3.9 MAINTENANCE

Quick link to Maintenance Summary Table

MA-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-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 [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

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 [*Assignment: organization-defined personnel or roles*] 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: [*Assignment: organization-defined information*];

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: [*Assignment: organization-defined information*].

Discussion: Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

Related Controls: CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.

Control Enhancements:

(1) CONTROLLED MAINTENANCE | RECORD CONTENT

[Withdrawn: Incorporated into MA-2.]

(2) CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES

(a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [*Assignment: organization-defined automated mechanisms*]; and

(b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

Discussion: The use of automated mechanisms to manage and control system maintenance programs and activities helps to ensure the generation of timely, accurate, complete, and consistent maintenance records.

Related Controls: MA-3.

References: [OMB A-130], [IR 8023].

MA-3 MAINTENANCE TOOLS

Control:

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools [*Assignment: organization-defined frequency*].

Discussion: Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

Related Controls: MA-2, PE-16.

Control Enhancements:

(1) MAINTENANCE TOOLS | INSPECT TOOLS

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Discussion: Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related Controls: SI-7.

(2) MAINTENANCE TOOLS | INSPECT MEDIA

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Discussion: If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related Controls: SI-3.

(3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL

Prevent the 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 [*Assignment: organization-defined personnel or roles*] explicitly authorizing removal of the equipment from the facility.

Discussion: Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

Related Controls: MP-6.

(4) MAINTENANCE TOOLS | RESTRICTED TOOL USE

Restrict the use of maintenance tools to authorized personnel only.

Discussion: Restricting the use of maintenance tools to only authorized personnel applies to systems that are used to carry out maintenance functions.

Related Controls: AC-3, AC-5, AC-6.

(5) MAINTENANCE TOOLS | EXECUTION WITH PRIVILEGE

Monitor the use of maintenance tools that execute with increased privilege.

Discussion: Maintenance tools that execute with increased system privilege can result in unauthorized access to organizational information and assets that would otherwise be inaccessible.

Related Controls: AC-3, AC-6.

(6) MAINTENANCE TOOLS | SOFTWARE UPDATES AND PATCHES

Inspect maintenance tools to ensure the latest software updates and patches are installed.

Discussion: Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations.

Related Controls: AC-3, AC-6.

References: [SP 800-88].

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.

Discussion: Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished, in part, by other controls. [SP 800-63B] provides additional guidance on strong authentication and authenticators.

Related Controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.

Control Enhancements:

(1) NONLOCAL MAINTENANCE | LOGGING AND REVIEW

(a) Log [*Assignment: organization-defined audit events*] for nonlocal maintenance and diagnostic sessions; and

(b) Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

Discussion: Audit logging for nonlocal maintenance is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls: AU-6, AU-12.

(2) NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE

[Withdrawn: Incorporated into MA-1 and MA-4.]

(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.

Discussion: Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

Related Controls: MP-6, SI-3, SI-7.

(4) NONLOCAL MAINTENANCE | AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS

Protect nonlocal maintenance sessions by:

(a) Employing [*Assignment: organization-defined authenticators that are replay resistant*]; and

(b) Separating the maintenance sessions from other network sessions with the system by either:

(1) Physically separated communications paths; or

(2) Logically separated communications paths.

Discussion: Communications paths can be logically separated using encryption.

Related Controls: None.

(5) NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS

(a) Require the approval of each nonlocal maintenance session by [*Assignment: organization-defined personnel or roles*]; and

(b) Notify the following personnel or roles of the date and time of planned nonlocal maintenance: [*Assignment: organization-defined personnel or roles*].

Discussion: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance is accomplished by personnel with sufficient information security and system knowledge to determine the appropriateness of the proposed maintenance.

Related Controls: None.

(6) NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION

Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: [*Assignment: organization-defined cryptographic mechanisms*].

Discussion: Failure to protect nonlocal maintenance and diagnostic communications can result in unauthorized individuals gaining access to organizational information. Unauthorized

access during remote maintenance sessions can result in a variety of hostile actions, including malicious code insertion, unauthorized changes to system parameters, and exfiltration of organizational information. Such actions can result in the loss or degradation of mission or business capabilities.

Related Controls: SC-8, SC-12, SC-13.

