

Department of the Interior
Security Control Standard
Maintenance

January 2012

Version: 1.2



Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	Date:

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 14, 2011	Initial draft
Timothy Brown	0.2	January 20, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	January 18, 2012	Incorporated the additional MA-5 control enhancements applicable to all Moderate and High systems

TABLE OF CONTENTS

REVISION HISTORY	3
TABLE OF CONTENTS	4
SECURITY CONTROL STANDARD: MAINTENANCE.....	5
MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES	5
MA-2 CONTROLLED MAINTENANCE	6
MA-3 MAINTENANCE TOOLS	7
MA-4 NON-LOCAL MAINTENANCE.....	7
MA-5 MAINTENANCE PERSONNEL	8
MA-6 TIMELY MAINTENANCE.....	10

SECURITY CONTROL STANDARD: MAINTENANCE

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Maintenance (MA) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

- a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in

general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW MA-1	MOD MA-1	HIGH MA-1
-----------	-----------------	-----------------	------------------

MA-2 CONTROLLED MAINTENANCE

Applicability: All Information Systems

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. Controls 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 a designated official 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; and
- e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Supplemental Guidance: The control is intended to address the information security aspects of the organization's information system maintenance program. Related controls: MP-6, SI-2.

Control Enhancements:

1. The organization maintains maintenance records for the information system that include:
 - a. Date and time of maintenance;
 - b. Name of the individual performing the maintenance;
 - c. Name of escort, if necessary;
 - d. A description of the maintenance performed; and
 - e. A list of equipment removed or replaced (including identification numbers, if applicable).
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.

References: None.

Priority and Baseline Allocation:

P2	LOW MA-2	MOD MA-2 (1)	HIGH MA-2 (1) (2)
-----------	-----------------	---------------------	--------------------------

MA-3 MAINTENANCE TOOLS

Applicability: Moderate and High Impact Information Systems

Control: The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.

Supplemental Guidance: The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

Related control: MP-6.

Control Enhancements:

1. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

2. The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.
3. The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.

References: NIST Special Publication 800-88.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MA-3 (1) (2) (3)	HIGH MA-3 (1) (2) (3)
-----------	-------------------------	-----------------------------	------------------------------

MA-4 NON-LOCAL MAINTENANCE

Applicability: All Information Systems

Control: The organization:

- 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.

Supplemental Guidance: Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. Strong authenticators include, for example, 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. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6, SC-7.

Control Enhancements:

- 1. The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.
- 2. The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.
- 3. The organization:
 - 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
 - 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.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.

Priority and Baseline Allocation:

P1	LOW MA-4	MOD MA-4 (1) (2)	HIGH MA-4 (1) (2) (3)
-----------	-----------------	-------------------------	------------------------------

MA-5 MAINTENANCE PERSONNEL

Applicability: All Information Systems

Control: The organization:

- a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and

- 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 personnel do not possess the required access authorizations.

Supplemental Guidance: Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period. Related controls: IA-8, MA-5.

Control Enhancements:

1. The organization maintains procedures for the use of maintenance personnel that lack appropriate background investigations and security clearances or are not U.S. citizens, that include the following requirements:
 - 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;
 - 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
 - c. In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.

Enhancement Supplemental Guidance: The intent of this control enhancement is to deny individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any Controlled Unclassified Information (CUI); information subject to the Privacy Act, including Personally Identifiable Information (PII); or any other sensitive agency information contained on the information system. Procedures for the use of maintenance personnel shall be documented in the security plan for the information system.

2. The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting sensitive agency information are cleared (i.e., possess appropriate background investigations and security clearances) for the highest level of information on the system.
3. The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting sensitive agency information are U.S. citizens.

References: None.

Priority and Baseline Allocation:

P1	LOW MA-5	MOD MA-5 (1) (2) (3)	HIGH MA-5 (1) (2) (3)
-----------	-----------------	-----------------------------	------------------------------

MA-6 TIMELY MAINTENANCE

Applicability: Moderate and High Impact Information Systems

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 the time periods defined in accordance with the contingency plan and business impact analysis for the information system.

Supplemental Guidance: The organization specifies those information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems. Related control: CP-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MA-6	HIGH MA-6
-----------	-------------------------	-----------------	------------------