology and related factors take place. If a policy was issued, for example, on the appropriate use within the Enterprise of a cutting-edge technology (whose security vulnerabilities are still largely unknown), it could require updating.
- Contain an Issue Statement—The Enterprise's position statement, applicability, roles and responsibilities, compliance, and point of contact shall be clear.
- Focus on Decisions—The decisions made by management to protect a particular system shall be explicitly stated, such as defining the extent to which individuals will be held accountable for their actions on the system.
- Be Made by a Management Official—An authorized person shall make management decisions based on a mission need.
- Vary for Differing Systems—Variances may occur because system security objectives are based on the system's operational requirements, environment, and the manager's acceptance of risk. Policy shall ensure the decision-maker's acceptance of risk does not cause risk to other systems. Similar systems shall not vary because variances may inhibit interoperability. Standards shall be used to ensure consistency. In addition, policies may vary based on differing needs for detail.
- Be Expressed as Rules—Who (by job category, Enterprise placement, or name) can do what (e.g., modify, delete) to which specific classes and records of data, and under what conditions.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

All policies, procedures, and standards shall be:

- **Supplemented**—Because policy may be written at a broad level, Enterprises also develop standards, guidelines, and procedures that offer users, managers, and others a clearer approach to implementing policy and meeting Enterprise goals. Standards, guidelines, and procedures shall be disseminated throughout an Enterprise via various methodologies including, but not limited to, handbooks, regulations, or manuals.
- **Visible**—Visibility aids in ensuring policies and standards are prevalent and accessible, and it helps to ensure they are fully communicated throughout the Enterprise.
- **Supported by Management**—Without management support, the policies and standards will not be implemented consistently across the Enterprise.
- **Consistent**—As appropriate, other federal laws, Executive Orders, regulations, directives, policies, procedures, Enterprise culture, guidelines, and Enterprise mission shall be considered when drafting IA Policies, Procedures, and Standards.

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. IA awareness and training programs are established to communicate IA policies, procedures, and standards.
2. The Enterprise has defined its organizations and authorities that will enable implementation and enforcement.
3. The Organization understands and has documented its environment, network, mission, and risk.
4. Governing bodies are in place to define Enterprise specific roles.
5. Higher-level policies, procedures, and standards are in place.

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 generates IA Policies, Procedures, and Standards for the entire Organization and potentially other Organizations as defined by authorities.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

2. The Capability creates measures and compliance mechanisms to enforce IA Policies, Procedures, and Standards.
3. The Capability ensures that corporate IA policies are incorporated into all levels of the Organization.
4. The Capability reuses policies, procedures, and standards where already defined and applicable.
5. IA policies and procedures are tailored, if necessary, to meet the mission of different Organizations or departments.
6. The Capability ensures that all IA Policies, Procedures, and Standards are followed appropriately.

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).

Each Organization will establish IA Policies, Procedures, and Standards to ensure a consistent and coherent Enterprise understanding of the Organization's risk tolerance. The policies, procedures, and standards will be consistent with higher-level policies and procedures and follow the guidance defined within the Community Gold Standard Capabilities.

Organizations will establish the Enterprise architecture as part of its vision, mission, and strategy. Organizational authorities shall understand who the policies, procedures, and standards can be imposed upon and the purview of the policies, procedures, and standards.

Each Organization will identify the policies, procedures, and standards defined at a higher level or at a peer Organization that will be implemented. To identify the applicable policies, procedures, and standards, each Organization will determine the appropriate authoritative sources (e.g., DoD, IC, CNSS, National Institute for Standards and Technology (NIST)) for different types of policies and procedures based on the Organization and the policies, procedures, and standards being defined. The Organization may reuse the policies, procedures, and standards, or they may be used in



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

the definition of lower-level, organizational, or program-specific policies, procedures, or standards.

