



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Configuration Management Capability

Version 1.1.1

The Configuration Management Capability comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configuration of those products and systems. Configuration Management focuses on Secure Configuration Management and Patch Management to provide assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications.

07/30/2012



CGS Configuration Management 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.....	8
5	Capability Post-Conditions.....	9
6	Organizational Implementation Considerations	9
7	Capability Interrelationships.....	13
7.1	Required Interrelationships	13
7.2	Core Interrelationships	14
7.3	Supporting Interrelationships.....	14
8	Security Controls	16
9	Directives, Policies, and Standards	23
10	Cost Considerations	29
11	Guidance Statements.....	30



CGS Configuration Management 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 Configuration Management 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 Configuration Management Capability comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configuration of those products and systems. In addition, Configuration Management starts with the establishment of a baseline and provides management of security features and assurances through control of changes made to hardware, firmware, software, and documentation to protect the information system against improper modifications during the system development lifecycle. Continuous monitoring, remediation, and reporting of system configurations are necessary for a successful Configuration Management program. Configuration Management focuses on Secure Configuration Management and Patch Management to provide assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. Configuration Management provides the following focus and capabilities:

1. Secure Configuration Management is the management and control of configurations for an information system with the goal of enabling security and managing risk. Secure Configuration Management applies the general concepts, processes, and activities of Configuration Management but with a focus on the outcomes that affect the security posture of the information system.
2. Patch Management employs a process to maintain systematic notification, identification, deployment, installation, and verification of operating system (OS) and application software code revisions as well as hardware and firmware. The revisions are known by terms such as updates, patches, hot fixes, and service packs.

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 Configuration Management Capability



Version 1.1.1

The Configuration Management Capability provides management of workstations, servers, network devices, and other configurable devices to provide security features and assurances through control of changes made to hardware, firmware, and software (including code) to protect the information system against improper modifications during the system operation and development lifecycle. Configuration of assets is performed only by authorized users or processes. Missions shall not be adversely affected by configuration changes. Continuous monitoring, remediation, and reporting of system configurations are necessary for a successful Configuration Management program.

Enterprise-wide, the Configuration Management Capability focuses on Secure Configuration Management and ties into the overall comprehensive Configuration Management. The Configuration Management Capability, in general, establishes baselines, deploys the configurations, monitors against the baseline (verifies that deployed devices meet the baseline), remediates, and provides periodic reviews to update baselines based on changes in environment. As part of the configuring process, the Secure Configuration Management process identifies four procedures that shall be defined for each project to ensure that a sound Secure Configuration Management process is implemented. The four procedures are configuration identification, configuration control, configuration status accounting, and configuration audits. These terms and definitions change from standard to standard but are essentially the same.

Where possible, all Enterprise systems and devices shall be in compliance with the approved configuration baseline. When mission needs dictate that certain systems deviate from the baseline, that deviation shall be appropriately documented in accordance with Enterprise policy. This documentation shall include the reason for the required deviation, the mission and project the system supports, and what the custom configuration entails. Special consideration may be granted for specialized environments, such as those used for development, testing, laboratories, or other mission needs.

The Configuration Management Capability detects changes in the asset database, which houses the hardware device and software inventories of all Enterprise assets. When the Configuration Management Capability detects a change in the inventory, it determines whether the change is in compliance with the approved configuration baseline or associated with an approved product. If Configuration Management determines that the change is not in compliance with the baseline, it makes the necessary modifications to the affected asset. This modification causes an update in the hardware device or software inventory (see the Hardware Device Inventory and



CGS Configuration Management Capability



Version 1.1.1

Software Inventory Capabilities). The Software Inventory Capability also maintains the software repository where software assets are held.

The Configuration Management Capability comprises a collection of activities focused on establishing and maintaining the integrity of products and systems. The practice of Configuration Management is implemented by establishing the baseline through planning, configuring, maintaining, and monitoring.

Planning:

1. Establishes a baseline for workstations, servers, network devices, and other configurable devices as well as a baseline for locks, guards, and doors as provided under the Physical and Environmental Protection Capability. Establishes an approved baseline and provides standard software, standard configurations, and standard OS based on Organization mission and policy.
2. Establishes a plan detailing how to conduct Configuration Management; the roles and responsibilities within the Configuration Management process, including the Configuration Control Board (CCB); authorities; execution elements; timelines; and the change process, which explains how changes are implemented. The plan also details automated tools available to demonstrate completion of the process, periodicity, and standard of acceptable deviation, which can leverage Community standards that can use standardized tools. In addition, the plan defines who is allowed to make changes based on type of change (system admin, security admin, and user), and how to maintain, authorize, and monitor the changes.
3. Establishes that as part of the planning process, the Configuration Management office overseeing all activities shall ensure that the baselines are deployed in a standardized, coordinated methodology using technologies defined as acceptable by the Organization's policies.
4. Establishes that the Configuration Management Plan is kept on a separate network from the devices being managed and protected by the System Protection and Data Protection Capabilities.
5. Identifies and documents the performance, functional, and physical characteristics of a configuration item.

