



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Operations and Maintenance Capability

Version 1.1.1

The Operations and Maintenance Capability encompasses the activities of the Operations and Maintenance phases of the system development lifecycle. These activities include technical and administrative procedures that account for the use and maintenance of hardware, software, and data assets that support the mission.



CGS Operations and Maintenance 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.....	9
7.1	Required Interrelationships	9
7.2	Core Interrelationships	10
7.3	Supporting Interrelationships.....	11
8	Security Controls	11
9	Directives, Policies, and Standards	17
10	Cost Considerations	22
11	Guidance Statements.....	23



CGS Operations and Maintenance 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 Operations and Maintenance 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 Operations and Maintenance Capability encompasses the activities of the Operations and Maintenance phases of the system development lifecycle. These activities include technical and administrative procedures that account for the use and maintenance of hardware, software, and data assets that support the mission. The Operations and Maintenance Capability shall employ an approved system development lifecycle process (established in accordance with the IA Policies, Procedures, and Standards Capability) that implements and maintains information assurance (IA) during Operations and Maintenance.

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 Operations and Maintenance Capability is responsible for ensuring that IA needs and activities are fully integrated during the Operations and Maintenance phases. The appropriate protection measures established by other Capabilities (i.e., System Protection, Data Protection, and Communication Protection) shall operate and be updated in accordance with protection needs. Any changes made under the auspices of this Capability shall maintain the expected risk posture as established by Risk Analysis and Risk Mitigation.

The Operations and Maintenance Capability shall ensure that users and administrators are properly trained in the use and support of Enterprise systems, as appropriate for their job function. This includes coordination with the IA Awareness and IA Training Capabilities to disseminate training and other applicable information. Users and administrators shall be provided continuous and evolving training and awareness to inform them of the latest developments and changes. This will ensure that they can



CGS Operations and Maintenance Capability



Version 1.1.1

continue to use and maintain systems without intentionally violating any IA requirements.

The Operations and Maintenance Capability requires the existence of teams composed of systems security engineers (SSEs). SSE teams ensure that all security requirements are considered, developed, and thoroughly documented. Any architectural or engineering changes, or changes that shall impact the risk posture of operational technical assets, shall be vetted through SSE teams. Input from SSE teams shall be incorporated for all changes, whether they are routine, major, or emergency changes.

The Operations and Maintenance Capability shall employ services from a program management (PM) role or office. This will ensure that all activities and resources are managed according to the PM plan and are able to meet the IA objectives established.

All changes made to systems as a part of Operations and Maintenance functions shall be vetted by a Change Control Board through an Enterprise-defined change control process. Change Control Boards are composed of or include input from individuals in management, SSE teams, IA stakeholders/representatives, and system owner(s), in addition to the personnel who will implement the change. For major changes, an Information Systems Security Officer (ISSO) shall be assigned to work with the Change Control Board to interface with an authority that has been designated by the Enterprise to approve changes. The approval authority shall make a final decision about whether to implement the change. This process is used to ensure that appropriate approvals are obtained before any changes are implemented. The Enterprise shall determine all of the processes for approving and implementing routine, major, and emergency changes.

Operations and Maintenance functions shall interface with the Configuration Management Capability, which is responsible for pushing out patches and updates to systems. In addition, Configuration Management handles the tracking and reporting of changes made during the Operations and Maintenance phases of the lifecycle. The Operations and Maintenance Capability is responsible for the system administrator and user actions required as a result of changes, when appropriate. For example, prompting the user to reboot his or her workstation after a patch is installed falls under Operations and Maintenance, while installing the patch itself is handled by Configuration Management.

