



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS System Protection Capability

Version 1.1.1

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.

07/30/2012



CGS System Protection Capability

Version 1.1.1



Table of Contents

1	Revisions	2
2	Capability Definition	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions.....	6
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations	7
7	Capability Interrelationships.....	8
7.1	Required Interrelationships	8
7.2	Core Interrelationships	9
7.3	Supporting Interrelationships.....	10
8	Security Controls	10
9	Directives, Policies, and Standards	25
10	Cost Considerations	30
11	Guidance Statements.....	31



CGS System Protection Capability



Version 1.1.1

1 Revisions

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



CGS System Protection 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.

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 capabilities such as Digital Policy Management, Configuration Management, Access Management, and Port Security. In addition, System Protection is responsible for employing malware defenses.

3 Capability Gold Standard Guidance

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

The System Protection Capability is focused on limiting the attack surface of Enterprise systems. Systems include an individual system itself or a system of systems (SoS). It provides the features and controls needed to protect the systems in the operating environment. As part of these protection mechanisms, various hardening techniques shall be employed, including layered and diverse defenses. All system security controls shall be assessed and authorized prior to system operation. System Protection requirements are driven by the mission needs and threat environment. Together, these shall determine the strength of the mechanism used for protection and the required level of assurance (confidence that the mechanism will work).

Hardware and software hardening begins during the acquisition activities of the system development lifecycle (see the Acquisition Capability for a more detailed description). During the acquisition process, considerations are made as to what functionality the system needs to possess to fulfill mission needs, and steps are taken to ensure that unnecessary services, modules, or devices are not included. If it is not possible to procure a system without the additional components, the Configuration Management



CGS System Protection Capability



Version 1.1.1

Capability shall be used to disable or remove components not required for mission needs and which fall outside of the Organization's established baselines. Configuration Management shall also provide pre-hardened baseline images for systems and will work with System Protection to employ self-testing checks at the operating system level, where available, for protection status.

The System Protection Capability shall employ Enterprise architects, which shall make the determination regarding which protections are required for both internal and remote Enterprise systems (including wireless devices). Information from the Risk Analysis, Understand Mission Flow, and Understand Data Flows Capabilities shall be used to make those determinations. This information shall be translated into digital policy (see the Digital Policy Management Capability) and distributed through the Configuration Management Capability to the applicable hardware and software components of the Enterprise systems.

Devices shall employ hardware detection, where possible, which allows the system to detect a change in the hardware modules, such as swapping out disk drives. Where possible, devices shall enforce a "whitelist," defined according to mission and policy needs, which will establish an acceptable list of hardware devices that may be connected to the system at any given time. This, along with protection mechanisms supplied by the Physical and Environmental Protections Capability, will prevent unauthorized modifications to the system hardware.

Software hardening consists of controlling software installation and execution as well as using established baselines and applying access controls. Again, whitelisting shall be employed to designate the critical software that is allowed (including applications) on all Enterprise systems. This information shall be maintained by the Configuration Management Capability.

For both hardware and software hardening, port security shall be employed. The Port Security Capability shall determine what ports, protocols, and services shall be allowed to pass to/from and through the system. The System Protection Capability shall enforce these rules by allowing only the authorized ports, protocols, and services to be used.

Malware defenses prevent malicious code from compromising systems. The System Protection Capability shall be responsible for employing malware defenses that are agile and enable timely updates. This includes protections from malicious code, phishing, and spam. Malware protection shall be deployed to any device for which



CGS System Protection Capability



Version 1.1.1

malware protection is commercially available or for which a custom product has been designed. The Configuration Management Capability shall include malware protection in its baselines. The System Protection Capability shall ensure that all applicable devices with signature-based malware detection are provided a connection to a signature repository (see Signature Repository Capability). Protection devices using methods other than signature detection shall also have access to an appropriate configuration repository. Automatic updates to the system shall be initiated once an update has been detected in the applicable repository. Not all updates will be provided immediately to the systems. Mission requirements shall dictate the update period; however, the time period shall allow for effective use of the updates (i.e., the updates are employed timely enough to prevent exposure).

Access management, including physical and logical access, is also a vital part of System Protection. The System Protection Capability relies on the Access Management Capability to make access decisions regarding who or what (users and non-human entities) may have access to all systems. The System Protection Capability shall enforce these access decisions within the system, preventing unauthorized access to internal system hardware and software. In addition to access management, the System Protection Capability shall work in coordination with the Physical and Environmental Protections Capability to restrict physical access to systems by providing locks, badging, access lists, and other facility protections.