Configuring:

1. Ensures that all information needed from the CGS Capabilities under the Know the Enterprise Capability Area is documented and available.



CGS Configuration Management Capability



Version 1.1.1

2. Configures and establishes baselines for all configurable devices, even those that have multiple baselines and are initially coordinated and deployed by an engineering staff/department (can be based on digital policies in the Digital Policy Management).
3. Ensures that baselines are monitored monthly and will be changed and configured as a result of patch management. System administrators will be notified before any deployment to ensure little or no mission impact. Testing will be completed before any deployment for every change, no matter how minor.
4. Ensures that preinstalled OS services will be verified as to whether they are needed, disabled, unneeded, and unused as part of the initial baseline configuration. All systems shall be hardened in accordance with the System Protection and Port Security Capabilities.
5. Ensures that dedicated configuration repositories are used to store and protect secure baseline configurations. The secure baseline configurations are disseminated directly from these repositories. Configuration repositories shall maintain high levels of confidentiality, integrity, and availability.

Maintaining:

1. Engineering staff manages updates, performs remediation, and maintains the baseline in accordance with authorized and approved changes. These activities all occur in a controlled and secure environment (secure storage).
2. Updates and changes are documented to ensure that the test processes are repeatable and that every change is handled the same way through the same change control process.
3. Levels of impact of change are recognized and defined according to American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) 649 and Configuration Management Military Standard (Mil-Std) 61A, as part of maintaining the baseline. These documents define the process used to facilitate orderly management of product information and product changes for beneficial purposes such as to revise a capability; improve performance, reliability, or maintainability; extend life; reduce cost; reduce risk and liability; or correct defects. In addition, these documents provide guidance on assessing the potential effects of a change and coordinating the impacts with the impacted areas of responsibility. The impact assessment evaluates the effects of the proposed change and ensures that all potential effects are identified. Personnel in the impacted areas of responsibility normally possess the specific detailed knowledge required for an accurate assessment.



CGS Configuration Management Capability



Version 1.1.1

Monitoring:

1. Verifies that the deployed device meets the baseline by periodically auditing the configuration (physical and functional) across the entire Enterprise to verify conformance with specifications, interface control documents, and other requirements. It records and reports information needed to manage configuration items effectively, including the status of proposed changes and implementation status of approved changes.
2. Provides system assessment and continuous monitoring so that strategic decisions can be made to determine whether current configuration can be improved upon.
3. Could be near real-time, depending on system criticality and available technology, such that if a system goes out of compliance, notification is sent automatically for analysis and response and provides input to the validated tool as well as to an automated risk analysis tool.

A patch is any change to software or firmware, such as OSs. Patches include vendor patches for security-related reasons and affect all systems that are part of the Enterprise. The Configuration Management Capability provides patch management by the notification of patch availability in a timely automated or manual manner, providing applicability assessment, testing, planning, deployment, and a review process:

1. Notification—Notification includes notice of patch availability in a timely automated or manual notification between vendor and customer. Manual notification will be provided when automated notification is not available. The security administrator receives notification, which includes information as to the fix and how to verify whether the information is correct. In addition, the notification consists of a description of the vulnerability and the mission criticality.
2. Applicability Assessment—During application assessment, applications are identified to determine the appropriate software/firmware patch based on a trusted source inventory, and obtained from that inventory. Applicability and other operational attributes are reviewed by the security administrator to make an informed risk decision on both the original software/firmware and the patch. Necessity for the patch is prioritized.
3. Testing—Patches are tested end-to-end in a nonproduction, segmented environment that mirrors, as closely as possible, the current operational environment, to determine impact to other subsystems, and patch stability. Regression testing, documentation validation, configuration settings, and interoperability issues are part of the testing. Testing will be prioritized and completed in a timely manner to meet schedule requirements. Testing shall confirm that if a rollback is required, it has been tested to ensure it is operational and the security administrator has been



CGS Configuration Management Capability



Version 1.1.1

informed of progress. If it is determined that the patch cannot be applied, a determination will be made whether the system will remain unpatched or whether an alternative mitigation will be employed. Considerations need to be made to balance mission need with thorough patch testing.