During the course of Operations and Maintenance activities, there may be planned or unplanned downtime of Enterprise resources. Any downtime shall be handled to



CGS Operations and Maintenance Capability



Version 1.1.1

maintain the Organization's availability requirements as set by the Utilization and Performance Management Capability. Planned downtime shall occur during off-peak times whenever possible and shall be announced through Organization-approved channels. Announcements shall be sent to all internal and external personnel who use the system that will experience downtime. The Operations and Maintenance Capability uses information provided by Understand Data Flow and Understand Mission Flow to understand the impact of downtime. This knowledge shall be used to prioritize fixing unplanned downtime and to schedule planned downtime.

The Operations and Maintenance Capability requires that testing shall occur whenever there is a proposed change. The testing process shall interact with other Capabilities to ensure the change does not have an unacceptable effect on the Enterprise security posture. Network Security Evaluations and Architecture Reviews each identify vulnerabilities, and Risk Analysis ensures that changes do not produce unacceptable risks. In addition, any applicable certification and accreditation documents shall be updated to reflect the changes. Approval from a Change Control Board may also be required, depending on Enterprise policy. Changes shall be audited in accordance with policies set by the Enterprise Audit Management Capability and records shall be stored in accordance with IA Policies, Procedures, and Standards. Some changes may have a tailored or shortened testing process depending on mission criticality of the system on which the change will be implemented. The Operations and Maintenance Capability shall follow Enterprise-established policy defining a minimum level of testing all changes shall go through and guidelines for when a change can bypass the remainder of the testing regimen.

The Operations and Maintenance Capability shall use appropriate maintenance agreements to meet mission objectives. When Operations and Maintenance tasks are performed by external entities, the Enterprise shall employ the appropriate Personnel Security controls and Physical and Environmental Protection to ensure continued adherence to Enterprise IA needs (for additional information, see the Personnel Security and Physical and Environmental Protection Capabilities). Certain systems shall be designated by the Enterprise as being too critical or sensitive to receive maintenance from external personnel. All contracts with external entities that perform Operations and Maintenance functions shall be governed by Enterprise policy.

All tools used during Operations and Maintenance functions shall be tested and approved prior to their use. Standards used for testing and approval shall follow Enterprise policy.



CGS Operations and Maintenance Capability



Version 1.1.1

When remote maintenance is used within the Enterprise, the communications shall be protected in accordance with the Communications Security Capability. Remote Maintenance shall be performed by only authorized and authenticated system administrators, and it shall be limited to circumstances dictated by Enterprise policy. The Operations and Maintenance Capability receives information from the Network Enterprise Monitoring Capability about the environment. Any unexpected anomalies to the Enterprise shall generate a response from Operations and Maintenance personnel, who shall ascertain the root cause of the anomaly and correct it.

The Operations and Maintenance Capability shall interact with the Development Capability by providing information and feedback to their processes so future systems are built such that Operations and Maintenance tasks associated with them are easier. It may also be necessary for the Operations and Maintenance Capability to work with the Decommission Capability to perform tasks while a system is still in operation to prepare for its decommissioning.

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. Resources are available to operate the mission.
2. The appropriate Capabilities are in place to support secure operation of the mission.
3. Performance and utilization goals are clearly defined.
4. Only authorized personnel are allowed to make approved system changes.
5. Changes and their impact to the overall security and risk posture are analyzed prior to being implemented.
6. The Organization's change management process has been defined.
7. All programs have an established PM role or office to manage activities and resources.

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 Operations and Maintenance Capability



Version 1.1.1

1. Contractual (or other) maintenance agreements are in place to obtain maintenance resources (including replacement).
2. The Capability maintains the system availability and performance requirements levied by the Utilization and Performance Management Capability.
3. Any changes made within this Capability aligns with the defined risk posture.

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 strive to maintain its systems in accordance with the accepted risk posture of the Enterprise. All users and administrators will perform their duties in full compliance with the Organization's established IA Policies, Procedures, and Standards. The functions of the Operations and Maintenance Capability will work to ensure the continued secure functionality of all necessary Enterprise systems and protection measures. The Organization's Operations and Maintenance personnel will work at an elevated level to ensure that all necessary actions are performed promptly.

