IT Security Procedural Guide:

Maintenance

CIO-IT Security-10-50

Revision 3

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 2 – August 20, 2015				
1	Haq/Sitcharing	Changes made throughout the document to reflect NIST and GSA requirements since the 2010 guide creation.	Updated to reflect and implement most current NIST SP 800-53 Rev 4 and GSA requirements.	Throughout
Revision 3 –				
1	Dean/Feliksa/ Klemens	Updated format and NIST SP 800-53 control parameters, and incorporated current Federal regulations and guidance.	Incorporate most current Federal regulations, NIST guidance, and GSA requirements.	Throughout

APPROVAL

IT Security Procedural Guide: Maintenance, CIO-IT Security-10-50, Revision 3 is hereby approved for distribution.

10/10/2017

X Kurt Garbars

Kurt D. Garbars
Chief Information Security Officer
Signed by: KURT GARBARS

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division, at ispcompliance@gsa.gov.

Table of Contents

1 Introduction

Information systems operate in highly dynamic operating environments, requiring continuous functionality of critical hardware and software components. Once a system enters the operations/maintenance phases of its life cycle, various types of planned and unplanned maintenance activities will need to be performed to effectively sustain system availability. It is therefore critical that an effective maintenance process is implemented to allow system components (hardware and software) to be maintained in accordance with manufacturer's recommendations, contractual requirements, and best business practices throughout the system's life cycle.

Every General Services Administration (GSA) Information Technology (IT) system must follow the Maintenance (MA) practices identified in this guide. Any deviations from the security requirements established in GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy,*" must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

The maintenance principles and practices described in this guide are based on guidance from the National Institute of Standards and Technology (NIST) including NIST Special Publication (SP) 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations.*" This guide provides an overview of maintenance, roles and responsibilities, NIST SP 800-53 maintenance requirements per Federal Information Processing Standard Publication (FIPS PUB) 199, "*Standards for Security Categorization of Federal Information and Information Systems*" security categorization level, and procedures for implementing these requirements.

Executive Order (EO), EO 13800, "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"* requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology (NIST) or any successor document to manage the agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework from NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach.*" Table 1-1, NIST SP 800-53 Control to CSF Mapping, provides how the NIST SP 800-53 controls within this guide are aligned with the CSF Category Unique Identifiers.

Table 1-1: NIST SP 800-53 Control to CSF Mapping

NIST SP 800-53 Security Controls Maintenance (MA)	CSF Category Unique Identifier Codes Identify - Governance (ID.GV) Protect – Maintenance (PR.MA)
MA-1	ID.GV-1, ID.GV-3
MA-2	PR.MA-1
MA-3	PR.MA-1
MA-4	PR.MA-2
MA-5	PR.MA-1
MA-6	PR.MA-1

1.1 Purpose

The purpose of this guide is to provide guidance for the MA security controls identified in NIST SP 800-53 and maintenance requirements specified in CIO 2100.1. This procedural guide provides GSA Federal employees and contractors with significant security responsibilities (as identified in CIO 2100.1), and other IT personnel involved in the maintenance of IT assets the specific procedures and processes they are to follow for maintaining GSA information systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in the maintenance of GSA information systems and data.

1.3 Policy

Maintenance is covered in Chapter 4, paragraph 2 of CIO 2100.1 as stated in the following paragraphs.

e. Hardware and software maintenance.

(1) *The availability and usability of GSA equipment and software must be maintained and safeguarded to enable agency objectives to be accomplished.*
(2) *Lost or stolen GSA IT assets must be immediately reported to the IT Service Desk.*
(3) *All information systems must be securely hardened and patched before being put into operation and while in operation. Hardening will be IAW GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Where a GSA benchmark exists, it must be used.*
(4) *Google Chrome Extensions (often developed by third parties) extend Google Chrome and Google Apps functionality. Extensions shall be disabled by default and enabled for business purposes following review and approval by the Security Engineering Division in the Office of the Chief Information Security.*

(5) *Maintenance of agency hardware and software must be restricted to authorized personnel.*
(6) *Hardware and software must be tested in a non-production environment to identify adverse effects on system functionality, be documented, and approved prior to promotion to production.*
(7) *In GSA facilities, only approved Government Furnished Equipment (GFE) is allowed connection (e.g., Ethernet) to the network unless specifically approved by the hosting/supporting system AO. All non-GFE will be given Internet only access, if possible.*
(8) *All GFE, to include hardware, software and COTS applications, must be approved through the GSA Helpdesk approval process prior to procurement.*
(9) *Ensure that maintenance activities of hardware and software are IAW with GSA-IT Security-10-50: Maintenance.*