4. Planning—A system administrator-developed plan must be defined that focuses on how and what specific patches are going to be installed and the required timeframe for that installation. The plan will include user-based notification of availability, changes, possible impacts, as well as the patch installation order and installation timeframe.
5. Deployment—Deployment focuses on how the patch will be distributed and updated. As soon as the patch is available in a trusted repository, it shall be pushed to all devices/assets for which it is intended. The patch repositories shall contain all patch metadata, assets, human- and machine-readable applicability information, release notes, tasking, and human- and machine-readable instruction.
6. Review Process—System administrators will ensure that each system received the required patch and that the patch has been successfully installed. Each system, either via automated or manual means (when automated notification is not available) reports to the application that it received the patch. Decisions are made accordingly as to the success of receipt and installation.

The Configuration Management Capability shall be agile enough to react to mission and adversary changes. Although performing Configuration Management ensures that all system configurations and software installed have been tested and approved, it also means that critical software patches are not installed as soon as they are available. The Enterprise shall establish acceptable timeframes in which critical patches shall be tested and deployed.

4 Environment Pre-Conditions

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

1. The environment can detect whether a change is made by an authorized administrator.
2. Risk analysis and mitigations are in place to define the baseline configurations.
3. Configuration Management Plans are maintained outside of the managed devices.



CGS Configuration Management Capability



Version 1.1.1

4. Security Assessments are performed, and the results are provided to the Configuration Management Monitoring and Maintenance process.
5. An overarching Enterprise Configuration Management process is documented.
6. Physical configuration and protections are provided by the environment.
7. A Memorandum of Agreement (MOA) is in place with sources/vendors.
8. The Organization knows what its assets are and what configuration is maintained for each asset.
9. Public Key Infrastructure (PKI) credentials, crypto keys, and trust authority must be in place.
10. Devices must be configurable and updatable.
11. A segregated testing environment is available.

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 Configuration Management Capability maintains a log of configuration changes and provides it to the Enterprise Audit Management Capability.
2. System configuration baselines are defined and securely stored.
3. The Configuration Management Capability reports compliance data for further analysis.
4. The CCB is established and operating.
5. Backup/restore procedures are in place in case a system configuration is compromised.
6. The Configuration Management Capability rapidly implements changes to the security configuration.
7. The Configuration Management Capability supports virtualized implementations.
8. The Configuration Management Capability provides the ability to approve changes by the CCB.
9. The Enterprise knows the hardware and software assets to which the patches must be applied.

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



CGS Configuration Management Capability



Version 1.1.1

Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

Organizations will ensure that their Configuration Management includes:

- Physical client and server hardware products and versions
- OS hardware and software products and versions as provided in the Hardware Device and Software Inventories
- Application development software products and versions
- Technical architecture product sets and versions as they are defined and introduced
- Thorough documentation
- Networking products and versions
- Live application products and versions
- Definitions of packages of software releases
- Definitions of hardware base configurations
- Configuration item standards and definitions

The benefits of computer hardware configuration management are:

- Minimization of the impact of changes
- Accurate information on configuration items
- Improved security by controlling the versions of configuration items in use
- Adherence to legal obligations
- Financial and expenditure planning

Organizations will ensure that their Configuration Management procedures are integrated into the Security Content Automation Protocol (SCAP), which is a method for using specific standards to enable automated vulnerability management, measurement, and Federal Information Security Management Act (FISMA) policy compliance evaluation. This will ensure repeatability and consistency and is an iterative process that requires periodic review of baseline changes.

Organizations will ensure that processes that link information assurance (IA) and Configuration Management include Secure Configuration Management and are a cornerstone of its IA standard. All baseline changes are reviewed with the understanding that the success of all missions is tightly coupled with strong IA.



CGS Configuration Management Capability



Version 1.1.1

Organizations will ensure that the practice of Configuration Management is implemented by establishing the baseline through planning, configuring, maintaining, and monitoring:

1. As part of the planning process, Organizations will document Configuration Management plans as part of a Program Management Plan (PMP) and/or in a Configuration Management Plan (CMP). Organizations will designate a Program Manager (PM) and CCB whose responsibilities include reviewing and approving the PMP and/or the CMP and provide a commitment to the plan. The Configuration Management Organization will develop procedures to implement the CMP, perform Configuration Management activities, and resolve Configuration Management deficiencies reports against Configuration Management tools, processes, procedures, and/or status reports. The Configuration Management Organization will also ensure that all systems are patched and up to date and oversee the procedures relating to that state. Organizations will also designate the Configuration Management manager who oversees implementation of Configuration Management tasks and identifies resources, positions, and tools needed to implement the CMP and supporting procedures. The Organization will establish guidelines for bypassing some of the steps in the planning process, depending on the size and scope of projects. For example, planning for the deployment of a small number of commercial off-the-shelf (COTS) products does not require the same level of planning as designing a custom system.
2. As part of the configuring process, Organizations will ensure that any changes will be traced to the baseline and will have the ability to verify that the final delivered hardware, software, and firmware has all of the planned enhancements included in the release. In addition, as part of the configuring process, the Secure Configuration Management process identifies four procedures that must be defined for each project to ensure that a sound Secure Configuration Management process is implemented. They are:
 - a. Configuration identification
 - b. Configuration control
 - c. Configuration status accounting
 - d. Configuration audits

These terms and definitions change from standard to standard, but are essentially the same.

