IT Security Procedural Guide: Maintenance (MA) CIO-IT Security-10-50

Revision 4

November 15, 2021

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	Hag/ 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 – October 10, 2017		
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
		Revision 4 – November 15, 2021		
1	Dean/ Klemens	Revisions included: • Updated to NIST SP 800-53, Revision 5 controls • Updated format.	Align to current NIST guidance and GSA parameters.	Throughout

Approval

IT Security Procedural Guide: Maintenance (MA), CIO-IT Security 10-50, Revision 4, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

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

Table of Contents

List of Tables

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Section 1.4. For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

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 system must follow the Maintenance 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 National Institute of Standards and Technology (NIST) including NIST Special Publication (SP) 800-53, Revision 5, "*Security and Privacy Controls for Information Systems and Organizations."* This guide provides an overview of GSA maintenance roles and responsibilities, NIST SP 800-53 MA control requirements per Federal Information Processing Standard (FIPS) Publication 199, "*Standards for Security Categorization of Federal Information and Information Systems*" security categorization level, and procedures for implementing these requirements.

Executive Order (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 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 (ID), Protect (PR), Detect (DE), Respond (RS), Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework (RMF) from NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*." Table 1-1, CSF Categories/Subcategories and the NIST 800-53 MA control family lists the Categories and Subcategories from the CSF that are supported by the implementation of policies, procedures, and processes from the NIST SP 800-53 MA control family. Throughout the remainder of this guide the identifier MA will be used when referring to NIST controls or the

control family, otherwise maintenance will be used. CIO 2100.1 and this procedural guide provide GSA's policies and procedural guidance regarding maintenance of GSA IT systems and implementation of MA controls.

Table 1-1: CSF Categories/Subcategories and the Maintenance Control Family

CSF Category/Subcategory Identifier	Definition/Description
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated. *(CIO 2100.1 and Sections 1.3 and 3.1 of this guide)* **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. *(CIO 2100.1 and Section 2 of this guide)*
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. *(Sections 3.2-3.3 and 3.5-3.6 of this guide)* **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. *(Section 3.4 of this guide)*

1.1 Purpose

The purpose of this guide is to provide guidance for the MA 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. All GSA information systems must adhere to the requirements and guidance provided with regards to maintenance procedures, processes, and methods as described in this guide. Per CIO 2100.1, a GSA information system is an information system:

- used or operated by GSA; or
- used or operated on behalf of GSA by a contractor of GSA or by another organization.

1.3 Policy

CIO 2100.1 contains the following policy statements regarding maintenance.

Chapter 4, Policy for Protect Function

1. Identity Management, Authentication and Access Control

v. Remote access/endpoint security

(5) In special cases for remote administration and maintenance tasks, contractors will be allowed restricted IPsec access to specific GSA IP addresses (contingent on passing the scans noted above). [Note: Scans are detailed in another section of CIO 2100.1.]

w. Remote access to the GSA domain must be restricted to secure methods using approved identification and authentication methods that provide detection of intrusion attempts and protection against unauthorized access

5. Maintenance.

a. Maintenance and repair of organizational assets must be performed and recorded with approved tools IAW GSA CIO-IT Security-10-50.

b. Maintenance of agency hardware and software must be restricted to authorized personnel.

c. System administration and patch implementation must be restricted to authorized personnel.

d. Remote or non-local maintenance of organizational assets must be authorized, recorded, and authenticated via MFA IAW GSA CIO-IT Security-10-50.

1.4 References

Federal Laws, Standards, Regulations, and Publications:

- EO 13800, *"Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"*
- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- NIST CSF, "Framework for Improving Critical Infrastructure Cybersecurity"
- NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"*
- NIST SP 800-53, Revision 5, "*Security and Privacy Controls for Information Systems and Organizations*"

GSA Policies, Procedures, Guidance:

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"

The GSA CIO-IT Security Procedural Guides listed below are available on the IT Security Procedural Guides page.

- CIO-IT Security-06-30, "*Managing Enterprise Cybersecurity Risk*"
- CIO-IT Security-06-32, "*Media Protection (MP)*"
- CIO-IT Security-09-44, "*Plans of Action & Milestones (POA&M)*"
- CIO-IT Security-18-90, "*Information Security Program Plan (ISPP)*"

2 Roles and Responsibilities

There are many roles associated with effectively maintaining information 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. The responsibilities listed in this guide are focused on maintaining information systems; a complete set of GSA security roles and responsibilities can be found in CIO 2100.1, Chapter 2. Throughout this guide, specific processes and procedures for implementing NIST's MA controls are described.