1.4 References

Federal Laws and Regulations:

- EO 13800, *"Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"*

Federal Standards and Guidance:

- FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems"*
- NIST SP 800-37, Revision 1, *"Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach"*
- NIST SP 800-53, Revision 4, *"Recommended Security Controls for Federal Information Systems and Organizations"*
- Cyber Security Framework, *"Framework for Improving Critical Infrastructure Cybersecurity"*

GSA Directives, Policies and Procedures:

- GSA Order CIO 2100.1, *"GSA Information Technology (IT) Security Policy"*
- GSA ISPP, *"Information Security Program Plan"*
- CIO-IT Security-06-32, *"Media Protection"*

2 Roles and Responsibilities

There are many roles associated with effectively maintaining IT systems. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. Throughout this guide specific processes and procedures for implementing NIST's MA controls are described.

2.1 The Chief Information Officer (CIO)

Responsibilities include the following:

- Developing and maintaining an agency-wide GSA IT Security Program.
- Ensuring the agency effectively implements and maintains information security policies and guidelines.
- Providing management processes to enable the Authorizing Official to implement the components of the IT Security Program for which they are responsible.

2.2 The Chief Information Security Officer (CISO)

Responsibilities include the following:

- Reporting to the GSA CIO on the implementation and maintenance of the GSA's IT Security Program and Security Policies.
- Implementing and overseeing GSA's IT Security Program by developing and publishing IT Security Procedural Guides that are consistent with this policy.
- Ensuring preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of GSA.

2.3 Authorizing Official (AO)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required security controls in accordance with GSA and Federal policies and requirements.
- Accepting the risk of operating GSA information systems under their purview where MA controls have not been fully implemented.
- Ensuring a plan of action and milestones (POA&M) item is established and managed to address MA controls that are not fully implemented.

2.4 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Monitoring and supporting the resolution of POA&Ms to mitigate system vulnerabilities regarding security controls for all systems under their purview.
- Ensuring POA&Ms are developed and uploaded into the GSA POA&M Management Site.
- Ensuring ISSOs and System Owners are maintaining POA&Ms for their systems, including taking remediation actions according to the scheduled milestones.

2.5 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary security controls are in place and operating as intended.
- Developing POA&Ms regarding MA controls for all systems under their purview.
- Ensuring system security measures are implemented effectively.

2.6 System Owner

Responsibilities include the following:

- Ensuring necessary security controls are in place and operating as intended.
- Obtaining and allocating the security resources for their respective systems.
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms regarding MA controls for their respective systems.
- Defining and scheduling software patches.
- Ensuring proper separation of duties for GSA IT system maintenance, management, and development processes.

2.7 Data Owners

Responsibilities include the following:

- Coordinating with System Owners, ISSMs, ISSOs, and System Owners to ensure implementation of security control requirements.
- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of system and data security requirements.

2.8 Custodians

Responsibilities include the following:

- Coordinating with data owners and system owners to ensure the data is properly stored, maintained, and protected.
- Providing and administering general controls such as back-up and recovery systems consistent with the policies and standards issued by the Data Owner.
- Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the AO.

2.9 System/Network Administrators

Responsibilities include the following:

- Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.
- Implementing system backups and patching of security vulnerabilities.

3 GSA Implementation Guidance for MA Controls

The GSA-defined parameter settings included in the control requirements are offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in the maintenance of GSA information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions/requirements for contractor systems will be included in the additional contractor system considerations portion of each control section. When "None" appears in the additional contractor system considerations it means that there are no additional instructions, such systems still must address applicable parts of the controls.

MA-1, System Maintenance Policy and Procedures, has been identified as a Common Control for all GSA/internally operated systems by GSA and as a Hybrid Control for contractor systems. The MA-2 to MA-6 controls, when included in a system's control set, are system specific controls allocated to the system for control implementation.

3.1 MA-1 Maintenance Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
    1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates the current:
    1. System maintenance policy [*biennially*]; and
    2. System maintenance procedures [*biennially*].

GSA Implementation Guidance: Control MA-1 is applicable at all FIPS 199 levels.