Within the System Protection Capability, virtualization techniques shall be employed at the system level to limit the attack surface of systems (e.g., a hypervisor). This technique shall be employed such that applications running within one virtual machine (VM) will not corrupt applications running in another VM. All VMs shall be hardened in accordance with the guidance in this System Protection Capability. VMs shall also be able to return to a known good state in the event of an attack without impact to other VMs. Application virtualization (i.e., sandboxing) shall also be employed where sensitivity and mission needs require.

The System Protection Capability shall also enforce availability protections, such as in the form of redundant systems or by the use of clustering to promote high availability, among others. Mission needs will dictate the level of availability required for specific systems as specified in the Contingency Planning Capability.

In cases where the hardware or software components of the system cannot be configured to provide the protections in this Capability, supplemental controls or devices



CGS System Protection Capability



Version 1.1.1

shall be employed to provide the necessary protection. For example, a host firewall may be used to filter authorized communications between devices if the systems themselves are not able to carry out that function through port security or other means.

Accountability shall be ensured so that if anything unauthorized occurs, it can be traced back to the user or users who initiated the change. System Protection will employ auditing of systems activity. The logs shall be maintained within the Enterprise Audit Management Capability. These logs shall include information such as the identity of the entity performing the action, timestamps, and the events that took place, among others as defined by organizational policy. The logs shall be regularly moved to a centrally managed storage and processing system within Enterprise Audit Management. Logging needs shall be reevaluated regularly to ensure that all relevant information is being captured. In addition to keeping logs, all aspects of the security system shall be thoroughly documented. This documentation shall be kept up to date with each revision.

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. All critical software is security tested prior to deployment.
2. The necessary physical and environmental protections are in place.
3. Hardware and software baselines have been established and are known for all Enterprise devices and systems.
4. Risk decisions have been made to determine the appropriate protections to apply to a system.
5. Risk decisions have been made authorizing operations based on validation that appropriate protections have been applied to a system.
6. Systems are procured using approved processes that include provisions for security.
7. Access management and policy management functions 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.



CGS System Protection Capability



Version 1.1.1

1. The Capability has access to a signature repository or other configuration repository that keeps malware protections up to date.
2. The Capability enforces the protections provided by multiple Management Capabilities (i.e., Configuration Management, Access Management, Port Security, Risk Analysis, and Risk Mitigation).
3. The Capability prevents malicious code from executing on the systems.

6 Organizational Implementation Considerations

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

The Organization will provide proper System Protection for its networks, including full functional availability, integrity, confidentiality, authentication, non-repudiation, and access control for all relevant resources. The entire Capability will be built to be as automated as possible; unnecessary human interaction will be kept to a minimum for routine tasks. This will include automation for configuration updates, malicious code detection software, and predefined access management policies for the System Protection Capability to enforce.

The Organization will implement system hardening techniques, including defining secure configuration baselines, employing malware defenses, and enforcing digital policies set forth in the Digital Policy Management Capability. Where malware defenses are employed (not all software assets have an associated commercial off-the-shelf [COTS] or government off-the-shelf [GOTS] malware solution), the Organization will ensure that connection to an updated signature repository or other applicable configuration repository is maintained. All applicable assets will be notified in near real-time of a change to the appropriate repository, and the update itself will be distributed within a mission-defined timeframe.

Physical access to systems will be controlled within the Organization to ensure that unauthorized access is not obtained. This access will be ensured through the Access Management and Physical and Environmental Protections Capabilities.



CGS System Protection Capability



Version 1.1.1

The Organization will audit system activity across the Enterprise. The audit data will provide accountability for system actions and enable a more robust System Protection Capability. Although this audit activity will not provide real-time detection of events, the Organization will use this audit information for response, proactive identification of malicious activity, and other detection activities for the system.

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 System Protection Capability relies on the Network Mapping Capability to provide information about the location of network components that are in the Enterprise to provide appropriate protection.
- Understand Mission Flows—The System Protection Capability relies on the Understand Mission Flows Capability to provide information about mission needs, which drive protection requirements.
- Understand Data Flows—The System Protection Capability relies on the Understand Data Flows Capability to provide information about the data flows that occur within the Enterprise, which drive protection requirements.
- Software Inventory—The System Protection Capability relies on the Software Inventory Capability to provide information used to understand the scope of applying systems protections to software/application assets.
- Physical and Environmental Protections—The System Protection Capability relies on the Physical and Environmental Protections Capability to provide the necessary physical protection for the systems themselves.
- Network Access Control—The System Protection Capability relies on the Network Access Control Capability to provide endpoint compliance and enforcement to ensure all system protections are in place prior to granting access to a system on a network.