3. As part of the maintaining process, Organizations will ensure that up-to-date records of all the component configurations, including related documentation, are stored together in a Configuration Management Database (CMDB). Infrastructure



CGS Configuration Management Capability



Version 1.1.1

updates and changes are documented to ensure that the process is repeatable, and that every change is handled the same way through the same change control process.

4. As part of the monitoring process, Organizations will ensure that configuration audits are broken into functional and physical configuration audits. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation. Audits occur either at delivery or at the time the change takes place. Organizations will perform Configuration Audits and Reviews as follows:
 - a. Quality Assurance (QA) audits the functional characteristics of the products to verify they have achieved the requirements specified in the functional and allocated configuration documentation.
 - b. QA audits the as-built product configurations against the technical documentation to establish or verify the product baseline.
 - c. The Configuration Management group supports the functional and physical audits, provides requested data, and performs periodic informal review of Configuration Management tasks, procedures, Configuration Status Accounting (CSA) reports, and products.
 - d. The Configuration Management manager oversees resolution of reported deficiencies against Configuration Management activities.

Organizations will ensure that all components of the information technology (IT) infrastructure are registered in the CMDB.

Organizations will ensure that a system is in place to monitor notifications of as many applicable software updates as possible. The sooner software updates are known to a network, the sooner they can be tested and deployed. In some instances, it may be advantageous to a network to develop a software patch in-house rather than wait for the software vendor to release its own patch.

Organizations will assess the potential effects of a change and coordinate impacts with the impacted areas of responsibility per Mil-Std 61A and ANSI/EIA 649 to evaluate the effects of the proposed change and ensure that all potential effects are identified. Personnel in the impacted areas of responsibility will possess the specific detailed knowledge required for an accurate assessment.



CGS Configuration Management 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 Network Mapping Capability relies on the Configuration Management Capability to ensure that all network boundary devices, entry points, and exits are compliant with configurations as outlined in the CMP. In addition, the Network Mapping Capability provides the visibility necessary to determine what needs to be protected and where. The Configuration Management Capability must understand what network components are in the Enterprise to configure them properly.
- Understand Mission Flows—The Configuration Management Capability relies on information from Understand Mission Flows to provide information for defining secure configurations for workstations, servers, network devices, and other configurable devices including changes made to hardware, firmware, and software to protect the information system against improper modifications.
- Understand Data Flows—The Configuration Management Capability relies on information from the Understand Data Flows Capability to provide information for defining secure configurations for workstations, servers, network devices, and other configurable devices including changes made to hardware, firmware, and software to protect the information system against improper modifications.
- Hardware Device Inventory—The Configuration Management Capability relies on the Hardware Device Inventory Capability for information about hardware changes and uses this information to maintain compliance with the appropriate baseline(s).
- Software Inventory—The Configuration Management Capability relies on the Software Inventory Capability for information about software changes and uses this information to maintain compliance with the appropriate configuration for software assets.
- Incident Analysis—The Configuration Management Capability relies on the Incident Analysis Capability for information used to make adjustments to



CGS Configuration Management Capability



Version 1.1.1

monitoring functions based on specific incident characteristics and to determine whether system hardware, software, and firmware need to be updated.

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

7.3 Supporting Interrelationships

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

- Network Boundary and Interfaces–The Network Boundary and Interfaces Capability relies on the Configuration Management Capability to ensure that all network boundary devices, entry points, and exits are compliant with configurations as outlined in the CMP. In addition, Configuration Management relies on Network Boundary and Interfaces for visualization of the configuration status of network components.
- Utilization and Performance Management–The Configuration Management Capability relies on Utilization and Performance Management information and baseline statistics analysis to provide information required for secure reconfiguration of baseline configurations.



