INFORMATION DIRECTIVE
INTERIM PROCEDURE

Information Security – Interim Maintenance Procedure		
Directive No.: 2150-P-09.2	CIO Approval: 12/28/2016	Transmittal No.: 17-004e

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

Information Security - Interim Maintenance Procedure

1. PURPOSE

To extend and provide specificity to the Environmental Protection Agency (EPA) Information Security Policy. This document shall be used to develop procedures, standards and guidance that facilitate the implementation of security control requirements for the Systems Maintenance (MA) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE

The procedure covers all 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.

The procedure applies to all EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

Based on federal requirements and mandates, the 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 through the use of the security controls defined in the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. This document addresses the procedures and standards set forth by the EPA, and complies with the Maintenance Policy and Procedures family of controls.

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act, as amended
- Cybersecurity Act of 2015, Public Law 114-113

- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic FOIA Amendments of 1996
- 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.)
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3519)
- Privacy Act of 1974 (5 U.S.C. § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—"Employees Responsible for the Management or Use of Federal Computer Systems", Section 930.301 through 930.305 (5 C.F.R. 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-06-16, "Protection of Sensitive Agency Information," June 2006
- OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Information Resources," November 2000
- FIPS 140-2, Security Requirements for Cryptographic Modules, May 2001
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA Information Security Continuous Monitoring Strategic Plan
- CIO (Chief Information Officer) Policy Framework and Numbering System

6. PROCEDURE

The "MA" designator identified in each procedure represents the NIST-specified identifier for the Maintenance Procedures control family, as identified in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

MA-1 – System Maintenance Policy and Procedures

For All Information Systems:

1) The Director of the Office of Information Technology Operations (OITO), in coordination with System Owners (SO), Information Security Officers (ISO), Information Owners (IO), Information Management Officers (IMO), and Information System Security Officers (ISSO) shall; and Service Managers (SM), in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Develop, document and disseminate to all EPA employees, contractors and other users of EPA systems:
        i) A system maintenance policy which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(1) Policies shall be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance where applicable.

ii) Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.

(1) Procedures shall be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance where applicable.

b) Review and update the current:
i) System maintenance policy annually; and
ii) System maintenance procedures annually.

For FedRAMP[1] Low and Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:
a) Review and update the current:
i) System maintenance policy at least every 3 years; and
ii) System maintenance procedures at least annually.

For FedRAMP High Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:
a) Review and update the current:
i) System maintenance policy at least annually; and
ii) System maintenance procedure at least annually.

MA-2 – Controlled Maintenance

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Schedule and perform maintenance and repairs on information system components in accordance with manufacturer or vendor specifications, and/or EPA requirements.

i) The maintenance schedule and procedures shall be documented in a Maintenance Plan.

(1) The Maintenance Plan shall address how the maintenance schedule is managed and the Point of Contact (POC) for scheduled maintenance.

(2) Scheduled maintenance shall include controls to monitor the completion of maintenance in accordance with the information system's documented maintenance schedule and vendor recommendations.

[1] *The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.*

(3) If a manufacturer, vendor or developer-provided maintenance schedule does not exist, the system shall be reviewed every three months in order to determine if maintenance is required.

(4) Any maintenance action that shall be performed outside of the scheduled maintenance timeframes shall adhere to the information system's documented procedures for unscheduled maintenance.

b) Document maintenance and repair activities, including non-local maintenance and diagnostics. The maintenance records shall be reviewed monthly.

c) Ensure that maintenance of an information system that requires a configuration change adheres to the requirements in Information Security – Configuration Management Procedures.

d) Control all maintenance activities under any circumstances:
   i) Whether performed on site or remotely.
   ii) Whether the equipment is serviced on site or removed for maintenance in another location.