CGS System Protection Capability



Version 1.1.1

- Access Management–The System Protection Capability relies on the Access Management Capability to provide the authentication function on systems.
- Key Management–The System Protection Capability relies on the Key Management Capability to provide cryptographic keys that enable encryption and integrity checking between systems as well as between components and services within a single system.
- Architecture Reviews–The System Protection Capability relies on the Architecture Reviews Capability to assess the security controls of a system to ensure that information assurance (IA) concepts (e.g., confidentiality, integrity, availability, authentication, and non-repudiation) are present in Enterprise architecture requirements.
- Deployment–The System Protection Capability relies on the Deployment Capability to test that protection mechanisms are implemented appropriately prior to the system becoming operational.

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 System Protection Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The System Protection Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The System Protection Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The System Protection Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The System Protection Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.



CGS System Protection 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.

- Host Intrusion Detection–The System Protection Capability relies on the Host Intrusion Detection Capability as an added layer of defense in defending systems.
- Host Intrusion Prevention–The System Protection Capability relies on the Host Intrusion Prevention Capability as an added layer of defense in defending systems.
- Risk Analysis–The System Protection Capability establishes protection mechanisms that are part of an accredited system and documented as such through a certification and accreditation process conducted by the Risk Analysis Capability.
- Risk Mitigation–The System Protection Capability relies on the Risk Mitigation Capability to establish the necessary safeguards to ensure the continued security of the Enterprise.
- Acquisition–The System Protection Capability relies on the Acquisition Capability to ensure that security is inherent to the system, to the extent possible. This enables the Organization to obtain a semi-hardened system, which may be further hardened according to the System Protection Capability.

8 Security Controls

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

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	
AC-2 ACCOUNT MANAGEMENT	Control: The organization manages information system accounts, including: e. Establishing, activating, modifying, disabling, and removing accounts; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; Enhancement/s:



CGS System Protection Capability



Version 1.1.1

	<p>(1) The organization employs automated mechanisms to support the management of information system accounts.</p> <p>(2) The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].</p> <p>(3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period].</p> <p>(4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.</p> <p>(5) The organization:</p> <p>(a) Requires that users log out when [Assignment: organization defined time-period of expected inactivity and/or description of when to log out];</p> <p>(b) Determines normal time-of-day and duration usage for information system accounts;</p> <p>(c) Monitors for atypical usage of information system accounts; and</p> <p>(d) Reports atypical usage to designated organizational officials.</p>
<p>AC-7 UNSUCCESSFUL LOGIN ATTEMPTS</p>	<p>Control: The information system:</p> <p>a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period]; and</p> <p>b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.</p> <p>Enhancement/s:</p> <p>(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.</p> <p>(2) The information system provides additional protection for mobile devices accessed via login by purging information from</p>



CGS System Protection Capability



Version 1.1.1

	<p>the device after [Assignment: organization-defined number] consecutive, unsuccessful login attempts to the device.</p>
<p>AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION</p>	<p>Control: The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).</p> <p>Enhancement/s:</p> <p>(1) The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.</p> <p>(2) The information system notifies the user of the number of [Selection: successful logins/accesses; unsuccessful login/access attempts; both] during [Assignment: organization-defined time period].</p> <p>(3) The information system notifies the user of [Assignment: organization-defined set of security-related changes to the user's account] during [Assignment: organization-defined time period].</p>
<p>AC-10 CONCURRENT SESSION CONTROL</p>	<p>Control: The information system limits the number of concurrent sessions for each system account to [Assignment: organization-defined number].</p> <p>Enhancement/s: None Specified</p>
<p>AC-11 SESSION LOCK</p>	<p>Control: The information system:</p> <p>a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and</p> <p>b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.</p> <p>Enhancement/s:</p> <p>(1) The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.</p>
<p>AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION</p>	<p>Control: The organization:</p> <p>a. Identifies specific user actions that can be performed on the information system without identification or authentication; and</p> <p>b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.</p>