(7) NONLOCAL MAINTENANCE | DISCONNECT VERIFICATION

Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

Discussion: Verifying the termination of a connection once maintenance is completed ensures that connections established during nonlocal maintenance and diagnostic sessions have been terminated and are no longer available for use.

Related Controls: AC-12.

References: [FIPS 140-3], [FIPS 197], [FIPS 201-2], [SP 800-63-3], [SP 800-88].

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.

Discussion: Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Related Controls: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

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 [*Assignment: organization-defined alternate controls*] in the event a system component cannot be sanitized, removed, or disconnected from the system.

Discussion: Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens are intended to deny visual and electronic access to classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

Related Controls: MP-6, PL-2.

(2) MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of information on the system.

Discussion: Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. To mitigate the inherent risk of such exposure, organizations use maintenance personnel that are cleared (i.e., possess security clearances) to the classification level of the information stored on the system.

Related Controls: PS-3.

(3) MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.

Discussion: Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. If access to classified information on organizational systems is restricted to U.S. citizens, the same restriction is applied to personnel performing maintenance on those systems.

Related Controls: PS-3.

(4) MAINTENANCE PERSONNEL | FOREIGN NATIONALS

Ensure that:

(a) Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and

(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.

Discussion: Personnel who conduct maintenance and diagnostic activities on organizational systems may be exposed to classified information. If non-U.S. citizens are permitted to perform maintenance and diagnostics activities on classified systems, then additional vetting is required to ensure agreements and restrictions are not being violated.

Related Controls: PS-3.

(5) MAINTENANCE PERSONNEL | NON-SYSTEM MAINTENANCE

Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.

Discussion: Personnel who perform maintenance activities in other capacities not directly related to the system include physical plant personnel and custodial personnel.

Related Controls: None.

References: None.

MA-6 TIMELY MAINTENANCE

Control: Obtain maintenance support and/or spare parts for [*Assignment: organization-defined system components*] within [*Assignment: organization-defined time period*] of failure.

Discussion: Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

Related Controls: CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4.

Control Enhancements:

(1) TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE

Perform preventive maintenance on [*Assignment: organization-defined system components*] at [*Assignment: organization-defined time intervals*].

Discussion: Preventive maintenance includes proactive care and the servicing of system components to maintain organizational equipment and facilities in satisfactory operating condition. Such maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects. The primary goal of preventive maintenance is to avoid or mitigate the consequences of equipment failures. Preventive maintenance is designed to preserve and restore equipment reliability by replacing worn components before they fail. Methods of determining what preventive (or other) failure management policies to apply include original equipment manufacturer recommendations; statistical failure records; expert opinion; maintenance that has already been conducted on similar equipment; requirements of codes, laws, or regulations within a jurisdiction; or measured values and performance indications.

Related Controls: None.

(2) TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE

Perform predictive maintenance on [*Assignment: organization-defined system components*] at [*Assignment: organization-defined time intervals*].

Discussion: Predictive maintenance evaluates the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold. The predictive component of predictive maintenance stems from the objective of predicting the future trend of the equipment's condition. The predictive maintenance approach employs principles of statistical process control to determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thus minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability.

Related Controls: None.

(3) TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE

Transfer predictive maintenance data to a maintenance management system using [*Assignment: organization-defined automated mechanisms*].

Discussion: A computerized maintenance management system maintains a database of information about the maintenance operations of organizations and automates the processing of equipment condition data to trigger maintenance planning, execution, and reporting.

Related Controls: None.

References: None.

MA-7 FIELD MAINTENANCE

Control: Restrict or prohibit field maintenance on [*Assignment: organization-defined systems or system components*] to [*Assignment: organization-defined trusted maintenance facilities*].

Discussion: Field maintenance is the type of maintenance conducted on a system or system component after the system or component has been deployed to a specific site (i.e., operational environment). In certain instances, field maintenance (i.e., local maintenance at the site) may not be executed with the same degree of rigor or with the same quality control checks as depot maintenance. For critical systems designated as such by the organization, it may be necessary to restrict or prohibit field maintenance at the local site and require that such maintenance be conducted in trusted facilities with additional controls.

Related Controls: MA-2, MA-4, MA-5.

Control Enhancements: None.

References: None.