2.1 Chief Information Security Officer (CISO)

Responsibilities include the following:

- Implementing and overseeing GSA's IT Security Program by developing and publishing security policies and IT security procedural guides that are consistent with the policy.
- Manage the development, documentation, and dissemination of the maintenance policy and procedures with regard to MA controls.
- Ensuring IT Acquisitions align with GSA information security requirements.
- Providing guidance, advice, and assistance to all S/SO/R on IT security issues, the IT Security Program, and security policies.

2.2 Authorizing Officials (AOs)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required MA controls in accordance with GSA and Federal policies and requirements.
- Identifying the level of acceptable risk for an information system and determining whether an acceptable level of risk has been obtained, including risks associated with MA controls.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current authorization to operate (ATO) issued IAW GSA CIO-IT Security-06-30.
- Ensuring a plan of action and milestones (POA&M) entry is created and managed to address any MA controls that are not fully implemented.

2.3 Information Systems Security Managers (ISSMs)

Responsibilities include the following:

- Verifying systems under their purview have appropriately addressed NIST SP 800-53 MA controls, assisting ISSOs, as necessary, to ensure MA controls are in place and operating as intended.
- Coordinating with the AO, System Owner, ISSOs, and OCISO Directors, as necessary, regarding MA control implementation and compliance with NIST and GSA requirements.

- Working with the ISSO and System Owner to develop, implement, and manage POA&Ms regarding MA controls that are not fully implemented for their respective systems IAW GSA CIO-IT Security-09-44.

2.4 Information Systems Security Officers (ISSOs)

Responsibilities include the following:

- Ensuring necessary MA controls are in place and operating as intended.
- Coordinating with ISSMs and System Owners, as necessary, regarding MA control implementation and compliance with NIST and GSA requirements.
- Working with the System Owner and ISSM to develop, implement, and manage POA&Ms regarding MA controls that are not fully implemented for their respective systems IAW GSA CIO-IT Security-09-44.

2.5 System Owners (SOs)

Responsibilities include the following:

- Ensuring necessary MA controls are in place and operating as intended.
- Coordinating with ISSOs and ISSMs, as necessary, regarding MA control implementation and compliance with NIST and GSA requirements.
- Working with ISSOs and ISSMs to develop, implement, and manage POA&Ms regarding MA controls that are not fully implemented for their respective systems IAW GSA CIO-IT Security-09-44.
- Ensuring records of maintenance performed in support of MA controls are documented and retained in accordance with GSA and Federal guidance.
- Obtaining the resources necessary to securely implement and manage MA controls for their respective systems.

2.6 Custodians

Responsibilities include the following:

- Coordinating with ISSMs, ISSOs, and System Owners to ensure maintenance in support of MA controls is supported and performed.
- Ensuring records of maintenance performed in support of MA controls are documented and retained in accordance with GSA and Federal guidance.

2.7 System/Network Administrators

Responsibilities include the following:

- Ensuring the appropriate MA controls are implemented consistent with GSA IT security policies and guidelines as described in this guide.
- Performing maintenance in support of MA controls, documenting its performance, and retaining the records in accordance with GSA and Federal guidance.

3 GSA Implementation Guidance for MA Controls

The GSA-defined parameter settings included in the control requirements are in blue, italicized text and offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to all GSA systems and must be followed by all GSA Federal employees and contractors involved in the maintenance of GSA information systems. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions or requirements for contractor systems will be included in the "Additional Contractor System Considerations" portion of each control section.

Table 3-1 identifies the designation of MA controls as Common, Hybrid, or System-Specific Controls for both Federal and Contractor systems. Effectively, common controls are provided by GSA at the enterprise level or by one of GSA's Major Information Systems (e.g., General Support System), system specific controls are implemented at the system level, and hybrid controls have shared responsibilities. CIO-IT Security-18-90, the ISPP, describes the GSA enterprise-wide common and hybrid controls and outlines the responsible parties for implementing them.