Each Organization will designate an authority to define the policy, procedure, or standard. When a policy is needed, it may be necessary to have an authority at a higher level define the policy or standard to be applied. Typically, policy needs will be identified and will be signed off by the Chief Information Officer (CIO)/CISO, but they can be defined at a lower level, depending on the Organization's authorities and the application of the policy, procedure, or standard. In addition, many individuals are involved in the standards creation process, including executive leadership, the CISO, other IA personnel, and any other stakeholders.

Each Organization will establish its corporate IA standards in accordance with policies set by governing Organizations and the Community. Some policies and standards will be written at a high level and will not include specific guidance because of the changing nature of technology. These policies and standards will be an outlook to the future and stand the test of time, so that they do not have to be constantly updated. However, flexibility needs to be built in to update technical procedures and standards because they exist in a more dynamic environment than the Organization's overall vision and mission. Each Organization will establish procedures and standards at the lower level and provide implementation guidance for the policy that considers mission impact and resources affected. Organizations will rely on organizational subject matter experts to define procedures and standards. Each organization will adopt a common vocabulary when writing policy and align with the Committee on National Security Systems Instruction (CNSSI) 4009 (IA Glossary).

Each Organization will ensure that stakeholders related to the policy, procedures, and standards area participate in the coordination, review, and approval of policies and standards. Coordination will occur in a timely manner such that the policies, procedures, and standards can affect the change. Designated authorities will remain engaged with stakeholders throughout the coordination and review process to be able to have an influence on changes as they occur.

Each Organization will establish or identify a Policy Management Office to define a process for distributing notification of new policies, procedures, and standards to interested parties. In addition, the Policy Management Office will define a configuration control process for the policy repository. Policies, procedures, and standards will be distributed only if the Organization is the originating source. When an Organization is not



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

the originating source, the Organization will provide links in the centralized repository to source documents. In addition, links to policies, procedures, and standards originated by an Organization shall be distributed for use by other Organizations. Old policies, procedures, and standards are maintained in the repository until a new document is signed and enacted. Archival of old documents will be in accordance with the applicable policy for managing records. Each Organization will ensure distribution occurs in a timely manner, as defined by the organizational authority, once a policy has been signed and enacted.

Responsibilities for implementing the defined policies, procedures, and standards are delegated to various functional groups within the Organization. The Organization shall identify the specific department or group and ensure it has the necessary authorities and resources to implement the policy, procedure, or standard. Implementation of the policy, procedure, or standard will occur in the timeframe dictated in the policy, procedure, or standard. If a timeframe is not dictated, the Organizational authority will define the timeframe.

Each Organization will create measures and compliance mechanisms to enforce IA policies, procedures, and standards. Organizations will provide protections that enforce the policy or deter actions outside of the policy. These protections can be provided by the Protect the Enterprise and Protect Data and Enable Access Capabilities, along with policies, procedures, and standards defined within this Capability. A senior authorizing official within the Organization, related to the policy or standard area, shall enforce the policies, procedures, and standards.

Each Organization will review its mission drivers, environment, risk posture, and the specific policy or standard area and establish a policy review cycle. How often policies, procedures, and standards are reviewed and updated is dependent on the Organization. If the Enterprise environment is dynamic, the frequency of reviews may be more often. In addition, procedures and standards are more volatile than policy and higher-level standards and will be reviewed more frequently. Policy changes, as well as technological evolution, can affect a procedure or standard change. Specific risks to the environment may affect an immediate policy, procedure, or standard change. Organizations will decide which factors will affect a procedure or standard change beyond these identified areas. The Organization will include the originator, stakeholders, and subject matter experts in the policies, procedures, and standards reviews.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

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.