The Organization will provide training to all personnel, as necessary, to ensure that they have the requisite knowledge to perform their duties in a secure manner (see IA Training and IA Awareness). All personnel will be trained to use systems only in their intended manner. The Organization will have all of its personnel agree to (sign) acceptable use policies to access systems. Administrators will receive training as new technologies are introduced to the system to make sure they always understand what they are working with. There will be a separation of duties so that system administrators perform routine functions, and security administrators are responsible for security functions. Personnel are encouraged to always practice proper OPSEC (operations security).

The Organization will use teams of SSE who work with Operations and Maintenance personnel to design secure solutions when significant changes to Enterprise systems need to be made. Proposed changes will be tested prior to being implemented, according to Organization policy. The level of testing each proposed change goes through will vary based on system criticality, the complexity of the change, and the



CGS Operations and Maintenance Capability



Version 1.1.1

timeframe. The Organization will establish a policy defining a minimum level of testing all changes will go through and guidelines for when a change can bypass the remainder of the testing regimen. Testing includes analysis by Architecture Reviews and Network Security Evaluations to identify any vulnerabilities and by Risk Analysis to ensure that they do not have a negative impact on the Enterprise risk posture. Changes will also be approved through the Organization's change approval process. This process will vary by Organization and depend on the complexity of the change and the criticality of the systems involved. Once a change has been implemented, the Organization will have the system recertified according to the relevant certification and accreditation procedures.

The Organization will maintain all system availability requirements as determined by Utilization and Performance Management. When downtime is necessary to complete system changes, the Operations and Maintenance Capability will plan the event carefully in accordance with Organization policy. Unplanned outages will be addressed promptly and prioritized according to information provided by Understand Data Flow and Understand Mission Flow. All outages will be handled to restore system availability as soon as feasible and in order, starting with the most critical systems.

The Organization will use remote maintenance techniques when appropriate, based on mission need and system criticality. Remote connections can include those that originate from outside the Enterprise or connections from another physical location within the Enterprise. All remote connections will be secured by Communication Protection and use strong authentication techniques provided by Access Management.

The Organization may employ external Operations and Maintenance personnel (e.g., contractors) to use or maintain internal systems. When outside contractors are involved, appropriate protections will be in place to secure the Organization's resources from unauthorized use or tampering, and security compliance metrics will be included in the service agreement. Some systems may have Operations and Maintenance functions performed on them only by internal personnel as specified by Organizational policy. For example, Organization policy may state that systems managing certain highly sensitive or mission-critical information may be used or maintained only by internal personnel.

The Organization will allow the Operations and Maintenance Capability to use only approved tools and methods. The approval process will be conducted according to Organization policy.



CGS Operations and Maintenance Capability



Version 1.1.1

The Organization will maintain open communication channels between personnel responsible for each phase of lifecycle management. The functions of each phase will be separated and use different personnel. Maintaining open communications between these different groups allows personnel to perform tasks that will facilitate the duties of later phases. For example, development personnel will design systems such that they are easy to maintain, while Operations and Maintenance personnel will maintain systems so they are easy to decommission.

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 Operations and Maintenance Capability relies on the Network Mapping Capability to provide information about the current state of the network, which will be factored into operations and maintenance decisions made throughout the lifecycle.
- Utilization and Performance Management–The Operations and Maintenance Capability relies on the Utilization and Performance Management Capability to provide information about the utilization, performance, and availability requirements for resources.
- Understand Mission Flows–The Operations and Maintenance Capability relies on the Understand Mission Flows Capability for information about mission flows, which is used to anticipate future activity and keep Enterprise systems operational to maintain the mission flow.
- Understand Data Flows–The Operations and Maintenance Capability relies on the Understand Data Flows Capability for information about data flows, which is used to anticipate future activity and keep Enterprise systems operational to maintain necessary data flows.
- Personnel Security–The Operations and Maintenance Capability relies on the Personnel Security Capability to provide protection to the Enterprise through the



CGS Operations and Maintenance Capability



Version 1.1.1

use of background investigations and security clearances to prevent malicious individuals from obtaining access to perform maintenance functions.