e) Ensure the removal of any information system or system components from organizational facilities for off-site maintenance adheres to the following requirements:

   i) Explicit approval from a designated official shall be obtained.
   ii) All information from associated media shall be removed through sanitization prior to equipment being removed from organizational facilities. This applies not only to components or media containing Personally Identifiable Information (PII) and other EPA sensitive information, but all EPA information.
      (1) Refer to Information Security – Media Protection Procedures for requirements on proper media handling and sanitization.
   iii) Maintenance contracts with third-party providers or vendors shall include Service Level Agreements (SLA) that are sufficient to support the information system's availability requirements and mission criticality.
   iv) NIST SP 800-35 shall be used as guidance on information technology (IT) security services.
      (1) Refer to Information Security – Personnel Security Procedures and Information Security – System and Services Acquisition Procedures for requirements on IT security services.
   v) Notification shall be provided to all impacted users informing them of scheduled, unscheduled and emergency maintenance on the information system.
      (1) Email notification is preferable for external users.
      (2) Notification via the web for external users shall consider the extent of information and detail of information disclosed.
         (a) For example, naming servers in the notification may provide information for social engineering threats.
      (3) Help desk personnel shall be notified and reminded not to provide unauthorized information unless the identity of the user can be confirmed. The following shall be addressed in the notification:
         (a) The expected start and finish time of the maintenance.
         (b) The purpose of the maintenance activity.

(c) The specific information systems or subcomponents that may be impacted by the maintenance.
(d) Any actions required of the impacted users in coordination with the maintenance effort.
(e) Contact information should a user have any questions or concerns related to the maintenance effort.

(4) An updated notification shall be sent should the expected start or finish time or any other parameter of the maintenance change.
(5) The System Owner and the party that requested the maintenance, if applicable, shall be notified when maintenance is completed.
(6) Following maintenance or repair actions, the security features and controls shall be checked to verify that they are still functioning properly.
(7) Maintenance records for the information system shall include the following:
(a) Date and time of maintenance.
(b) Name 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).
(8) Maintenance records of the aforementioned items shall be kept on file.

MA-2 (1) – Controlled Maintenance | Record Content

Incorporated into MA-2.

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

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Employ automated mechanisms to ensure that maintenance and repairs are scheduled, conducted and documented as required, producing a log of maintenance and repair actions (needed, in process, and completed) that is up-to-date, accurate, complete and available.

b) Ensure the creation and maintenance of up-to-date, accurate and complete records of all maintenance and repair actions requested, scheduled, in-process and completed.

MA-3 – Maintenance Tools

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Ensure the use of information system maintenance tools is approved, controlled and monitored.

Note: This procedure addresses 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 hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this procedure.

b) Use approved maintenance tools that are defined and documented in the Maintenance Plan.

i) If a tool is needed (e.g., in emergency maintenance situations) and the tool is not listed in the Maintenance Plan, written approval shall be given by the SO.

(1) The SO's written approval shall then be included as an attachment to the Maintenance Plan after the fact.
(2) Once the emergency maintenance has been performed on the information system, one of the following actions shall be taken:
(a) The tool shall be formally documented and added to the list in the Maintenance Plan.
(b) The tool shall be removed from the information system and no longer used.
(i) Any maintenance ports, services, and protocols that, according to configuration standards, shall be disabled, but shall be used by approved maintenance tools, are only permitted to be enabled during maintenance.
(1) Refer to Information Security – Configuration Management Procedures for requirements on ports, services and protocols.

ii) The approved tools shall be maintained on an ongoing basis.

(1) A maintenance schedule shall include the maintenance of the information system's maintenance tools and the schedule shall be documented in the Maintenance Plan.

(2) Maintenance tools shall receive vendor-recommended maintenance, and the maintenance shall be documented with other information system maintenance records.

(3) If maintenance tools are supported by vendor or third-party agreements, the agreements shall include SLAs appropriate for the information system.

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

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

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Ensure that all maintenance tools carried into a facility by maintenance personnel be inspected for obvious improper modifications.

i) If, upon inspection of maintenance tools, Information System Personnel determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident shall be handled in a way that is consistent with EPA's incident handling policies and procedures. Refer to Information Security – Incident Response Procedures.