- Network Mapping—The IA Policies, Procedures, and Standards Capability relies on the Network Mapping Capability to provide information about the Enterprise environment so that the appropriate policies, procedures, and standards are applied.
- Network Boundary and Interfaces—The IA Policies, Procedures, and Standards Capability relies on the Network Boundary and Interfaces Capability to provide information about the Enterprise environment so that the appropriate policies, procedures, and standards are applied.
- Utilization and Performance Management—The IA Policies, Procedures, and Standards Capability relies on the Utilization and Performance Management Capability to provide information about the Enterprise environment so that the appropriate policies, procedures, and standards are applied.
- Understand Mission Flows—The IA Policies, Procedures, and Standards Capability relies on the Understand Mission Flows Capability to provide information about the Enterprise environment so that the appropriate policies, procedures, and standards are applied.
- Understand Data Flows—The IA Policies, Procedures, and Standards Capability relies on the Understand Data Flows Capability to provide information about the Enterprise environment so that the appropriate policies, procedures, and standards are applied.
- Hardware Device Inventory—The IA Policies, Procedures, and Standards Capability relies on the Hardware Device Inventory Capability to provide information about the Enterprise environment so that the appropriate policies, procedures, and standards are applied.
- Software Inventory—The IA Policies, Procedures, and Standards Capability relies on the Software Inventory Capability to provide information about the Enterprise environment so that the appropriate policies, procedures, and standards are applied.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

- Understand the Physical Environment—The IA Policies, Procedures, and Standards Capability relies on the Understand the Physical Environment Capability to provide information about the Enterprise environment so that the appropriate policies, procedures, and standards are applied.
- System Protection—The IA Policies, Procedures, and Standards Capability relies on the System Protection Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Communication Protection—The IA Policies, Procedures, and Standards Capability relies on the Communication Protection Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Physical and Environmental Protection—The IA Policies, Procedures, and Standards Capability relies on the Physical and Environmental Protection Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Personnel Security—The IA Policies, Procedures, and Standards Capability relies on the Personnel Security Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Network Access Control—The IA Policies, Procedures, and Standards Capability relies on the Network Access Control Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Configuration Management—The IA Policies, Procedures, and Standards Capability relies on the Configuration Management Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Port Security—The IA Policies, Procedures, and Standards Capability relies on the Port Security Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Network Boundary Protection—The IA Policies, Procedures, and Standards Capability relies on the Network Boundary Protection Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Identity Management—The IA Policies, Procedures, and Standards Capability relies on the Identity Management Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Access Management—The IA Policies, Procedures, and Standards Capability relies on the Access Management Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

- Key Management—The IA Policies, Procedures, and Standards Capability relies on the Key Management Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Digital Policy Management—The IA Policies, Procedures, and Standards Capability relies on the Digital Policy Management Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Metadata Management—The IA Policies, Procedures, and Standards Capability relies on the Metadata Management Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Credential Management—The IA Policies, Procedures, and Standards Capability relies on the Credential Management Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Attribute Management—The IA Policies, Procedures, and Standards Capability relies on the Attribute Management Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.
- Data Protection—The IA Policies, Procedures, and Standards Capability relies on the Data Protection Capability to create measures and compliance mechanisms to enforce IA policies, procedures, and standards.

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 IA Policies, Procedures, and Standards Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Awareness—The IA Policies, Procedures, and Standards Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The IA Policies, Procedures, and Standards Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities—The IA Policies, Procedures, and Standards Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

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.

- None

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-1 ACCESS CONTROL POLICIES AND PROCEDURES	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Enhancements: None Specified
AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. Enhancement/s: None Specified
AU-1 AUDIT AND ACCOUNTABILITY POLICY AND	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented audit and accountability policy that



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

<p><i>PROCEDURES</i></p>	<p>addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.</p> <p>Enhancement/s: None Specified</p>
<p><i>CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES</i></p>	<p>Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:</p> <p>a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.</p> <p>Enhancement/s: None Specified</p>
<p><i>CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES</i></p>	<p>Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:</p> <p>a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.</p> <p>Enhancement/s: None Specified</p>
<p><i>CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES</i></p>	<p>Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:</p> <p>a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls</p>



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

	Enhancement/s: None Specified
IA-1 <i>IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES</i>	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. Enhancement/s: None Specified
IR-1 <i>INCIDENT RESPONSE POLICY AND PROCEDURES</i>	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. Enhancement/s: None Specified
MA-1 <i>SYSTEM MAINTENANCE POLICY AND PROCEDURES</i>	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. Enhancement/s: None Specified.
MP-1 <i>MEDIA PROTECTION POLICY AND PROCEDURES</i>	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