- Configuration Management–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.
- Access Management–The Operations and Maintenance Capability relies on the Access Management Capability to provide controlled access to Enterprise systems while systems are undergoing maintenance and to prevent unauthorized use or changes to operational technical assets.
- Architecture Reviews–The Operations and Maintenance Capability relies on the Architecture Reviews Capability to evaluate systems for met and unmet security requirements.
- Network Enterprise Monitoring–The Operations and Maintenance Capability relies on the Network Enterprise Monitoring Capability to provide information about the status of the Enterprise for situational awareness.
- Risk Analysis–The Operations and Maintenance Capability relies on the Risk Analysis Capability to analyze changes to ensure that they do not cause any unacceptable risks to the Enterprise.
- Finance–The Operations and Maintenance Capability relies on the Finance Capability to provide funding, including certification and accreditation funding, throughout operations and maintenance.
- Deployment–The Operations and Maintenance Capability relies on the Deployment Capability to deploy systems.
- Decommission–The Operations and Maintenance Capability relies on the Decommission Capability to define the decommission activities for operational systems.

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 Operations and Maintenance 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 Operations and Maintenance Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.



CGS Operations and Maintenance Capability



Version 1.1.1

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

- System Protection–The Operations and Maintenance Capability relies on the System Protection Capability to provide appropriate protection mechanisms to Enterprise systems.
- Communication Protection–The Operations and Maintenance Capability relies on the Communication Protection Capability to secure all remote support sessions.
- Physical and Environmental Protections–The Operations and Maintenance Capability relies on the Physical and Environmental Protections Capability to provide critical protection to Enterprise resources while operations and maintenance functions are performed.

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>	
PL-2 SYSTEM SECURITY PLAN	Control: The organization: <ul style="list-style-type: none"> a. Develops a security plan for the information system that: <ul style="list-style-type: none"> – Is consistent with the organization’s enterprise architecture; – Explicitly defines the authorization boundary for the



CGS Operations and Maintenance Capability



Version 1.1.1

	<p>system;</p> <ul style="list-style-type: none">- 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 system;- 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> <p>(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</p> <p>(b) Reviews and updates the CONOPS [Assignment: organization-defined frequency].</p> <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> <p>(a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;</p>
--	--



CGS Operations and Maintenance Capability



Version 1.1.1

	<p>(b) User roles and the access privileges assigned to each role;</p> <p>(c) Unique security requirements;</p> <p>(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</p> <p>(e) Restoration priority of information or information system services.</p>
<p><i>SA-3 LIFE CYCLE SUPPORT</i></p>	<p>Control: The organization:</p> <p>a. Manages the information system using a system development life cycle methodology that includes information security considerations;</p> <p>Enhancement/s: None Specified</p>
<p><i>MA-2 CONTROLLED MAINTENANCE</i></p>	<p>Control: The organization:</p> <p>a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;</p> <p>b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;</p> <p>c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs’;</p> <p>d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and</p> <p>e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.</p> <p>Enhancement/s:</p> <p>(1) The organization maintains maintenance records for the information system that include:</p> <p>(a) Date and time of maintenance;</p> <p>(b) Name of the individual performing the maintenance;</p> <p>(c) Name of escort, if necessary;</p> <p>(d) A description of the maintenance performed; and</p> <p>(e) A list of equipment removed or replaced (including</p>



CGS Operations and Maintenance Capability



Version 1.1.1

	<p>identification numbers, if applicable).</p> <p>(2) The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.</p>
<p>MA-3 MAINTENANCE TOOLS</p>	<p>Control: The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.</p> <p>Enhancement/s:</p> <p>(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.</p>
<p>MA-4 NON-LOCAL MAINTENANCE</p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed. <p>Enhancement/s:</p> <p>(1) The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.</p> <p>(2) The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.</p> <p>(3) The organization:</p> <ul style="list-style-type: none"> (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or