System maintenance policy and procedures is a common control provided by the GSA OCISO Policy and Compliance Division (ISP). System maintenance policy is included in CIO 2100.1, "*GSA Security Policy,*" Chapter 4, Policy on Operational Controls. The policy states, "*The availability and usability of GSA equipment and software must be maintained and safeguarded to enable agency objectives to be accomplished.*" GSA OCISO ISP has also defined agency-wide system maintenance control procedures in this guide. GSA's security policy and procedural guides are disseminated via the GSA IT Security InSite page.

CIO 2100.1 and this guide are reviewed/updated biennially.

Additional Contractor System Considerations:

Vendors/Contractors may defer to the GSA policy and guide or implement their own system maintenance policies and procedures which comply with GSA's requirements with the approval of the Authorizing Official (AO).

3.2 MA-2 Controlled Maintenance

Control: The organization:

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;
b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Requires that [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
f. Includes [*Date and time of maintenance; Name of the individual performing the maintenance; Name of escort, if necessary; A description of the maintenance performed; A list of equipment removed or replaced (including identification numbers, if applicable)*] in organizational maintenance records.

Control Enhancements:

(2) Controlled Maintenance | Automated Maintenance Activities.
The organization:
(a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and
(b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

GSA Implementation Guidance: Control MA-2 is applicable at all FIPS 199 levels. Enhancement MA-2(2) is applicable at the FIPS PUB 199 High level.

The focus of this control is to ensure that all maintenance activities required for the information system are performed through a controlled process. Maintenance activities are defined as repairs to hardware and preventative maintenance, and do not include flaw remediation which is covered under control SI-2 in NIST SP 800-53. All GSA information systems must implement a controlled maintenance process. Maintenance activities should be integrated into the information system's configuration management process in order to provide the required risk-based review and approval of any potential impact to the system's security and operational status.

Removal of hardware for offsite maintenance must be approved by the System Owner, must be securely transported per requirements under control MP-5 in NIST SP 800-53, and sanitized (if necessary) consistent with the procedures in the GSA-IT Security Procedural Guide 06-32, "*Media Protection.*"

All GSA information systems' maintenance records must include:

- date and time of maintenance
- the name of the person(s) performing maintenance
- the name of escort, if necessary
- a description of the maintenance performed
- a list of any equipment removed or replaced including identification numbers, if applicable.

OCISO recommends S/SOs create standard forms to facilitate implementation of this requirement.

FIPS 199 High impact systems must use automated mechanisms for scheduling, performing and recording information system maintenance activities. Examples of automated mechanisms to be used to support the requirements of this control enhancement would include configuration management or system maintenance tracking software.

Additional Contractor System Considerations: *None.*

3.3 MA-3 Maintenance Tools

Control: The organization approves, controls, and monitors information system maintenance tools.

Control Enhancements:

(1) Maintenance Tools | Inspect Tools. The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

(2) Maintenance Tools | Inspect Media. The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

(3) Maintenance Tools | Prevent Unauthorized Removal. The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

  (a) Verifying that there is no organizational information contained on the equipment;

  (b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or
(d) Obtaining an exemption from [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] explicitly authorizing removal of the equipment from the facility.

GSA Implementation Guidance: Control MA-3 and enhancements MA-3(1) and (2) are applicable at FIPS 199 Moderate and High levels. Enhancement MA-3(3) is applicable at the FIPS 199 High level.

Systems must use only approved technologies for the performance of maintenance activities such as diagnostics and repairs. GSA provides an up-to-date list of approved technologies at the GSA Enterprise Architecture (EA) Analytics and Reporting (GEAR) website. Any tools that are brought in to a GSA facility by maintenance personnel must be inspected to ensure improper modifications have not been made that could impact the confidentiality, integrity, or availability of GSA systems and their data. Any media that contain diagnostic, test, or repair programs must be scanned for malicious code prior to being connected to a GSA information system.

All GSA FIPS 199 High impact systems must implement one or more of the following actions to prevent the unauthorized removal of organizational information on maintenance equipment.

- Verify maintenance equipment used does not contain organizational information prior to its removal.
- Sanitize or destroy maintenance equipment used consistent with the requirements in CIO-IT Security-06-32.
- Retain the maintenance equipment.
- Obtain an exemption from the GSA AO authorizing the removal of the maintenance equipment used.

Additional Contractor System Considerations: *None.*

3.4 MA-4 Nonlocal Maintenance

Control: The organization:

a. Approves and monitors nonlocal maintenance and diagnostic activities;
b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintains records for nonlocal maintenance and diagnostic activities; and
e. Terminates session and network connections when nonlocal maintenance is completed.