CGS System Protection Capability



Version 1.1.1

	<p>Enhancement/s:</p> <p>(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.</p>
<p><i>AC-17 REMOTE ACCESS</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. <p>Enhancement/s:</p> <p>(7) The organization ensures that remote sessions for accessing [Assignment: organization-defined list of security functions and security-relevant information] employ [Assignment: organization-defined additional security measures] and are audited.</p> <p>(8) The organization disables [Assignment: organization-defined networking protocols within the information system deemed to be nonsecure] except for explicitly identified components in support of specific operational requirements.</p>
<p><i>AC-19 ACCESS CONTROL FOR MOBILE DEVICES</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> g. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures
<p><i>CM-2 BASELINE CONFIGURATION</i></p>	<p>Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.</p> <p>Enhancement/s:</p> <p>(4) The organization:</p> <ul style="list-style-type: none"> (a) Develops and maintains [Assignment: organization-defined list of software programs not authorized to execute on the information system]; and



CGS System Protection Capability



Version 1.1.1

	<p>(b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.</p> <p>(5) The organization:</p> <p>(a) Develops and maintains [Assignment: organization-defined list of software programs authorized to execute on the information system]; and</p> <p>(b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.</p>
<p>CM-5 ACCESS RESTRICTIONS FOR CHANGE</p>	<p>Control: The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.</p> <p>Enhancement/s:</p> <p>(7) The information system automatically implements [Assignment: organization-defined safeguards and countermeasures] if security functions (or mechanisms) are changed inappropriately.</p>
<p>CM-7 LEAST FUNCTIONALITY</p>	<p>Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services].</p> <p>Enhancement/s:</p> <p>(1) The organization reviews the information system [Assignment: organization-defined frequency] to identify and eliminate unnecessary functions, ports, protocols, and/or services.</p> <p>(2) The organization employs automated mechanisms to prevent program execution in accordance with [Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage].</p> <p>(3) The organization ensures compliance with [Assignment: organization-defined registration requirements for ports, protocols, and services].</p>
<p>MA-4 NON-LOCAL</p>	<p>Control: The organization:</p>



CGS System Protection Capability



Version 1.1.1

<p><i>MAINTENANCE</i></p>	<p>e. Terminates all sessions and network connections when non-local maintenance is completed.</p> <p>Enhancement/s:</p> <p>(3) The organization:</p> <p>(b) Removes the component to be services from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.</p>
<p><i>MA-5 MAINTENANCE PERSONNEL</i></p>	<p>Enhancement/s:</p> <p>(1b) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed of physically disconnected from the system and secured.</p>
<p><i>MP-6 MEDIA SANITIZATION</i></p>	<p>Enhancement/s:</p> <p>(3) The organization sanitized portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined list of circumstances requiring sanitization of portable, removable, storage devices].</p>
<p><i>PL-2 SYSTEM SECURITY PLAN</i></p>	<p>Control: The organization:</p> <p>a. Develops a security plan for the information system that:</p> <ul style="list-style-type: none"> - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the



CGS System Protection Capability



Version 1.1.1

	<p>system;</p> <ul style="list-style-type: none"> - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; <p>b. Reviews the security plan for the information system [Assignment: organization-defined frequency]; and</p> <p>c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.</p> <p>Enhancement/s:</p> <p>(1) The organization:</p> <ul style="list-style-type: none"> (a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and (b) Reviews and updates the CONOPS [Assignment: organization-defined frequency]. <p>Enhancement Supplemental Guidance: The security CONOPS may be included in the security plan for the information system.</p> <p>(2) The organization develops a functional architecture for the information system that identifies and maintains:</p> <ul style="list-style-type: none"> (a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface; (b) User roles and the access privileges assigned to each role; (c) Unique security requirements; (d) Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and (e) Restoration priority of information or information system services.
SA-5 INFORMATION	Control: The organization:



CGS System Protection Capability



Version 1.1.1

<p><i>SYSTEM DOCUMENTATION</i></p>	<p>b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:</p> <ul style="list-style-type: none"> - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; <p>Enhancement/s:</p> <p>(1) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacture documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.</p> <p>(2) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacture documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.</p> <p>(3) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacture documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.</p> <p>(4) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacture documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.</p> <p>(5) The organization obtains, protects as required, and makes available to authorized personnel, the source code for the information system to permit analysis and testing.</p>
<p><i>SA-7 USER-INSTALLED</i></p>	<p>Control: The organization enforces explicit rules governing the installation of software by users.</p>