CGS Operations and Maintenance Capability



Version 1.1.1

	<p>(b) Removes the component to be serviced 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>(4) The organization protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either:</p> <p>(a) Physically separated communications paths; or</p> <p>(b) Logically separated communications paths based upon encryption. Enhancement Supplemental Guidance: Related control: SC-13.</p> <p>(5) The organization requires that:</p> <p>(a) Maintenance personnel notify [Assignment: organization-defined personnel] when non-local maintenance is planned (i.e., date/time); and</p> <p>(b) A designated organizational official with specific information security/information system knowledge approves the non-local maintenance.</p> <p>(6) The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.</p> <p>(7) The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.</p>
<p>MA-5 MAINTENANCE PERSONNEL</p>	<p>Control: The organization:</p> <p>a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and</p> <p>b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance</p>



CGS Operations and Maintenance Capability



Version 1.1.1

	<p>personnel do not possess the required access authorizations. Enhancement/s:</p> <p>(1) The organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:</p> <p>(a) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;</p> <p>(b) 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 or physically disconnected from the system and secured; and</p> <p>(c) In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.</p> <p>(2) The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are cleared (i.e., possess appropriate security clearances) for the highest level of information on the system.</p> <p>(3) The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens.</p> <p>(4) The organization ensures that:</p> <p>(a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on an information system only when the system is jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and</p>
--	---



CGS Operations and Maintenance Capability



Version 1.1.1

	(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on an information system are fully documented within a Memorandum of Agreement.
MA-6 <i>TIMELY MAINTENANCE</i>	Control: The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined list of security-critical information system components and/or key information technology components] within [Assignment: organization-defined time period] of failure. Enhancement/s: None Specified

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Operations and Maintenance Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 801, Acquisition, 16 August 2009, Unclassified	Summary: National Intelligence Program (NIP) major system acquisitions (MSA) shall use the acquisition process model identified in Intelligence Community (IC) Policy Guidance (ICPG) 801.1 to ensure that a set of validated and approved requirements is implemented using a disciplined process through development, integration, and testing within an established schedule and budget.
ICPG 801.1, Acquisition, 12 July 2007, Unclassified	Summary: As directed in Intelligence Community Directive (ICD) 801, the IC acquisition approach will follow the Intelligence Community Acquisition Model (ICAM) and will be either a single-step development or, more frequently, an evolutionary development. Both single-step and evolutionary developments are characterized by discrete phases (e.g., concept refinement, development, production, deployment, and sustainment [includes Operations and Maintenance]) that correspond to the maturity of a technical solution to meet validated user requirements.



CGS Operations and Maintenance Capability



Version 1.1.1

Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 4151.18, Maintenance of Military Material, 31 March 2004, Unclassified	Summary: Maintenance programs for Department of Defense (DoD) materiel shall be structured and managed to achieve inherent performance, safety, and reliability levels of the materiel. Among the stated policies, maintenance programs shall be designed for minimizing the total lifecycle cost of ownership and adjusted periodically to reduce that cost.
DoDI 4151.22, Condition- Based Maintenance Plus (CBM+) for Material Maintenance, 2 December 2007, Unclassified	Summary: Condition-based Maintenance Plus (CBM+) is the primary reliability driver in the total lifecycle systems management (TLCSM) supportability strategy of the DoD. It is DoD policy that: a. CBM+ be included in the selection of maintenance concepts, technologies, and processes for all new weapon systems, equipment, and materiel programs based on readiness requirements, lifecycle cost goals, and reliability centered maintenance-based functional analysis. b. CBM+ be implemented into current weapon systems, equipment, and materiel sustainment programs where technically feasible and beneficial.
DoDD 5000.01, The Defense Acquisition System, 20 November 2007, Unclassified	Summary: Consistent with statute and the regulatory requirements specified in this directive and in DoD Instruction (DoDI) 5000.02, every program manager shall establish program goals for the minimum number of cost, schedule, and performance parameters that describe the program over its entire lifecycle. Program managers shall consider supportability, lifecycle costs, performance, and schedule comparable in making program decisions. Planning for operation and support and the estimation of