CGS Configuration Management Capability



Version 1.1.1

- System Protection—The System Protection Capability enforces the configuration baselines established by the Configuration Management Capability. In addition, System Protection provides information to Configuration Management to help define baseline configurations.
- Metadata Management—The Configuration Management Capability relies on the Metadata Management Capability to use IA metadata to store security information for configuration files.
- Data Protection—The Data Protection Capability relies on the Configuration Management Capability to provide secure configurations of systems and devices. Configurations can provide data protection, and data protection mechanisms keep configurations secure.
- Vulnerability Assessment—The Vulnerability Assessment Capability feeds prioritized vulnerability alerts to the Configuration Management Capability to determine potential effects resulting from misconfiguration or missing patches. The Configuration Management Capability provides information to the Vulnerability Assessment Capability that contributes to determining applicability of a vulnerability.
- Signature Repository—The Configuration Management Capability maintains the deployed signature as part of the device’s baseline.
- Network Hunting—The Network Hunting Capability provides information to the Configuration Management Capability to make adjustments to hardware, software, and firmware baselines based on specific incident characteristics. Configuration Management provides baseline information to Network Hunting for changes to the baseline as indicators.
- Risk Mitigation—The Risk Mitigation Capability relies on the information obtained from the Configuration Management Capability to determine which configurable items need to be monitored, as well as which have been successfully mitigated. Configuration Management relies on information from Risk Mitigation to help define baseline configurations.
- Operations and Maintenance—The Operations and Maintenance Capability relies on the Configuration Management Capability to push out patches and updates to systems and to handle the tracking and reporting of changes made during the operations and maintenance phases of the lifecycle. The Configuration Management Capability relies on the Operations and Maintenance Capability to manage any system administrator and user actions required as a result of changes.
- Decommission—The Configuration Management Capability relies on the Decommission Capability to decommission configurable systems and devices in



CGS Configuration Management Capability



Version 1.1.1

the Enterprise. The Decommission Capability devises the IA-oriented decommission plan and carries out the decommission actions while the Configuration Management Capability tracks the changes that occur.

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>	
CA-7 CONTINUOUS MONITORING	Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; Enhancement/s: None applied
CM-2 BASELINE CONFIGURATION	Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Enhancement/s: (1) The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades. (2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. (3) The organization retains older versions of baseline configurations as deemed necessary to support rollback. (5) The organization:



CGS Configuration Management Capability



Version 1.1.1

	<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>(6) The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.</p>
<p>CM-3 <i>CONFIGURATION CHANGE CONTROL</i></p>	<p>Control: The organization:</p> <ol style="list-style-type: none"> a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board) that convenes [Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]]. <p>Enhancement/s:</p> <ol style="list-style-type: none"> (1) The organization employs automated mechanisms to: <ol style="list-style-type: none"> (a) Document proposed changes to the information system; (b) Notify designated approval authorities; (c) Highlight approvals that have not been received by [Assignment: organization-defined time period]; (d) Inhibit change until designated approvals are received; and (e) Document completed changes to the information system. (2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system. (3) The organization employs automated mechanisms to



CGS Configuration Management Capability



Version 1.1.1

	<p>implement changes to the current information system baseline and deploys the updated baseline across the installed base.</p> <p>(4) The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element (e.g., committee, board)].</p>
<p>CM-4 SECURITY IMPACT ANALYSIS</p>	<p>Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. (NOTE: This analysis is based on the existing threats and vulnerabilities which could pose a risk to the organization.)</p> <p>Enhancement/s: None applicable</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>(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.</p> <p>(2) The organization conducts audits of information system changes [Assignment: organization-defined frequency] and when indications so warrant to determine whether unauthorized changes have occurred.</p> <p>(3) The information system prevents the installation of [Assignment: organization-defined critical software programs] that are not signed with a certificate that is recognized and approved by the organization.</p> <p>(4) The organization enforces a two-person rule for changes to [Assignment: organization-defined information system components and system-level information].</p> <p>(5) The organization:</p> <p>(a) Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and</p> <p>(b) Reviews and reevaluates information system developer/integrator privileges [Assignment: organization-defined frequency].</p>



CGS Configuration Management Capability



Version 1.1.1

	<p>(6) The organization limits privileges to change software resident within software libraries (including privileged programs).</p>
<p>CM-6 <i>CONFIGURATION SETTINGS</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings. (2) The organization employs automated mechanisms to respond to unauthorized changes to [Assignment: organization-defined configuration settings]. (3) The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes. (4) The information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.
<p>CM-7 <i>LEAST FUNCTIONALITY</i></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>



CGS Configuration Management Capability



Version 1.1.1

	<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>CM-8 INFORMATION SYSTEM COMPONENT INVENTORY</p>	<p>Control: The organization develops, documents, and maintains an inventory of information system components that:</p> <ul style="list-style-type: none"> a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [Assignment: organization-defined information deemed necessary to achieve effective property accountability]; and e. Is available for review and audit by designated organizational officials. <p>Enhancement/s:</p> <p>(5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.</p> <p>(6) The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.</p>
<p>CM-9 CONFIGURATION MANAGEMENT PLAN</p>	<p>Control: The organization develops, documents, and implements a configuration management plan for the information system that:</p> <ul style="list-style-type: none"> a. Addresses roles, responsibilities, and configuration management processes and procedures;



