Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Maintenance (MA) Procedure

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Maintenance (MA) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

2. SCOPE

These procedures address all United States EPA information and information systems to include information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. BACKGROUND

EPA is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems. All EPA information systems shall meet security requirements by implementing the security controls defined in the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

This document adopts procedures and standards for the EPA consistent with FIPS Publication 200.

5. AUTHORITY

Additional legal foundations for the Maintenance Procedure include:

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)

- OMB Circular A-130, "Managing Information as a Strategic Resource," Appendix I, "Responsibilities for Protecting and Managing Federal Information Resources," July 2016
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

6. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide, and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "MA" designator (e.g., MA-2, MA-3) identified for each procedure below corresponds to the NIST- identifier for the Maintenance control family, as identified in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*.

NIST defines the applicable MA security and privacy baseline controls in NIST 800-53B, Control Baselines for Information Systems and Organizations. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name.

MA-2 – Controlled Maintenance

For All Systems:

1) Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2) 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;
3) Require that the SO (ISO in the event the SO is unavailable) or property owner reviews requests from system administrators (SA) and explicitly approves the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
4) Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: all information including Controlled Unclassified Information (CUI) and other EPA sensitive information;

5) Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
6) Include the following information in organizational maintenance records:
   a) Date and time of maintenance;
   b) Name and organization of individual(s) performing the maintenance;
   c) Name of escort, if applicable;
   d) Description of maintenance performed;
   e) List of equipment removed or replaced (including identification numbers, if applicable); and
   f) Details on all items installed as listed as part of the system component inventory in CM-8.

MA-2(2) – Controlled Maintenance | Automated Maintenance Activities

For High Systems:

1) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using automated mechanisms; and
2) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

MA-3 – Maintenance Tools

For Moderate and High Systems:

1) Approve, control, and monitor the use of system maintenance tools; and
2) Review previously approved system maintenance tools annually.

MA-3(1) – Maintenance Tools | Inspect Tools

For Moderate and High Systems:

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

MA-3(2) – Maintenance Tools | Inspect Media

For Moderate and High Systems:

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

MA-3(3) – Maintenance Tools | Prevent Unauthorized Removal

For Moderate and High Systems:

1) 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 the Region/Program Office SIO explicitly authorizing removal of the equipment from the facility.

MA-4 – Non-local Maintenance

For All Systems:

1) Approve and monitor nonlocal maintenance and diagnostic activities;
2) Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
3) Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
4) Maintain records for nonlocal maintenance and diagnostic activities; and
5) Terminate session and network connections when nonlocal maintenance is completed.

MA-4(3) – Non-Local Maintenance | Comparable Security and Sanitization

For High Systems:

1) 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
2) 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.

MA-5 – Maintenance Personnel

For All Systems:

1) Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;
2) Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
3) 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.

MA-5(1) – Maintenance Personnel | Individuals Without Appropriate Access

For High Systems:

1) Implement procedures for the use of maintenance personnel that lack appropriate 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 system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and
   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 system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
2) Develop and implement alternate security safeguards, approved by (but not created by) the SO and ISO in the event a system component cannot be sanitized, removed, or disconnected from the system.

MA-6 – Timely Maintenance

For Moderate and High Systems:

1) Obtain maintenance support and/or spare parts for critical components needed for mission performance or business operations within the time specified in the Recovery Time Objectives (RTO) established in the Business Impact Analysis (BIA) or Contingency Plan of failure.

7. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

8. RELATED INFORMATION

The information listed below relates to the Maintenance Procedure

- NIST Special Publications, 800 series

9. DEFINITIONS

Definitions which pertain to the Maintenance Procedure are listed below.

- **Information System:** discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- **Information Technology:** any services, equipment or interconnected system(s) or subsystem(s) of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the Agency. For purposes of this definition, such services or equipment if used by the Agency directly or is used by a contractor under a contract with the Agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service) and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.
- **Local Maintenance:** 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.
- **Nonlocal Maintenance:** nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., Internet) or an internal network.
- **Records:** the recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
- **Signature (of an individual):** a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation. Can be accomplished manually, sometimes referred to as a “wet signature,” or electronically.
- **Significant Change:** a change that is likely to substantively affect the security or privacy posture of a system.
- **Written (or in writing):** to officially document the action or decision, either manually or electronically, and includes a signature.

10. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA’s Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

11. MATERIAL SUPERSEDED

Information Directive: CIO 2150-P-09.2, Information Security – Interim Maintenance Procedures.

12. CONTACTS

For further information, please contact the OMS, Office of Information Security and Privacy (OISP).

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2023.06.20 14:06:30 -04'00'

Vaughn Noga
Chief Information Officer and Deputy Assistant Administrator
for Environmental Information
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

BIA	Business Impact Assessment
CUI	Controlled Unclassified Information
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IT	Information Technology
MA	Maintenance
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
OMS	Office of Mission Support
PII	Personally Identifiable Information
SIO	Senior Information Official
SO	System Owner
SP	Special Publication
U.S.C.	United States Code