CGS Operations and Maintenance Capability



Version 1.1.1

	<p>total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system lifecycle.</p>
<p>DoDI 5000.02, Operation of Defense Acquisition System, 8 December 2008, Unclassified</p>	<p>Summary: This instruction implements DoDD 5000.01 by establishing 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. It describes the five phases of the Defense Acquisition Management System: Materiel Solution Analysis, Technology Development, Engineering & Manufacturing Development, Production & Deployment, and Operations & Support [includes Maintenance]. Systems engineering shall be embedded in program planning and be designed to support the entire acquisition lifecycle.</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 IA capabilities and services and provides visibility of accreditation decisions. The DIACAP requirements, activities, and tasks described are applicable throughout the information system's lifecycle, which includes Operations and Maintenance.</p>
<p>DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2007, Unclassified</p>	<p>Summary: IA shall be implemented in all system and services acquisitions at levels appropriate to the system characteristics and requirements throughout the entire lifecycle of the acquisition in accordance with an adequate and appropriate Acquisition IA Strategy that shall be reviewed prior to all acquisition milestone decisions, program decision reviews, and acquisition contract awards.</p>
<p>CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems, 15 December</p>	<p>Summary: It is Joint Staff policy to ensure that DoD components develop, acquire, deploy, and maintain information technology (IT) and National Security Systems (NSS) that (1) meet the essential operational needs of U.S. forces; (2) are interoperable with existing and proposed IT and NSS through standards, defined interfaces, modular</p>



CGS Operations and Maintenance Capability



Version 1.1.1

2008, Unclassified	design, and reuse of existing IT and NSS solutions; ... DoD combatant commands/services/agencies (C/S/A) play a key role in ensuring consistent interoperability is appropriately inculcated into the capability's lifecycle.
Defense Acquisition Guidebook, https://dag.dau.mil/Palques/Default.aspx , 17 December 2009, Unclassified	Summary: This document complements DoD Directive (DoDD) 5000.01 and DoDI 5000.02 by providing the acquisition workforce with discretionary best practices that should be tailored to the needs of each program. Section 4.3, Systems Engineering in the System Life Cycle, provides an integrated technical framework for systems engineering activities throughout the acquisition phases of a system's lifecycle, highlighting the particular systems engineering inputs, activities, products, technical reviews, and outputs of each acquisition phase.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Operations and Maintenance Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	



CGS Operations and Maintenance Capability



Version 1.1.1

Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP 800-64 Rev 2, Security Considerations in the System Development Life Cycle, October 2008, Unclassified	Summary: This special publication focuses on the information security components of the system development lifecycle (SDLC). It describes the key security roles and responsibilities that are needed in development of most information systems. Its scope is security activities that occur within the linear, sequential (a.k.a. waterfall) SDLC methodology. The five-step SDLC cited in this document [includes Maintenance] is an example of one method of development and is not intended to mandate this methodology.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
ISO/IEC 15288:2008, Systems and Software Engineering—System Life Cycle Processes, 1 February 2008, Unclassified	Summary: This document provides a common process framework and the processes for acquiring and supplying systems. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of these processes can be applied throughout the full system lifecycle (e.g., conception of ideas, development, production, utilization, support, and retirement of the system) and to the acquisition and supply of systems.
IEEE 1220-2005, IEEE Standard for Application and Management of the Systems Engineering	Summary: This standard defines the interdisciplinary tasks that are required throughout a system's lifecycle to transform stakeholder needs, requirements, and constraints into a system solution. It is intended to guide