CGS Configuration Management Capability



Version 1.1.1

	<p>b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and</p> <p>c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.</p> <p>Enhancement/s:</p> <p>(1) The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.</p>
<p><i>SA-5 INFORMATION SYSTEM DOCUMENTATION</i></p>	<p>Control: The organization:</p> <p>a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:</p> <ul style="list-style-type: none"> - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and <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: None applied</p>
<p><i>SA-6 SOFTWARE USAGE RESTRICTIONS</i></p>	<p>Control: The organization:</p> <p>a. Uses software and associated documentation in accordance with contract agreements and copyright laws;</p> <p>b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and</p>



CGS Configuration Management Capability



Version 1.1.1

	<p>c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.</p> <p>Enhancement/s:</p> <p>(1) The organization:</p> <p>(a) Prohibits the use of binary or machine executable code from sources with limited or no warranty without accompanying source code; and</p> <p>(b) Provides exceptions to the source code requirement only for compelling mission/operational requirements when no alternative solutions are available and with the express written consent of the authorizing official.</p>
<p><i>SA-7 USER-INSTALLED SOFTWARE</i></p>	<p>Control: The organization enforces explicit rules governing the installation of software by users.</p> <p>Enhancement/s: None Specified</p>
<p><i>SC-30 VIRTUALIZATION TECHNIQUES</i></p>	<p>Control: The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.</p>
<p><i>SI-2 FLAW REMEDIATION</i></p>	<p>Control: The organization:</p> <p>a. Identifies, reports, and corrects information system flaws;</p> <p>b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and</p> <p>c. Incorporates flaw remediation into the organizational configuration management process.</p> <p>Enhancement/s:</p> <p>(1) The organization centrally manages the flaw remediation process and installs software updates automatically.</p> <p>(2) The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.</p> <p>(3) The organization measures the time between flaw identification and flaw remediation, comparing with [Assignment: organization-defined benchmarks].</p> <p>(4) The organization employs automated patch management tools to facilitate flaw remediation to [Assignment: organization-</p>



CGS Configuration Management Capability



Version 1.1.1

	defined information system components].
SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [Assignment: organization-defined list of personnel (identified by name and/or by role)]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

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.

Configuration Management Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	



CGS Configuration Management Capability



Version 1.1.1

<p>DoDI 5000.02, Operation of the Defense Acquisition System, 8 December 2008, Unclassified</p>	<p>Summary: This instruction establishes a simplified and flexible management framework for translating capability needs and technology opportunities, based on approved capability needs, into stable, affordable, and well-managed acquisition programs that include weapon systems, services, and automated information systems (AISs). ... A Configuration Management approach shall be used to establish and control product attributes and the technical baseline across the total system lifecycle. This approach shall identify, document, audit, and control the functional and physical characteristics of the system design; track any changes; provide an audit trail of program design decisions and design modifications; and be integrated with the Systems Engineering Plan and technical planning.</p>
<p>DoDI 8240.XX, Configuration Management for the Global Information Grid (GIG) (Draft), 16 October 2009, Unclassified</p>	<p>Summary: This instruction establishes policy and assigns responsibility for configuration management of the Global Information Grid (GIG) to enable the net-centric environment and to ensure interoperability and security across the Department of Defense (DoD) enterprise. Implements a standardized set of functional activities across all DoD components to maintain configuration management and establishes a configuration management governance structure for the GIG.</p>
<p>DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007, Unclassified</p>	<p>Summary: This instruction establishes the DoD Information Assurance Certification and Accreditation Process (DIACAP) for authorizing the operation of DoD information systems. The process manages the implementation of information assurance (IA) capabilities and services and provides visibility of accreditation decisions. Among the key processes described is configuration management of the DoD IA controls and supporting implementation materials throughout the information system's lifecycle.</p>
<p>MIL-HDBK-61A, Configuration Management Guidance, 7 February 2001, Unclassified</p>	<p>Summary: This guidance provides guidance and information to DoD acquisition managers, logistics managers, and other individuals assigned responsibility for configuration management. Its purpose is to assist them in planning for and implementing effective DoD configuration management activities and practices during all lifecycle</p>



CGS Configuration Management Capability



Version 1.1.1

	phases of defense systems and configuration items.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Federal Desktop Core Configuration (FDCC) Major Version 1.0, 20 June 2008	Summary: This document establishes security settings and configuration control items for Windows XPTM and/or upgrades to VISTATM operating systems.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
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 enterprise architectures 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 5 titles. The Federal Information Security Management Act of 2002 (FISMA) 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 information security program ... that includes ... policies and procedures that ... ensure compliance with ... minimally acceptable system configuration requirements, as determined by the agency...