	<p>b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. Enhancement/s: None Specified.</p>
<p><i>PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES</i></p>	<p>Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:</p> <p>a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. Enhancement/s: None Specified.</p>
<p><i>PL-1 SECURITY PLANNING POLICY AND PROCEDURES</i></p>	<p>Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:</p> <p>a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</p> <p>b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls. Enhancement/s: None Specified</p>
<p><i>PM-1 INFORMATION SECURITY PROGRAM PLAN</i></p>	<p>Control: The organization:</p> <p>a. Develops and disseminates an organization-wide information security program plan that:</p> <ul style="list-style-type: none"> – Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; – Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

	<p>as intended;</p> <ul style="list-style-type: none"> – Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; – Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; <p>b. Reviews the organization-wide information security program plan [Assignment: organization-defined frequency]; and</p> <p>c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.</p> <p>Enhancement/s: None Specified</p>
PM-7 ENTERPRISE ARCHITECTURE	<p>Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.</p> <p>Enhancement/s: None Specified</p>
PM-9 RISK MANAGEMENT STRATEGY	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization. <p>Enhancement/s: None Specified</p>
PM-11 MISSION/BUSINESS PROCESS DEFINITION	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. <p>Enhancement/s: None Specified</p>
PS-1 PERSONNEL SECURITY POLICY	<p>Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:</p>



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

<p><i>AND PROCEDURES</i></p>	<p>a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. Enhancement/s: None Specified.</p>
<p><i>RA-1 RISK ASSESSMENT POLICY AND PROCEDURES</i></p>	<p>Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. Enhancement/s: None Specified.</p>
<p><i>SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES</i></p>	<p>Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls. Enhancement/s: None Specified</p>
<p><i>SA-9 EXTERNAL INFORMATION SYSTEM SERVICES</i></p>	<p>Control: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; Enhancement/s: (b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment:</p>



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

	organization-defined senior organizational official].
SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. Enhancement/s: None Specified.
SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. 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.

IA Policies, Procedures, and Standards Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 500 Director of National Intelligence, Chief Information Officer, 7 August 2008, Unclassified	Summary: This Intelligence Community (IC) Directive sets forth the authorities and responsibilities of the Chief information Officer of the Intelligence Community (Associate Director of National Intelligence/Chief Information Officer [ADNI/CIO]). The IC CIO is responsible for overseeing IC information security policies and practices for National



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

	Security Systems (NSS), in coordination with the Secretary of Defense or his or her designee, the Director of the Central Intelligence Agency (CIA), or his or her designee, or other heads of agencies operating NSS.
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 CIOs of the Department of Defense (DoD), the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). This policy 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.
ODNI/CIO-2008-108 Memorandum, Committee on National Security Systems (CNSS) Agreement to Use National Institutes of Standards and Technology (NIST) Documents as Basis for Information Security Controls and Risk Management, 20 April 2009, Unclassified	Summary: This IC CIO memorandum "...directs the National Security Community, including the IC and Department of Defense, to use the same baseline of standards, controls, and procedures to secure government information systems..."
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.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

Department of Defense (DoD)	
DoDD 5144.1 Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, 2 May 2005, Unclassified	The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (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; IT, including NSS; information resources management (IRM); spectrum management; network operations; information systems; IA; positioning, navigation, and timing (PNT) policy, including air, space, and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters. The ASD(NII)/DoD CIO is responsible for developing and maintaining the DoD IA program and associated policies, procedures, and standards. Additional responsibilities are to serve as the information architect for the DoD Enterprise information environment and provide oversight and policy guidance to ensure compliance with standards for developing, maintaining, and implementing sound integrated and interoperable architectures across the department, including intelligence systems and architectures.
DoDD 8000.01, Management of DoD Information Enterprise, 10 February 2009, Unclassified	Summary: This directive establishes the ASD(NII) with responsibility for providing standards for developing, maintaining, and implementing a DoD Enterprise architecture. It assigns responsibility to the DoD component CIOs to advise the ASD(NII)/DoD CIO and ensure that the policies and guidance issued by the ASD(NII)/DoD CIO are implemented, and contribute to the DoD strategic IRM plan.
DoDD 8500.01E Information Assurance, 23 April 2007, Unclassified	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.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