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

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Ensure that all media containing diagnostic and test programs (e.g., software or firmware used for system maintenance or diagnostics) is checked for malicious code before the media are used in the information system.

i) If, upon inspection of media containing maintenance diagnostic and test programs, Information System Personnel determine that the media contain malicious code, the incident shall be handled consistent with EPA's incident handling policies and procedures. Refer to Information Security – Incident Response Procedures.

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

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Prevent the unauthorized removal of maintenance equipment by:

i) Verifying that there is no EPA information contained on the equipment;

ii) Sanitizing or destroying the equipment;

(1) Refer to Information Security – Media Protection Procedures for requirements on sanitization.

iii) Retaining the equipment securely within the facility; or

iv) Obtaining an exemption from the System Owner explicitly authorizing the removal of the equipment from the facility.

For FedRAMP Moderate and High Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Prevent the unauthorized removal of maintenance equipment by:

i) Verifying that there is no EPA information contained on the equipment;

ii) Sanitizing or destroying the equipment;

(1) Refer to Information Security – Media Protection Procedures for requirements on sanitization.

iii) Retaining the equipment securely within the facility.

iv) Obtaining an exemption from a designated EPA official explicitly authorizing the removal of the equipment from the facility.

MA-3 (4) – Maintenance Tools | Restricted Tool Use

Not selected as part of the control base.

MA-4 – Non-local Maintenance

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Approve and monitor non-local maintenance and diagnostic activities performed on the information system.

Note: Non-local 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. 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.

b) Allow only the use of non-local maintenance and diagnostic tools that are consistent with EPA policy and requirements and documented in the information system's System Security Plan (SSP).

i) Non-locally executed maintenance and diagnostic activities shall not bypass IT security controls or violate EPA policy or requirements.

c) Employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.

i) Authentication techniques shall be consistent with the network access requirements in IA-2 found in Information Security – Identification and Authentication Procedure.

d) Maintain maintenance records for all non-local maintenance, diagnostic and service activities.

i) Refer to MA-2 – Controlled Maintenance section of this procedure document for EPA standards on the components of all maintenance records.

e) Ensure access information such as passwords or port information shall be communicated out of band by secure means (e.g., encrypted communications, phone).

f) Accomplish the following when maintenance is to be conducted externally by a non-EPA third party:

i) Set up the required connection features.

ii) Provide assistance to the non-EPA third-party individual during the non-local connection session and also monitor the process in real time (i.e., as it is happening).

iii) Grant temporary access rights to the non-EPA third-party individual only for the time needed to perform the maintenance.

iv) Verify the completion of the non-local maintenance.

g) Disable disallowed maintenance ports, services and protocols when not in-use for their authorized maintenance purposes.

i) Refer to Information Security – Configuration Management Procedures for requirements on ports, services and protocols.

h) Verify the following once non-local maintenance and diagnostic activities are completed:

i) All sessions and network connections invoked in the performance of the activity shall be terminated.

ii) All temporarily enabled or opened maintenance ports, services, or protocols shall be disabled or closed again.

iii) All temporary access shall be disabled.

MA-4 (1) – Non-Local Maintenance | Auditing and Review

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Audit all non-local maintenance and diagnostic sessions, and review the records of the maintenance and diagnostic sessions for discrepancies.

MA-4 (2) – Non-Local Maintenance | Document Non-local Maintenance

For Moderate and High Information Systems:

1) SO), in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Document policies and procedures for the establishment and use of non-local maintenance and diagnostic connections in the information system's SSP.

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

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Perform non-local maintenance or diagnostic services from an information system that implements security capabilities comparable to the capability implemented on the information system being serviced.

i) If the above condition cannot be met, the component to be serviced shall be removed from the information system and, prior to non-local maintenance and diagnostic services, sanitized (with regard to organizational information) before removal from organizational facilities. It shall also be inspected and sanitized (with regard to potentially malicious software and surreptitious implants) after the service is performed and before reconnecting the component to any of EPA's information systems.