Configuration Management Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	



CGS Configuration Management Capability



Version 1.1.1

Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, Revision 4, 1 January 2006, Unclassified	Summary: This standard provides procedural guidance for the protection, use, management, and dissemination of Sensitive Compartmented Information (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 ensure the confidentiality, integrity, and availability of that information. Requirements and responsibilities for configuration management are addressed throughout the document.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
FIPS-200, Minimum Security Requirements for Federal Information and Information Systems, March 2006, Unclassified	Summary: This standard specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal Government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. Configuration management is one of the 17 security-related areas covered.
NIST SP 800-117, Guide to Adopting and Using the Security Content Automation Protocol (SCAP) (Draft), May 2009, Unclassified	Summary: This special publication (SP) provides a conceptual level overview of the Security Content Automation Protocol (SCAP). SCAP comprises a suite of specifications for organizing and expressing security-related information in standardized ways, as well as related reference data, such as identifiers for software flaws and security configuration issues. It can be used for maintaining the security of enterprise systems, such as automatically verifying the installation of patches, checking system security configuration settings, and examining systems for



CGS Configuration Management Capability



Version 1.1.1

	signs of compromise. A SCAP-expressed checklist documents desired security configuration settings, installed patches, and other system security elements in a standardized format.
NIST SP 800-126, The Technical Specification for the Security Content Automation Protocol, November 2009, Unclassified	Summary: This SP provides the definitive technical specification for Version 1.0 of the SCAP, consisting of a suite of specifications for standardizing the format and nomenclature by which security software communicates information about software flaws and security configurations. [See entry above for SP 800-117]
NIST SP 800-128, The Draft Guide for Security Configuration Management of Information Systems, September 2010, Unclassified	Summary: This SP provides guidelines for managing the configuration of information system architectures and associated components for secure processing, storing, and transmitting of information.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
ANSI/EIA-649-A, National Consensus Standard for Configuration Management, 1 April 2004, Unclassified	Summary: This standard provides the basic Configuration Management principles and the best practices employed by industry to identify product configuration and effect orderly management of product change.
ANSI/EIA-836-A, Consensus Standard for Configuration Management Data Exchange and Interoperability, 1 June 2007, Unclassified	Summary: This standard facilitates the interoperability and exchange of configuration management data.
ANSI/EIA-632, Processes	Summary: This standard describes the systems



CGS Configuration Management Capability



Version 1.1.1

<p>for Engineering a System, 1 September 2003, Unclassified</p>	<p>engineering process of which configuration management is an integral part. [See Section 4.2.2]</p>
<p>IEEE 12207-2008, Standard for Information Technology-Software Life Cycle Processes, 1 February 2008, Unclassified</p>	<p>Summary: This standard defines a comprehensive set of processes that cover the entire lifecycle of a software system, of which configuration management is an integral part—from the time a concept is made to the retirement of the software.</p>
<p>Common Configuration Enumeration (CCE™) MITRE manages and maintains the creation of the CCE List with assistance from the CCE Working Group, conducts community outreach activities, maintains the CCE public website, and provides neutral guidance throughout the process to ensure that CCE serves the public interest. http://cce.mitre.org</p>	<p>Summary: Common Configuration Enumeration (CCE™) provides unique identifiers to security-related system configuration issues to improve workflow by facilitating fast and accurate correlation of configuration data across multiple information sources and tools. CCE Identifiers can be used to associate checks in configuration assessment tools with statements in configuration best practice documents. CCE Identifiers are the main identifiers used for the settings in the U.S. Federal Desktop Core Configuration (FDCC) data file downloads; and provide a mapping between the elements in configuration best practice documents including National Institute of Standards and Technology's (NIST) Security Configuration Guides, National Security Agency's (NSA) Security Configuration Guides, and Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGS). CCE is also one of six existing open standards used by NIST in its SCAP program, which combines "a suite of tools to help automate vulnerability management and evaluate compliance with federal information technology security requirements." Numerous products have been validated by NIST as conforming to the CCE component of SCAP.</p>
<p>Common Platform Enumeration (CPE™) http://cpe.mitre.org</p>	<p>Summary: Common Platform Enumeration (CPE™) is a structured naming scheme for information technology (IT) systems, platforms, and packages. Based on the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a</p>



CGS Configuration Management Capability



Version 1.1.1

	<p>system, and a description format for binding text and tests to a name. CPE provides a more formal, consistent, and uniform naming scheme that allows tools (as well as humans) to clearly identify the IT platforms to which a vulnerability or element of guidance applies. The CPE Specification includes a naming syntax and conventions for constructing CPE Names from product information, an algorithm for matching, a language for describing complex platforms, and an Extensible Markup Language (XML) schema for binding descriptive and diagnostic information to a name.</p>

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. Manpower to implement, maintain, and execute—The Capability will require manpower for the development of compliance verification methods and the creation of acceptable baselines (i.e., different types of devices).
2. Time to implement, maintain, and execute—The acceptable baselines will take time to prepare and time to test.