Control Enhancements:

(2) Nonlocal Maintenance | Document Nonlocal Maintenance. The organization documents, in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

(3) Nonlocal Maintenance | Comparable Security/Sanitization. The organization:

  (a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or

  (b) Removes the component to be serviced from the information system prior to nonlocal 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) before reconnecting the component to the information system.

GSA Implementation Guidance: Control MA-4 is applicable at all FIPS 199 levels. Enhancement MA-4(2) is applicable at FIPS 199 Moderate and High levels. Enhancement MA-4(3) is applicable at the FIPS 199 High level.

Systems must implement proper control on non-local maintenance activities. Non-local maintenance activities are performed via connection through an internal or external connection, and are not performed while physically present at the information system. Any use of non-local maintenance and diagnostic connections to the information system must be documented in the System Security Plan (SSP). These activities must be authorized and monitored and controlled as follows in accordance with this control:

- Requires multifactor authentication as specified by NIST SP 800-53 Control IA-2.
- Maintains a record of the activities (e.g., day/time, person/organization performing activities, activities performed, components maintained).
- Ends the session and network connection when activities are complete.

Note: This control is not applicable if all maintenance activities are performed locally at the information system.

For FIPS 199 High impact systems if the nonlocal maintenance/diagnostic services are not performed from an information system that implements the same level of security as the system being serviced, then the components to be serviced must be sanitized of organizational information prior to the service in accordance with CIO-IT Security-06-32. In addition, after the service is performed the component must be inspected and sanitized, if necessary (i.e., potentially malicious software is discovered during inspection), prior to returning the component to service in the information system.

Additional Contractor System Considerations: *None.*

3.5 MA-5 Maintenance Personnel

Control: The organization:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Control Enhancements:

(1) Maintenance Personnel | Individuals Without Appropriate Access. The organization:
- (a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
  - (1) 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;
  - (2) 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
- (b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

GSA Implementation Guidance: Control MA-5 is applicable at all FIPS 199 levels. Enhancement MA-5(1) is only applicable at the FIPS 199 High level.

The focus of this control is to ensure only authorized personnel and/or organizations have access to the information system for maintenance activities. A list identifying all authorized maintenance personnel and organizations/vendors must be developed and updated as necessary. System personnel must verify against this list prior to allowing maintenance personnel physical or logical access to the system.

Individuals who do not have system access authorization must be supervised at all times by designated system personnel who have the technical knowledge to effectively ensure only appropriate maintenance is performed. Maintenance personnel who require privileged access to the information such as vendor personnel or consultants may be issued temporary credentials for one-time use or for a limited access period, provided an assessment of risk has been performed which concluded that issuing such credentials/accounts is acceptable.

FIPS 199 High systems must have procedures to escort maintenance personnel who lack the appropriate clearance, are not U.S. citizens, or do not have the appropriate access authorization/approval. In addition, the system personnel must enforce one of the following options:

(1) The system's volatile information storage components must be sanitized of organizational information and nonvolatile storage media must be removed or physically disconnected from the system and secured.
(2) Develops and implements approved alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

In addition to the above, the system must uniquely identify non-organizational maintenance personnel in accordance with the requirements specified in NIST SP 800-53 Control IA-8.

Additional Contractor System Considerations: *None.*

3.6 MA-6 Timely Maintenance

Control: The organization obtains maintenance support and/or spare parts for [*GSA S/SO or Contractor recommended information system components to be approved and accepted by the GSA AO*] within [*a time period as determined by the Contingency Plan and BIA*] of failure.

GSA Implementation Guidance: Control MA-6 is applicable at the FIPS 199 Moderate and High levels.

The focus of this control is to ensure that a system is prepared for the emergency maintenance of key system components. Key system components and the timeframes within which they must be returned to service via maintenance or replacement are defined in the information system's Contingency Plan and Business Impact Assessment (BIA). Systems must ensure that maintenance support (normal and emergency) and/or spare parts are in place. Typically contractual agreements are the mechanism used to meet this requirement.

Additional Contractor System Considerations: *None.*

4 Summary

An effective, efficient maintenance process must be implemented to maintain continuous, uninterrupted operation of an information system throughout its lifecycle. Such a process ensures required maintenance is performed and that unintentional effects are not caused by maintenance activities. Maintenance activities can also provide evidence to support warranties, guarantees, and vendor service level agreements.

Where there is a conflict between NIST guidance and GSA guidance, contact the OCISO, ISP Division for guidance, at ispcompliance@gsa.gov.