Note: Until the ISPP is updated to NIST SP 800-53, Revision 5, contact ispcompliance@gsa.gov for guidance if there is a discrepancy between this guide and the ISPP.

Table 3-1: Designation of MA Controls

System Type	Federal	Contractor
Common	MA-1	
Hybrid	MA-4, MA-5	MA-1
System-Specific	MA-2, 2(2); MA-3, 3(1), 3(2), 3(3), MA-4(3); MA-5(1); MA-6	MA-2, 2(2); MA-3, 3(1), 3(2), 3(3), MA-4, 4(3); MA-5, 5(1); MA-6

Table 3-2 identifies GSA MA control applicability at the FIPS 199 Low, Moderate, and High levels.

Table 3-2: GSA Designation of MA Control Applicability

FIPS 199 Level	Applicable Controls
Low	MA-1, MA-2, MA-4, MA-5
Moderate	MA-1, MA-2, MA-3, MA-3(1), MA-3(2), MA-3(3), MA-4, MA-5, MA-6
High	MA-1, MA-2, MA-2(2), MA-3, MA-3(1), MA-3(2), MA-3(3), MA-4, MA-4(3), MA-5, MA-5(1), MA-6

3.1 MA-1 Policy and Procedures

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
   1. [*Organization-level*] maintenance policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
c. Review and update the current maintenance:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

GSA Implementation Guidance: Control MA-1 is applicable at all FIPS 199 levels. MA-1 is a Common Control for Federal systems and a Hybrid Control for Contractor systems.

Common Control Implementation:

The GSA maintenance policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding the maintenance for GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site.

Maintenance procedures are documented in CIO-IT Security-10-50, "*IT Security Procedural Guide: Maintenance (MA)*" [this guide]. The procedures facilitate the implementation of the maintenance policy and associated controls. The guide is disseminated GSA-wide via GSA's InSite centralized agency web site.

Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.

The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually.

The GSA OCISO is responsible for reviewing and updating CIO-IT Security-10-50 every three years and following changes to Federal or GSA policies, requirements, or guidance.

Federal System System-Specific Expectation:
None, MA-1 is a common control. However, GSA Services/Staff Offices (S/SO) or System Owners may augment the maintenance policies and procedures included in 2100.1 and CIO-IT Security-10-50 to address additional organizational or system-specific maintenance requirements. Any such policies and procedures must establish timeframes for updating them.

Additional Contractor System Considerations: Vendors/contractors may defer to the GSA policy and guide or implement their own maintenance policies and procedures which comply with GSA's requirements with the approval of the Authorizing Official (AO).

Note: Contractor systems, per CIO 2100.1, are information systems in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.

3.2 MA-2 Controlled Maintenance

Control:

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
c. Require that [*Information System Security Manager, Information System Security Officer, System Owners, Custodians*] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [*Controlled Unclassified Information, system configuration information (e.g., account names, internal IP addresses, etc.)*];
e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
f. Include the following information in organizational maintenance records: *[(1) Date and time of maintenance, (2) Name of the individual performing the maintenance, (3) Name of escort, if necessary, (4) A description of the maintenance performed, (5) A list of equipment removed or replaced (including identification numbers, if applicable)*].

Control Enhancements:

(2) Controlled Maintenance | Automated Maintenance Activities.
  (a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [*ServiceNow or automated mechanisms as defined in the system CM Plan*]; and
  (b) Produce up-to-date, accurate, and complete records of all maintenance, repair and replacement actions requested, scheduled, in process, and completed.

GSA Implementation Guidance: Control MA-2 is applicable at all FIPS 199 levels. Control MA-2(2) is applicable at the FIPS 199 High level. MA-2 and 2(2) are System-Specific Controls for both Federal and Contractor systems.

Federal System System-Specific Expectation:
The focus of this control is to ensure that all maintenance activities required for the information system are performed through a controlled process, including appropriate approvals and monitoring. 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 (CM) process in order to provide the required risk-based review and approval of any potential impact to the system's security and operational status and other security controls.

Removal of the system or system components for maintenance must be approved by the System Owner. Any component with associated media that is removed for off-site maintenance must adhere to the guidance in CIO-IT Security-06-32.