<p>DoDI 8500.2, Information Assurance (IA) Implementation, 6 February 2003, Unclassified</p>	<p>Summary: This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoDD 8500.1.</p>
<p>DoDD O-8530.1, Computer Network Defense (CND), 8 January 2001, Classified</p>	<p>See CGS Classified Annex.</p>
<p>DoDD 8570.01 Information Assurance Training, Certification and Workplace Management, certified current 23 April 2007, Unclassified</p>	<p>Summary: This instruction establishes policy and assigns responsibilities for DoD IA training, certification, and workforce management.</p>
<p>Committee for National Security Systems (CNSS)</p>	
<p>CNSSD 502 National Directive on Security of National Security Systems, 16 December 2004, Unclassified</p>	<p>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.</p>
<p>CNSSI 1253, Security Categorization and Control Selection for National Security Systems, October 2009, Unclassified</p>	<p>Summary: This policy provides all federal government departments, agencies, bureaus, and offices with a process for security categorization of NSS that collect, generate process, store, display, transmit, or receive National Security Information. This policy also references a comprehensive set of security controls and enhancements associated with the selection of the determined level of potential impact (or loss) to confidentiality, integrity, and availability that may be applied to any NSS developed and employed by the National Security Community. In addition, this policy provides tailoring guidance, so that Organizations may select a robust set of security controls to secure their NSS, based on assessed risk. This policy is the companion</p>



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

	document to NIST Special Publication (SP) 800-53.
CNSSI 1300, Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy, Under CNSSP-25, October 2009, Unclassified	Summary: This instruction provides a secure, interoperable electronic environment that closes the gap between the classified Federal Public Key Infrastructure (PKI), managed by the Federal PKI Policy Authority, and the highly classified IC PKI, managed by the Office of the Director of National Intelligence (ODNI). This instruction (Certificate Policy) states the requirements for issuing and managing certificates that Relying Parties can use in making decisions regarding what assurance they can place in a certificate issued by an NSS PKI Certificate Authority.
CNSSI 4009, National Information Assurance (IA) Glossary, 26 April 2010, Unclassified	Summary: This glossary provides definitions of IA terms used by the DoD, IC, and civil agencies for consistent terminology as those terms apply to their NSS.
CNSSP-15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems, 29 May 2010, Classified	See CGS Classified Annex
CNSSP-22, Information Assurance Risk Management Policy for National Security Systems, February 2009, Unclassified	Summary: This policy derives its authority from National Security Directive 42 (NSD 42), which outlines the roles and responsibilities for securing NSS, and applicable sections of the Federal Information Security Management Act (FISMA) of 2002.
CNSSP-24, Policy for Assured Information Sharing (AIS) for National Security Systems (NSS), May 2010, Unclassified	Summary: Pursuant to Executive Order 13256, the United States Government is responsible for sharing timely, secure information with decision-makers, intelligence analysis, warfighters, and policy-makers through a risk-managed approach among authorized U.S. entities. This policy establishes a framework for supporting AIS among



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

	Committee on National Security Systems (CNSS) members.
CNSSP-25, National Policy for Public Key Infrastructure in National Security Systems, March 2009, Unclassified	Summary: This policy establishes the requirement for all federal departments and agencies to have a PKI to manage and support their Secret and Unclassified NSS.
NSTISSP No. 11, Revised Fact Sheet National Information Assurance Acquisition Policy, July 2003, Unclassified	Summary: This policy establishes that COTS products acquired by U.S. government departments and agencies be subject to a standardized evaluation process, which will provide some assurances that these products perform as advertised. Accordingly, the policy provides a means of addressing this problem for those products acquired for national security applications.
Other Federal (OMB, NIST, ...)	
NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002, Unclassified	Summary: This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems.
Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010, Unclassified	Summary: The purpose of this publication is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. The guidelines have been developed: <ul style="list-style-type: none"> – To ensure that managing information system-related security risks is consistent with the organization’s mission/business objectives and overall risk strategy established by the senior leadership through the risk executive (function); – To ensure that information security requirements, including necessary security controls, are integrated into the organization’s enterprise architecture and system