CGS Configuration Management Capability



Version 1.1.1

11 Guidance Statements

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

- The Enterprise shall provide management of workstations, servers, network devices, and other configurable devices to provide security features and assurances through control of changes made to hardware, firmware, and software (including code) to protect the information system against improper modifications during the system operation and development lifecycle.
- The Enterprise shall establish a baseline for workstations, servers, network devices, and other configurable devices including locks, guards, and doors.
- The Enterprise shall establish a baseline and provide standard software, standard configurations, and a standard operating system based on Organization mission and policy.
- When mission needs dictate that certain systems deviate from the baseline, that deviation shall be appropriately documented in accordance with Enterprise policy. This documentation shall include the reason for the required deviation, the mission and project the system supports, and what the custom configuration entails.
- The Enterprise shall establish a plan detailing how to manage configurations including the timelines and the change process, which explains how changes are implemented.
- The plan to manage configurations shall detail automated tools available to demonstrate completion of the process, periodicity, and standard of acceptable deviation, which can leverage community standards that can use standardized tools.
- The Enterprise shall establish the roles and responsibilities within the configuration management process, including the CCB, authorities, and execution elements.
- The Enterprise shall establish a plan that defines who is allowed to make changes based on type of change (system admin, security admin, and user), and how to maintain, authorize, and monitor the changes.
- The Enterprise shall ensure that baselines are deployed in a standardized, coordinated methodology using technologies defined as acceptable by the Organization's policies.



CGS Configuration Management Capability



Version 1.1.1

- The Configuration Management Plan shall be kept on a separate system from the devices being managed and protected.
- The Configuration Management Plan shall identify and document the performance, functional, and physical characteristics of a configuration item.
- The Enterprise shall configure and establish baselines for all configurable devices, even those that have multiple baselines and are initially coordinated and deployed by an engineering staff/department.
- Baselines shall be monitored monthly and shall be changed and configured as a result of patch management.
- System administrators shall be notified before any deployment to ensure little or no adverse mission impact.
- Testing shall be completed before any deployment for every change.
- Preinstalled operating system services shall be verified as to whether they are needed, disabled, or unused as part of the initial baseline configuration.
- Dedicated configuration repositories shall be used to store, protect, and disseminate secure baseline configurations and shall maintain high levels of confidentiality, integrity, and availability.
- Engineering staff shall manage updates and remediate and maintain the baseline based on authorized and approved changes in a controlled and secure environment (secure storage).
- Updates and changes shall be documented to ensure that the test processes are repeatable, and that every change is handled the same way through the same change control process.
- Impact assessments to evaluate the effects of a proposed change shall be performed in accordance with American National Standards Institute/Electronic Industries Alliance 649 and Configuration Management Military Standard 61A.
- The Enterprise shall verify that a deployed device meets the appropriate baseline by periodically auditing the configuration (physical and functional) across the entire Enterprise to verify conformance to specifications, interface control documents, and other requirements.
- The Enterprise shall provide system assessment and continuous monitoring so that strategic decisions can be made to determine whether current configuration can be improved upon.
- Configuration changes shall be monitored near real-time (as they occur), such that if a system goes out of compliance, notification is sent automatically for analysis and response.



CGS Configuration Management Capability



Version 1.1.1

- Notification of patch availability to security administrators shall occur in a timely (as available) and automated manner, where possible.
- Patch notifications shall include information regarding the fix and how to verify whether the information is correct and shall include a description of the vulnerability and the mission criticality.
- During application assessment, applications shall be identified to determine the appropriate software/firmware patch based on a trusted source inventory and shall be obtained from that inventory. Applicability and other operational attributes shall be reviewed by the security administrator to make an informed risk decision on both the original software/firmware and the patch, and the necessity for the patch shall be prioritized.
- Patches shall be tested end to end in a nonproduction, segmented environment as well as an environment that mirrors, as closely as possible, the current production environment, to determine impact on other subsystems, and patch stability.
- Patch testing shall include regression testing, documentation validation, configuration settings, and interoperability issues.
- Patch testing shall be prioritized and completed in a timely manner to meet schedule requirements.
- Patch testing shall confirm that if a rollback is required, it has been tested to ensure it is operational and the security administrator has been informed of progress. If it is determined that the patch cannot be applied, a determination shall be made of an alternative mitigation based on mission needs.
- A system administrator-developed plan shall be defined to include user-based notification of availability, changes, possible impacts, as well as the patch installation order and installation timeframe.
- When the patch is available in a trusted repository, it shall be pushed to all devices/assets for which it is intended.
- Patch repositories shall contain all patch metadata, assets, human- and machine-readable applicability information, release notes, tasking, and human- and machine-readable instruction.
- After patch deployment, system administrators shall ensure that each system received the required patch and that the patch was successfully installed. Each system shall report to the application that it received the patch either via automated or manual means (when automated notification is not available).