All GSA information systems' maintenance records must include:

- the date and time of maintenance
- a description of the maintenance performed
- the names of the individuals or group performing the maintenance
- the name of the escort
- a list of system components or equipment that are removed or replaced

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

For MA-2(2), 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 CM or system maintenance tracking software.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.3 MA-3 Maintenance Tools

Control:

a. Approve, control, and monitor the use of system maintenance tools; and
b. Review previously approved system maintenance tools [*annually as part of CM Plan review*].

Control Enhancements:

(1) Maintenance Tools | Inspect Tools. Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications

(2) Maintenance Tools | Inspect Media. Check media containing diagnostic and test programs for malicious code before the media are used in the system.
(3) Maintenance Tools | Prevent Unauthorized Removal. Prevent the removal of maintenance equipment containing organizational information by:
  (a) Verifying that there is no organizational information by:
  (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, Custodians*] explicitly authorizing removal of the equipment from the facility.

GSA Implementation Guidance: Controls MA-3, 3(1), 3(2), and 3(3) are applicable at the FIPS 199 Moderate and High levels; they are System-Specific Controls for both Federal and Contractor systems.

Federal System System-Specific Expectation:
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 into 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. Approved systems maintenance tools must be reviewed annually as part of the annual review of the system's CM plan to determine their use is still relevant to the system.

For MA-3(3) – 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 System Owner, Custodian, and GSA ISSO/ISSM, authorizing the removal of the maintenance equipment used.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.4 MA-4 Nonlocal Maintenance

Control

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintain records for nonlocal maintenance and diagnostic activities; and
e. Terminate session and network connections when nonlocal maintenance is completed

Control Enhancements:

(3) Nonlocal Maintenance | Comparable Security and Sanitization.
  (a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or
  (b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

GSA Implementation Guidance: Control MA-4 is applicable at all FIPS 199 levels. Control MA-4(3) is applicable at the FIPS 199 High level. MA-4 is a Hybrid Control for Federal systems, and a System-Specific Control for Contractor systems. MA-4(3) is a System-Specific Control for Federal and Contractor systems.

Proper control must be maintained on non-local maintenance activities. Non-local maintenance activities are performed via internal or external connections 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 and Privacy Plan (SSPP). 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.

For MA-4(3), 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.

Federal System Common Control Implementation:

The common portion of nonlocal maintenance services are managed by GSA's GSSs, Platforms, or major information systems (e.g., Enterprise Infrastructure Operations [EIO]).

Federal System System-Specific Expectation:
Regarding the provision of common nonlocal maintenance, the system owner of a hosted system must communicate with the system (e.g., EIO) they are inheriting the nonlocal maintenance services from, in order to ensure scheduling conflicts do not arise where systems are trying to perform functions while nonlocal maintenance is occurring.

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

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.5 MA-5 Maintenance Personnel

Control:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;
b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
c. Designate 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
  (a) Implement 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 system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and
    (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 system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
  (b) Develop and implement [*GSA S/SO or Contractor recommended alternate controls approved by the GSA CISO and AO*] in the event a system component cannot be sanitized, removed, or disconnected from the system.

GSA Implementation Guidance: Control MA-5 is applicable at all FIPS 199 levels. Control MA-5(1) is applicable at the FIPS 199 High level. MA-5 is a Hybrid Control for Federal systems, and a System-Specific Control for Contractor systems. MA-5(1) is System-Specific Control for Federal and Contractor systems.

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.

For MA-5(1), 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.

Federal System Common Control Implementation:
The common portion of the maintenance personnel control is managed by GSA's GSSs, Platforms, or major information systems (e.g., Enterprise Infrastructure Operations [EIO]).

Federal System System-Specific Expectation:
Regarding maintenance personnel, the system owner of a hosted system must coordinate with the system (e.g., EIO) they are inheriting the maintenance personnel control from, in order to ensure the maintenance personnel are authorized have the required access authorizations for their system and provide supervision for any who do not possess the required authorizations.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.6 MA-6 Timely Maintenance

Control: Obtain maintenance support and/or spare parts for [*GSA S/SO or Contractor recommended information system components to be approved by the GSA CISO and 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. MA-6 is a System-Specific Control for both Federal and Contractor systems.

Federal System System-Specific Expectation:
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 Analysis (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: Vendors/contractors are required to comply with the control statements.

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.