CGS System Protection Capability



Version 1.1.1

SOFTWARE	Enhancement/s: None Specified
SA-14 CRITICAL INFORMATION SYSTEM COMPONENTS	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Determines [Assignment: organization-defined list of critical information system components that require re-implementation]; and b. Re-implements or custom develops such information system components. <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The organization: <ul style="list-style-type: none"> (a) Identifies information system components for which alternative sourcing is not viable; and (b) Employs [Assignment: organization-defined measures] to ensure that critical security controls for the information system components are not compromised.
SC-2 APPLICATION PARTITIONING	<p>Control: The information system separates user functionality (including user interface services) from information system management functionality.</p> <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The information system prevents the presentation of information system management-related functionality at an interface for general (i.e., non-privileged) users.
SC-3 SECURITY FUNCTION ISOLATION	<p>Control: The information system isolates security functions from non-security functions.</p> <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The information system implements underlying hardware separation mechanisms to facilitate security function isolation. (2) The information system isolates security functions enforcing access and information flow control from both non security functions and from other security functions. (3) The organization implements an information system isolation boundary to minimize the number of non-security functions included within the boundary containing security functions. (4) The organization implements security functions as largely independent modules that avoid unnecessary interactions between modules. (5) The organization implements security functions as a layered structure minimizing interactions between layers of the design



CGS System Protection Capability



Version 1.1.1

	and avoiding any dependence by lower layers on the functionality or correctness of higher layers.
SC-4 <i>INFORMATION IN SHARED RESOURCES</i>	Control: The information system prevents unauthorized and unintended information transfer via shared system resources. Enhancement/s: (1) The information system does not share resources that are used to interface with systems operating at different security levels.
SC-6 <i>RESOURCE PRIORITY</i>	Control: The information system limits the use of resources by priority. Enhancement/s: None Specified
SC-14 <i>PUBLIC ACCESS PROTECTIONS</i>	Control: The information system protects the integrity and availability of publicly available information and applications. Enhancement/s: None Specified
SC-15 <i>COLLABORATIVE COMPUTING DEVICES</i>	Control: The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices. Enhancement/s: (1) The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use. (2) The information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers. (3) The organization disables or removes collaborative computing devices from information systems in [Assignment: organization-defined secure work areas].
SC-16 <i>TRANSMISSION OF SECURITY ATTRIBUTES</i>	Control: The information system associates security attributes with information exchanged between information systems. Enhancement/s: (1) The information system validates the integrity of security attributes exchanged between systems.
SC-18 <i>MOBILE</i>	Control: The organization:



CGS System Protection Capability



Version 1.1.1

<p><i>CODE</i></p>	<p>a. Defines acceptable and unacceptable mobile code and mobile code technologies;</p> <p>b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and</p> <p>c. Authorizes, monitors, and controls the use of mobile code within the information system.</p> <p>Enhancement/s:</p> <p>(1) The information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.</p> <p>(2) The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets [Assignment: organization-defined mobile code requirements].</p> <p>(3) The information system prevents the download and execution of prohibited mobile code.</p> <p>(4) The information system prevents the automatic execution of mobile code in [Assignment: organization-defined software applications] and requires [Assignment: organization-defined actions] prior to executing the code.</p>
<p><i>SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE</i></p>	<p>Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.</p> <p>Enhancement/s: None Specified.</p>
<p><i>SC-25 THIN NODES</i></p>	<p>Control: The information system employs processing components that have minimal functionality and information storage.</p> <p>Enhancement/s: None Specified.</p>
<p><i>SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS</i></p>	<p>Control: The information system includes: [Assignment: organization-defined operating system-independent applications].</p> <p>Enhancement/s: None Specified.</p>
<p><i>SC-29 HETEROGENEITY</i></p>	<p>Control: The organization employs diverse information technologies in the implementation of the information system.</p>



CGS System Protection Capability



Version 1.1.1

	Enhancement/s: None Specified.
SC-30 <i>VIRTUALIZATION TECHNIQUES</i>	Control: The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations. Enhancement/s: (1) The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency]. (2) The organization employs randomness in the implementation of the virtualization techniques.
SC-31 <i>COVERT CHANNEL ANALYSIS</i>	Control: The organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels. Enhancement/s: (1) The organization tests a subset of the vendor-identified covert channel avenues to determine if they are exploitable.
SC-32 <i>INFORMATION SYSTEM PARTITIONING</i>	Control: The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. Enhancement/s: None Specified.
SC-34 <i>NON-MODIFIABLE EXECUTABLE PROGRAMS</i>	Control: The information system at [Assignment: organization-defined information system components]: a. Loads and executes the operating environment from hardware-enforced, read-only media; and b. Loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media. Enhancement/s: The organization employs [Assignment: organization-defined information system components] with no writeable storage that is persistent across component restart or power on/off. (2) The organization protects the integrity of the information on read-only media.
SI-3 <i>MALICIOUS CODE PROTECTION</i>	Control: The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect



CGS System Protection Capability



Version 1.1.1

	<p>and eradicate malicious code:</p> <ul style="list-style-type: none"> - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; <p>b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;</p> <p>c. Configures malicious code protection mechanisms to:</p> <ul style="list-style-type: none"> - Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and - [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and <p>Enhancement/s:</p> <p>(3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.</p>
<p>SI-6 SECURITY FUNCTIONALITY VERIFICATION</p>	<p>Control: The information system verifies the correct operation of security functions [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.</p> <p>Enhancement/s:</p> <p>(1) The information system provides notification of failed automated security tests.</p> <p>(2) The information system provides automated support for the management of distributed security testing.</p> <p>(3) The organization reports the result of security function verification to designated organizational officials with information security responsibilities.</p>



CGS System Protection Capability



Version 1.1.1

<p>SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS</p>	<p>Control: The information system at [Assignment: organization-defined information system components]:</p> <ul style="list-style-type: none"> a. Loads and executes the operating environment from hardware-enforced, read-only media; and b. Loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media. <p>Enhancement/s:</p> <p>The organization employs [Assignment: organization-defined information system components] with no writeable storage that is persistent across component restart or power on/off.</p> <p>(2) The organization protects the integrity of the information on read-only media.</p>
<p>SI-3 MALICIOUS CODE PROTECTION</p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: <ul style="list-style-type: none"> - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: <ul style="list-style-type: none"> - Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and - [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and <p>Enhancement/s:</p> <p>(3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.</p>



CGS System Protection Capability



Version 1.1.1

<p>SI-6 SECURITY FUNCTIONALITY VERIFICATION</p>	<p>Control: The information system verifies the correct operation of security functions [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.</p> <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The information system provides notification of failed automated security tests. (2) The information system provides automated support for the management of distributed security testing. (3) The organization reports the result of security function verification to designated organizational officials with information security responsibilities.
<p>SI-7 SOFTWARE AND INFORMATION INTEGRITY</p>	<p>Control: The information system detects unauthorized changes to software and information.</p> <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The organization reassesses the integrity of software and information by performing [Assignment: organization-defined frequency] integrity scans of the information system. (2) The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification. (3) The organization employs centrally managed integrity verification tools. (4) The organization requires use of tamper-evident packaging for [Assignment: organization-defined information system components] during [Selection: transportation from vendor to operational site; during operation; both].
<p>SI-8 SPAM PROTECTION</p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature



CGS System Protection Capability



Version 1.1.1

	<p>definitions) when new releases are available in accordance with organizational configuration management policy and procedures.</p> <p>Enhancement/s:</p> <p>(1) The organization centrally manages spam protection mechanisms.</p> <p>(2) The information system automatically updates spam protection mechanisms (including signature definitions).</p>
<p>SI-9 <i>INFORMATION INPUT RESTRICTIONS</i></p>	<p>Control: The organization restricts the capability to input information to the information system to authorized personnel.</p> <p>Enhancement/s: None Specified.</p>

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.

System Protection Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Intelligence Community Public Key Infrastructure (PKI) Overarching Policy for the SCI Fabric, 25 October 1999, Classified	Summary: It is the policy of the Intelligence Community (IC) that a single-root, hierarchical Public Key Infrastructure (PKI) be established for use on Sensitive Compartmented Information (SCI) networks between members of the Community. The IC PKI will provide IC member Organizations, for those applications that require them, strong identification and authentication, data integrity, digital signature, non-repudiation, and encryption services for all information system-based communications and services traversing Community SCI networks. These services shall be used for communications and services between IC member Organizations and those Organizations and their customers.
Intelligence Community Certificate Policy, Version 4.3.3, 25 September 2008, Classified	Summary: This document provides uniform policy guidance and requirements for ensuring interoperability between Certification Authorities (CAs) within the IC PKI. It establishes standard operating policies and procedures to