(1) Refer to Information Security – Media Protection Procedures for requirements on sanitization.

MA-4 (4) – Non-Local Maintenance | Authentication / Separation of Maintenance Sessions

Not selected as part of the control base.

MA-4 (5) – Non-Local Maintenance | Approvals and Notifications

Not selected as part of the control base.

MA-4 (6) – Non-Local Maintenance | Cryptographic Protection

Not selected as part of the control base.

MA-4 (7) – Non-Local Maintenance | Remote Disconnect Verification

Not selected as part of the control base.

MA-5 – Maintenance Personnel

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Establish a process for maintenance personnel authorization.

i) Only authorized personnel shall perform maintenance on the information system.

ii) A current list of authorized maintenance organizations or personnel shall be maintained.

b) Ensure that non-escorted personnel performing maintenance on the information system have the required access authorizations.

c) Designate EPA personnel with the required access authorizations and technical competence to supervise information system maintenance activities of personnel who do not possess the required access authorizations.

i) Maintenance personnel who do not possess the required access authorizations shall be escorted at all times while performing information system maintenance.

ii) Before accessing an EPA information system, all third-party maintenance personnel shall have:

(1) Individually signed a non-disclosure form.

(2) Provided valid identification.

(3) Been validated by the Contracting Officer or Contracting Officer Technical Representative (COTR) that the maintenance personnel have been screened by their respective employers to the equivalent level of a National Agency Check with Inquiries (NACI) or to the appropriate level based on the information system's confidentiality requirement.

(a) Refer to Information Security – Personnel Security Procedures for requirements on screening.

iii) Personnel who are to perform routine maintenance shall be both expected (i.e., there shall be a schedule or notification) and pre-approved.

(1) When emergency maintenance is needed, the personnel shall still be pre-approved.

(2) If individuals not previously identified in the information system (e.g., vendor personnel, consultants) legitimately require privileged access to the system because they are required to conduct maintenance or diagnostic activities with little or no notice, EPA may issue temporary credentials; however, issuing those credentials shall be based on a prior assessment of risk.

iv) The Contracting Officer or COTR shall ensure maintenance personnel screening and access requirements are detailed in the Statement of Work (SOW) or contract covering the information system's maintenance.

(1) Refer to Information Security – System and Services Acquisition Procedures for requirements on SOWs and contracts.

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

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, which include the following requirements:

i) 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 EPA personnel who are fully cleared, have appropriate access authorizations and are technically qualified.

ii) 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.

b) Develop and implement alternate security safeguards in the event an information system component cannot be sanitized, removed or disconnected from the system.

For FedRAMP Moderate and High Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, which include the following requirements:

(i) 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 EPA personnel who are fully cleared, have appropriate access authorizations and are technically qualified.

(ii) 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.

b) Develop and implement alternate security safeguards in the event an information system component cannot be sanitized, removed or disconnected from the system.

MA-5 (2) – Maintenance Personnel | Security Clearances for Classified Systems

Not selected as part of the control base.

MA-5 (3) – Maintenance Personnel | Citizenship Requirements for Classified Systems

Not selected as part of the control base.

MA-5 (4) – Maintenance Personnel | Foreign Nationals

Not selected as part of the control base.

MA-5 (5) – Maintenance Personnel | Nonsystem-Related Maintenance

Not selected as part of the control base.

MA-6 – Timely Maintenance

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Ensure timely maintenance provisions (i.e., SLAs or equivalent language) are included in all maintenance agreements for the information system.

i) The provisions shall cover maintenance support and/or spare or replacement parts for both routine maintenance and when there are failures, emergencies or a need for unscheduled maintenance.

ii) The provisions shall be expressed in terms of the timeframe from notification of the failure, emergency or need for unscheduled maintenance.

iii) The provisions shall address the timeframe for dispatching technicians.

iv) The maintenance agreements shall define the security-critical information system components and/or key IT components for which spare parts or replacement parts shall be made available.