CGS Operations and Maintenance Capability



Version 1.1.1

<p>Process, 9 September 2005, Unclassified</p>	<p>the development of systems for commercial, government, military, and space applications and applies to projects within an Enterprise that is responsible for developing a product design and establishing the lifecycle infrastructure needed for lifecycle sustainment.</p>
<p>International Council on Systems Engineering (INCOSE) Systems Engineering Handbook, version 3.1, 2007, Unclassified</p>	<p>Summary: This document describes the key process activities performed by systems engineers, covering in detail the purpose for each process activity, what needs to be done, and how to do it. It provides sufficient information to determine whether a given process activity is appropriate in supporting program objectives and how to go about implementing the process activity.</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. Complexity of systems being operated and maintained—More complex systems may require more resources and time to operate and maintain.
2. Necessary training—Both users and systems maintainers will need to go through proper training and periodic retraining to ensure proper use and maintenance of all Enterprise systems.



CGS Operations and Maintenance 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 Operations and Maintenance Capability.

- The Enterprise shall be responsible for ensuring that IA needs and activities are fully integrated during the Operations and Maintenance phases.
- The Enterprise shall operate and update all protection measures in accordance with protection needs.
- Any changes made under operations and maintenance shall maintain the expected risk posture established by the Enterprise.
- The Enterprise shall ensure that users and administrators are properly trained in the use and support of Enterprise systems, as appropriate for their job function.
- Users and administrators shall be provided continuous and evolving training and awareness to inform them of the latest developments and changes to ensure that they can continue to use and maintain systems without intentionally violating any IA requirements.
- The Enterprise shall use teams composed of SSEs for operations and maintenance to ensure that all security requirements are considered, developed, and thoroughly documented.
- Architectural or engineering changes, or changes that impact the risk posture of operational technical assets, shall be vetted through systems security engineering teams.
- Input from systems security engineering teams shall be incorporated for all changes, whether they are routine, major, or emergency changes.
- The Enterprise shall employ services from a PM role or office to ensure that all activities and resources are managed according to the PM plan and are able to meet the IA objectives established.
- All changes made to systems as a part of operations and maintenance functions shall be vetted by a Change Control Board through an Enterprise-defined change control process.
- The approval authority shall make a final decision about whether to implement the change to ensure that appropriate approvals are obtained before any changes are implemented.
- The Enterprise shall determine all of the processes for approving and implementing routine, major, and emergency changes.



CGS Operations and Maintenance Capability



Version 1.1.1

- Operations and maintenance functions shall interface with a configuration management system, which is responsible for pushing out patches and updates to systems.
- Planned or unplanned downtime of Enterprise resources shall be handled to maintain the Organization's availability requirements and shall occur during off-peak times whenever possible and shall be announced through Organization-approved channels.
- The Enterprise shall understand the impact of downtime and use it to prioritize fixing unplanned downtime and to schedule planned downtime.
- The Enterprise shall employ testing for proposed changes to ensure the change does not have an unacceptable effect on the Enterprise security posture.
- The Enterprise shall follow Enterprise-established policy defining a minimum level of testing all changes must go through and guidelines for when a change can bypass the remainder of the testing regimen.
- The Enterprise shall use appropriate maintenance agreements to meet mission objectives.
- The Enterprise shall employ the appropriate personnel security and environmental controls to ensure continued adherence to Enterprise IA needs for tasks that are performed by external entities.
- All contracts with external entities that perform operations and maintenance functions shall be governed by Enterprise policy.
- All tools used during operations and maintenance functions shall be tested and approved prior to their use.
- When remote maintenance is used within the Enterprise, the communications shall be protected in accordance with the communications security policy.
- Remote maintenance shall be performed by only authorized and authenticated system administrators, and it shall be limited to circumstances dictated by Enterprise policy.
- Any unexpected anomalies to the Enterprise shall generate a response from operations and maintenance personnel, who shall ascertain the root cause of the anomaly and correct it.
- The Enterprise shall provide information and feedback on its development processes so future systems are built such that operations and maintenance tasks associated with them are easier.