CGS System Protection Capability



Version 1.1.1

	<p>be used by IC agencies/components for services between members of the U.S. IC, IC customers, and others as approved by the Information and Technology Governance Board (ITGB) and the Intelligence Community Chief Information Officer (IC CIO). IC PKI public certificates and associated private keys have applicability to areas such as, but not limited to, confidentiality of information, digital signatures, and identification and authentication of individuals, as well as information system infrastructure components.</p>
<p>ICPM 2007-500-3, Intelligence Information Sharing, 22 December 2007, Unclassified,</p>	<p>Summary: Policy: To maximize the dissemination of intelligence information to IC customers relevant to their missions, while balancing the obligation to protect intelligence sources and methods, the IC elements shall ...</p> <p>b. Implement DNI approved information technology, personnel/physical security standards, and procedures for providing and protecting intelligence information.</p>
<p>Comprehensive National Cybersecurity Initiative (CNCI)</p>	
<p>NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified</p>	<p>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.</p>
<p>Department of Defense (DoD)</p>	
<p>DoD 5200.1-R, Information Security Program, 14 January 1997, Unclassified</p>	<p>Summary: This document establishes the Department of Defense (DoD) Information Security Program to promote proper and effective classification, protection, and downgrading of official information requiring protection in the interest of the national security. It provides guidance and references addressing protection of automated information systems and networks.</p>
<p>DoDD 8000.01, Management of the DoD Information Enterprise, 10 February 2009,</p>	<p>Summary: It is DoD policy that:</p> <p>a. Information shall be considered a strategic asset to the Department of Defense; it shall be appropriately secured, shared, and made available throughout the information life</p>



CGS System Protection Capability



Version 1.1.1

<p>Unclassified</p>	<p>cycle to any DoD user or mission partner to the maximum extent allowed by law and DoD policy. ... d. Information solutions shall provide reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities, natural disasters, and accidents.</p>
<p>DoDD 8500.01E, Information Assurance, 23 April 2007, Unclassified</p>	<p>Summary: All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflects a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction on the DoD information system; and cost effectiveness.</p>
<p>DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 1 April 2004, Unclassified</p>	<p>Summary: This instruction implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a department-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption. It aligns DoD PKI and PK-enabling activities with DoD Directive 8500.1, as implemented by DoD Instruction 8500.2, and the DoD Common Access Card (CAC) Program, as specified by DoD Directive 8190.3.</p>
<p>DoDI 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense, 8 June 2010, Unclassified</p>	<p>Summary: This instruction establishes that all DoD-owned or controlled space systems, regardless of their mission assurance category or confidentiality level, must comply with the specified procedures which cover communications processes, use of cryptography, and other information assurance (IA) considerations.</p>
<p>CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified</p>	<p>Summary: This instruction provides joint policy and guidance for IA and Computer Network Defense (CND) operations. Policy includes that Communications Security (COMSEC) material and techniques will be used to safeguard communications and communications systems.</p>
<p>DISA Network Infrastructure Security</p>	<p>Summary: This Security Technical Implementation Guide (STIG) provides security considerations at the network</p>



CGS System Protection Capability



Version 1.1.1

Technical Implementation Guide (STIG), version 7.1, 25 October 2007, Unclassified	level needed to achieve an acceptable level of risk for information as it is transmitted through an enclave. It was developed to enhance the confidentiality, integrity, and availability of sensitive DoD automated information systems.
DISA Enclave Security Technical Implementation Guide (STIG), version 4.2, 10 March 2008, Unclassified	Summary: This STIG provides Organizations an overview of the applicable policy and additional STIG documents required to implement secure information systems and networks while ensuring interoperability.
Committee for National Security Systems (CNSS)	
CNSSP-12, National Information Assurance Policy for Space Systems Used to Support National Security Missions, 20 March 2007, Unclassified	Summary: Applicable space systems shall all comply with the specified set of IA requirements including considerations for IA throughout the lifecycle of a product, compliance with the Federal Information Security Management Act, and use of National Security Agency (NSA) approved cryptographic methods.
CNSSP-21, National Information Assurance Policy on Enterprise Architectures for National Security Systems, March 2007, Unclassified	Summary: Federal department and agency Enterprise architectures (EA) shall integrate IA capabilities to mitigate risks associated with national security information. Security controls shall be incorporated at the component, system, service, and application levels of EAs, including plans to manage risk, protect privacy, and provide availability, integrity, authentication, confidentiality, and non-repudiation as part of an integrated IA approach.
Other Federal (OMB, NIST, ...)	
OMB Memo M-08-22, Guidance on the Federal Desktop Core Configuration (FDCC), Unclassified	Summary: This memo provides guidance for the application of the Federal Desktop Core Configuration (FDCC). Agencies employing applicable operating systems are required to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the DoD, and the Department of Homeland Security (DHS).
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	