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

	<p>development lifecycle processes;</p> <ul style="list-style-type: none"> – To support consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk management-related information, and reciprocity; and – To achieve more secure information and information systems within the federal government through the implementation of appropriate risk mitigation strategies.
NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 3, August 2009, Unclassified	<p>Summary: The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the Federal Government to meet the requirements of Federal Information Processing Standard (FIPS) 200.</p>
NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Revision, 1 June 2010, Unclassified	<p>Summary: This document is written to facilitate security control assessments conducted within an effective risk management framework. The assessment results provide organizational officials with:</p> <ul style="list-style-type: none"> • Evidence about the effectiveness of security controls in organizational information systems • An indication of the quality of the risk management processes employed within the organization • Information about the strengths and weaknesses of information systems that are supporting organizational missions and business functions in a global environment of sophisticated and changing threats.
Executive Branch (EO, PD, NSD, HSPD, ...)	
HSPD-12, Policies for a Common Identification Standard for Federal Employees and Contractors, 27 August 2004, Unclassified	<p>Summary: This directive mandates a federal standard for secure and reliable forms of identification to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy.</p>
NSD 42, National Policy	<p>Summary: This directive establishes initial objectives,</p>



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

<p>for the Security of National Security Telecommunications and Information Systems, 5 July 1990, Classified</p>	<p>policies, and an organizational structure to guide the conduct of activities to secure NSS from exploitation. It establishes a mechanism for policy development and dissemination and assigns responsibilities for implementation.</p>
<p>Executive Order 12333, United States Intelligence Activities, 30 July 2008, Unclassified</p>	<p>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.</p>
<p>Legislative</p>	
<p>FISMA, 44 U.S.C. §3544 and §3547, and 40 U.S.C. §11331, Unclassified</p>	<p>Summary: §3544 outlines the responsibilities for federal agencies' security responsibilities. §3547 outlines the responsibilities for federal agencies operating NSS. §11331(e) allows the head of an executive agency to apply more stringent standards for non-NSS than prescribed by NIST.</p>
<p>E-Government Act of 2002, P.L. 107-347, 17 December 2002, Unclassified</p>	<p>Summary: The E-Government Act amended the Clinger-Cohen Act that initially established federal Chief Information Officers (CIOs) who have a number of responsibilities including, but not limited to :</p> <ul style="list-style-type: none"> - Strategically planning for all information and information technology management functions; - Managing IT capital planning and investment; - Ensuring compliance with the requirement to protect information and systems; and - Ensuring that the agency implements and enforces a variety of federal laws including the Federal Records Act, Privacy Act, and Paperwork Reduction Act.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

IA Policies, Procedures, and Standards Capability Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICS 500-10 Intelligence Community Standard For Information Security Marking Metadata , 19 August 2008, Unclassified	See CGS Classified Annex.
ICS 500-1 Intelligence Community Standard for IC E-mail Encryption Policy Clarification and Standards for HCS and GAMMA Information, July 2007, Classified	See CGS Classified Annex
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, ...)	
FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, Unclassified	Summary: This publication addresses the development of standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal Government, promotes: (i) effective management and oversight of information security systems...; and (ii) consistent reporting ... on the adequacy and effectiveness of



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

	information security policies, procedures, and practices.
FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006, Unclassified	Summary: This standard addresses the specification of minimum security requirements for federal information and information systems.
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. Solution used for implementation—There needs to be a function by which to generate and distribute policies.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

2. Storage requirements—Policies need to be stored in a secure manner such that they are accessible when needed.
3. Lifecycle maintenance—Policies need to be reviewed, updated, and maintained.
4. Manpower to implement, maintain, and execute—The definition, review, and maintenance of policies requires the use of personnel.
5. Policy origin—Policy generation versus inheritance affects the overall cost structure.