Note: Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers and intrusion prevention systems.

(1) The 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 shall be specified.

(2) The provisions shall address both the availability and the delivery of spare or replacement parts.

v) The timely maintenance provisions shall be able to support the required availability timeframe determined by the Business Impact Assessment (BIA) for the information system.

MA-6 (1) – Timely Maintenance | Preventive Maintenance

Not selected as part of the control base.

MA-6 (2) – Timely Maintenance | Predictive Maintenance

Not selected as part of the control base.

MA-6 (3) – Timely Maintenance | Automated Support for Predictive Maintenance

Not selected as part of the control base.

7. ROLES AND RESPONSIBILITIES

Contracting Officers or Contracting Officer Technical Representatives (COTR)

1) Contracting Officers or COTRs have the following responsibilities with respect to maintenance:
   a) Ensure that maintenance personnel have been screened by their respective employers to the equivalent level of a NACI or to the appropriate level based on the information system's confidentiality requirement.
   b) Ensure that maintenance personnel screening and access requirements are detailed in the SOW or contract covering the information system's maintenance.

c) Ensure appropriate contract language and SLAs are part of maintenance contracts, as appropriate.

Information Management Officers (IMO)

1) IMOs have the following responsibilities with respect to maintenance:
   a) Implement policies, procedures, control techniques and processes identified in the EPA Information Security Program.
   b) Ensure all EPA information and information system users within their organizations successfully complete information security awareness training prior to initial access to EPA systems and information and at least annually thereafter to maintain access.
   c) Coordinate with the Senior Agency Information Security Officer (SAISO) and other EPA Information Security representatives in responding to information security data calls, audit requests, and reporting.

Information Owners (IO)

1) IOs have the following responsibilities with respect to maintenance:
   a) Coordinate with the SAISO and other information security representatives in responding to information security data calls, audit requests, and reporting.
   b) Review and approve maintenance requests for systems that process and store information under their purview, as applicable.
   c) Implement policies, procedures and control techniques identified in the EPA Information Security Program.
   d) Assign an ISSO in writing for each non-enterprise service obtained.
   e) Categorize information and provide results to SOs, service managers, common control providers and service providers.
   f) Coordinate with SOs, service managers, common control providers and service providers to ensure supporting systems are properly categorized according to information categorization.
   g) Ensure service providers' systems supporting non-enterprise services are configured, continuously monitored and maintained to protect supported information within acceptable risks adequately.
   h) Develop, maintain and provide information security documents as required under the EPA Information Security Program for non-enterprise services obtained.
   i) Conduct, or ensure service providers conduct, impact analyses for proposed or actual changes to systems or their operational environments for non-enterprise services obtained.
   j) Ensure service providers establish, manage and use configuration change management processes for non-enterprise services obtained.
   k) Approve who has access to a system or service containing information for which the IO is responsible, to include types of privileges and access rights.

Information System Security Officers (ISSO)

1) ISSOs have the following responsibilities with respect to maintenance:
   a) Carry out the following when maintenance is to be conducted non-locally by a non-EPA third party:

i) Set up the required connection features; provide assistance to the third-party individual during the non-local connection session and also monitor the process in real time (i.e., as it is happening); grant temporary access rights to the non-EPA third-party individual; and disable all temporary access and sessions and network connections once the non-local maintenance is completed and verified.

b) Change passwords following each non-local maintenance service, if password-based authentication is used.

c) Verify that security features are still functioning properly after maintenance is completed.

System Owners (SO)

1) SOs have the following responsibilities with respect to maintenance:
   a) Give written approval to use maintenance tools that are not contained in the maintenance plan prior to using that tool.
   b) Make the determination to allow maintenance tools to be used.
   c) Plan, budget, develop and implement maintenance agreements for their information systems.
      i) Ensure adequate controls over maintenance activities.
      ii) Monitor controls over maintenance.
   d) Develop appropriate contract language and SLAs for their information systems consistent with EPA and federal policies, procedures and BIAs.
   e) Ensure adequate controls are addressed and documentation and records are reviewed and kept in accordance with established requirements.
   f) Review acquisition, agreement and SLA documentation for necessary maintenance language and requirements.