CGS System Protection Capability



Version 1.1.1

Legislative	
Public Law 107-347, E.-Government Act, 17 December 2002, Unclassified	Summary: This Public Law was enacted to enhance the management and promotion of electronic government services and processes. It requires the development of EAs within and across the Federal Government, and the provision of information security protections commensurate with the risk and magnitude of the harm resulting from information systems' corruption. It is divided into five titles. The Federal Information Security Management Act of 2002 was enacted as Title III of the E-Government Act. The act recognized the importance of information security to the economic and national security interests of the United States and requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

System Protection Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Intelligence Community Public Key Infrastructure (PKI) Interface Specification (Draft), Version 2.9.4, September 2009, Classified	Summary: This document describes the interfaces to the IC PKI, defines the interface requirements for creating X.509 Version 3 (V3) certificates and X.509 Version 2 (V2) Certificate Revocation Lists (CRLs), provides a baseline for IC PKI certificate profiles (largely mirroring those of the DoD's PKI certificate profiles), and establishes the content for PKI certificates.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Joint DoDIIS /Cryptologic	Summary: This document provides procedural guidance for



CGS System Protection Capability



Version 1.1.1

SCI Information Systems Security Standards, Revision 4, 1 January 2006, Unclassified	the protection, use, management, and dissemination of SCI. The combination of security safeguards and procedures used for information systems shall achieve U.S. government policy that all classified information must be appropriately safeguarded to assure the confidentiality, integrity, and availability of that information.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996, Unclassified	Summary: This special publication (SP) presents generally accepted system security principles and common practices that are used in securing information technology 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



CGS System Protection Capability



Version 1.1.1

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—This Capability will require, among other things, software that performs virtualization services, system imaging, and malware scanning.
2. Necessary licensing—Commercial malware and virtualization software will require licensing agreements.

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 System Protection Capability.

- System Protection is a broader security capability that is focused on hardware and software (including applications) hardening and enforcement of related protection policies.
- The Enterprise shall use various hardening techniques to protection systems, including layered and diverse defenses.
- All system security controls shall be assessed and authorized prior to system operation.
- System protection requirements shall be driven by mission needs and threat environment. Together, these shall determine the strength of the mechanism used for protection and the required level of assurance (confidence that the mechanism will work).
- During the acquisition process for resources, the Enterprise shall determine what functionality the system needs to possess and shall take the necessary steps to ensure that non-required services, modules, and devices are not included, when possible.



CGS System Protection Capability



Version 1.1.1

- The Enterprise shall perform configuration management to establish configuration baselines and ensure that unnecessary components are removed or disabled on systems.
- The Enterprise shall use configuration management services to perform self-testing checks of systems at the operating system level.
- The Enterprise shall control the software that can be installed and executed on Enterprise systems.
- Enterprise architects shall determine the protections that are required for all Enterprise systems, including remote and wireless devices.
- Digital policies that describe and enforce security policy shall be distributed throughout the Enterprise using a configuration management system.
- Devices shall employ hardware detection, where possible, which allows the system to detect a change in the hardware modules, such as swapping out disk drives.
- Devices shall enforce a “whitelist,” where possible, which is defined according to mission and policy needs and establishes an acceptable list of hardware devices that may be connected to the system at any given time. This, along with other protection mechanisms, will prevent unauthorized modifications to the system hardware.
- Only authorized ports, protocols, and services shall be used to pass to/from and through the system.
- Malware defenses shall be deployed on all devices, where possible, including protections against malicious code, phishing, and spam. Malware protection shall be deployed to any device for which malware protection is commercially available or for which a custom product has been designed.
- All protection systems shall ensure that all applicable devices with signature-based malware detection are provided a connection to a signature repository or appropriate configuration repository, as necessary.
- The Enterprise shall enforce access management decisions, preventing unauthorized access to internal system resources.
- Appropriate physical protection mechanisms shall be in place to guard against unauthorized physical access to systems and resources.
- The Enterprise shall employ the use of appropriate virtualization technologies to limit the attack surface of systems. This technique shall be employed such that applications running within one VM will not corrupt applications running in another VM.



CGS System Protection Capability



Version 1.1.1

- All systems shall adhere to their availability requirements as dictated by mission needs.
- Logs of system and user activity shall be maintained and audited to ensure the identification and accountability for unauthorized activity.
- The logs shall be regularly moved to a centrally managed storage and processing system within the Enterprise.
- Logging needs shall be reevaluated regularly to ensure that all relevant information is being captured.