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 IA Policies, Procedures, and Standards Capability.

- The IA policies, procedures, and standards define the Enterprise's vision, mission, and strategy. The Enterprise shall define, distribute, store, implement, enforce, review, and maintain policies, procedures, and standards, as needed. IA policies, procedures, and standards shall be defined by an Organization in accordance with national, DoD, and IC policies.
- Senior management policies shall be responsible for creating an IA program for the Enterprise.
- The Enterprise shall ensure that its policies, procedures, and standards enable interoperability between partnering organizations.
- The Enterprise shall identify existing Community and Organization policies, procedures, and standards to support reuse of higher-level and peer-level policies, where possible.
- The Enterprise shall define, distribute, store, implement, enforce, review, and maintain policies, procedures, and standards as applicable.
- The Enterprise shall establish an appropriate authority to define policies, procedures, and standards for the Organization and subordinate Enterprises.
- The Enterprise shall document the reason for defining each policy, procedure, or standard.
- The Enterprise shall document the alignment of Organizational policies, procedures, and standards with those issued at a higher level.
- The Enterprise shall determine at what level Organizational policies, procedures, and standards must exist and be implemented.
- The Enterprise shall store its policies, procedures, and standards through a centrally managed system.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

- The Enterprise shall provide a process for notifying interested parties of new policies, procedures, and standards.
- The Enterprise shall ensure old policies, procedures, and standards are archived based on Enterprise requirements.
- The Enterprise shall delegate responsibility to the appropriate personnel and groups for the implementation of policies, procedures, and standards.
- The Enterprise shall establish governance practices to ensure compliance with policies, procedures, and standards.
- The Enterprise shall provide the ability to identify higher-level, overarching policies (e.g., source and content) and analyze gaps.
- All IA policies, procedures, and standards shall undergo a periodic review process to address identified gaps and to ensure their continued effectiveness and applicability to technological advances.
- Changes to policies, procedures, and standards shall be implemented in a timely manner to align with Enterprise needs.
- Procedures and standards shall be reviewed and updated anytime policies or processes change.
- The frequency by which IA policies, procedures, and standards are reviewed shall be dictated by a standard set either by a high level Organization or by the Enterprise.
- The Enterprise's higher-level policies and standards shall create and define an IA policy.
- The Enterprise's higher-level policies and standards shall set Enterprise vision, mission, and strategy including defining the goals of the Enterprise.
- The Enterprise's higher-level policies and standards shall assign responsibilities.
- The Enterprise's higher-level policies and standards shall address compliance issues to establish: 1) the responsibilities assigned therein to various Enterprise components, and 2) the use of specified penalties and disciplinary actions.
- The Enterprise's policies, procedures, and standards shall address specific areas of concern for the Organization.
- The Enterprise's policies, procedures, and standards shall be updated frequently in accordance with Enterprise needs and as changes in technology and related factors take place.
- The Enterprise's policies, procedures, and standards shall contain an issue statement specifying applicability, role and responsibilities, compliance, and point of contact.



CGS IA Policies, Procedures, and Standards Capability



Version 1.1.1

- The Enterprise's policies, procedures, and standards shall focus on decisions made by management to protect a particular system.
- The Enterprise's policies, procedures, and standards shall be issued by an appropriate management official.
- The Enterprise's policies, procedures, and standards shall vary for different systems in accordance with operational needs.
- The Enterprise's policies, procedures, and standards shall be expressed as rules.
- All policies, procedures, and standards shall be supplemented by necessary supporting documents or guidance.
- All policies, procedures, and standards shall be visible to the Enterprise.
- All policies, procedures, and standards shall be supported by necessary management personnel.
- All policies, procedures, and standards shall be consistent with existing Enterprise directives, culture, guidance, and mission.