Service Managers (SM)

1) SMs have the following responsibilities with respect to maintenance:
   a) Implement policies, procedures and control techniques identified in the EPA Information Security Program.
   b) Assign an ISSO in writing for each enterprise solution obtained.
   c) Coordinate with information owners for deciding who has access to the service (and with what types of privileges or access rights) and ensure service users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).
   d) Follow FedRAMP requirements.
   e) Obtain authorizations to operate or authorizations to test from the appropriate SIO prior to operational use or testing of any service for enterprise services.
   f) Ensure service providers deploy and operate systems according to the security requirements documented in security plans.
   g) Conduct, or ensure service providers conduct, impact analyses for proposed or actual changes to systems or their operational environments for enterprise services.
   h) Ensure service providers establish, manage and use configuration change management processes for enterprise services.
   i) Coordinate with the Director of OITO and service providers for service providers implementing controls to ensure compatibility and

interoperability with enterprise tools and controls for enterprise services.

EPA Personnel (e.g., System Users)

1) EPA Personnel have the following responsibilities with respect to maintenance:
   a) Supervise and escort maintenance personnel at all times while maintenance activities are being performed on the information system, as required.
   b) Question and verify the identity of unfamiliar maintenance personnel.
   c) Contact the EPA Help Desk regarding any observed suspicious activity.

8. RELATED INFORMATION

- NIST Special Publications, 800 series
- Related policy and procedures are available on the Office of Environmental Information's (OEI) Policy Resources website: http://intranet.epa.gov/oei/imitpolicy/policies.htm
- Related standards and guidance are available on OEI's website.

9. DEFINITIONS

- **Availability:** ensuring timely and reliable access to and use of information.
- **Confidentiality:** preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- **Controlled Area:** any area or space for which EPA has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
- **Information System:** discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.
- **Information Technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
- **Integrity:** guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **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.
- **Written (or in writing):** to officially document the action or decision, either manually or electronically, and includes a signature.

Abbreviations including acronyms are summarized in *Appendix: Acronyms & Abbreviations*.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- Substantive business case need(s)
- Demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

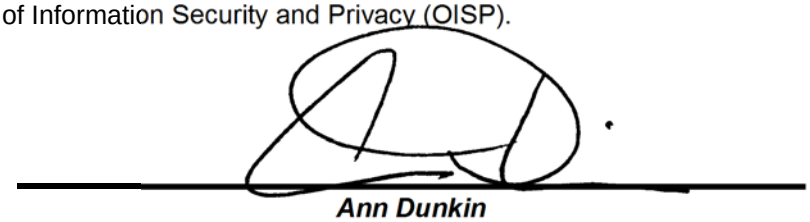
The SAISO and Director of OITO shall coordinate to maintain a central repository of all waivers.

11. MATERIAL SUPERSEDED

- EPA Information Procedures: CIO 2150.3-P-09.1, Information Security – Interim Maintenance Procedures, July 18, 2012.

12. CONTACTS

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



Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

Information Security – Interim Maintenance Procedure		
Directive No.: 2150-P-09.2	CIO Approval: 12/28/2016	Transmittal No.: 17-004e

APPENDIX:
ACRONYMS & ABBREVIATIONS

BIA	Business Impact Assessment
CIO	Chief Information Officer
COTR	Contracting Officer Technical Representative
EPA	Environmental Protection Agency
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
IMO	Information Management Officer
IO	Information Owner
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
NACI	National Agency Check Inquiries
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OISP	Office of Information Security and Privacy
OITO	Office of Information Technology Operations
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POC	Point of Contact
SAISO	Senior Agency Information Security Officer
SLA	Service Level Agreement
SM	Service Manager
SO	System Owner
SOW	Statement of Work
SP	Special Publication
SSP	System Security Plan