EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-09.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

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

INFORMATION SECURITY – INTERIM MAINTENANCE PROCEDURES V1.8 JULY 18, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Maintenance control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

These procedures cover 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 agency.

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that 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 must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the maintenance family of controls found in NIST SP 800-53, Revision 3.

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III*, Federal Information Security*

Management Act (FISMA) as amended

- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 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
- Federal Information Processing Standards (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

6. PROCEDURES

MA-2 – Controlled Maintenance

a. Maintenance and repairs on information system components must be scheduled and performed in accordance with manufacturer or vendor specifications and/or EPA requirements.
    i. The maintenance schedule and procedures must be documented in a Maintenance Plan.
        - The Maintenance Plan must address how the maintenance schedule is managed and the Point of Contact (POC) for scheduled maintenance.
    ii. Scheduled maintenance must include controls to monitor the completion of maintenance in accordance with the information system's documented maintenance schedule and vendor recommendations.
    iii. If a manufacturer, vendor, or developer provided maintenance schedule does not exist, the system must be reviewed every three months in order to determine if maintenance is required.
    iv. Any maintenance action that must be performed outside of the scheduled maintenance timeframes must adhere to the information system's documented procedures for unscheduled maintenance.

b. Maintenance and repair activities, including non-local maintenance and diagnostics, must be documented and the records must be reviewed monthly.

c. Any maintenance of an information system that requires a configuration change must adhere to the requirements in *Information Security – Interim Configuration Management Procedures*.

d. All maintenance activities must be controlled under all circumstances:
    i. Whether performed on site or remotely.
    ii. Whether the equipment is serviced on site or removed to another location.

e. The removal of any information system or system components from organizational facilities for off-site maintenance or repairs must adhere to the following requirements:
    i. Explicit approval from a designated official must be obtained.
    ii. All information from associated media must 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.
        - Refer to *Information Security – Interim Media Protection Procedures* for requirements on proper media handling and sanitization.

f. If scheduled maintenance of an information system is outsourced to a third-party or vendor, the organization responsible for information system maintenance must be named in the System Security Plan (SSP) along with current POC information.
    i. Maintenance contracts with third party providers or vendors must include Service Level Agreements (SLAs) that are sufficient to support the information system's availability requirements and mission criticality.
    ii. NIST SP 800-35 must be used as guidance on information technology security services.
    iii. Refer to *Information Security – Interim Personnel Security Procedures* and *Information Security – System and Services Acquisition Procedures* for requirements on information technology security services.

g. Notification must be provided to all impacted users informing them of scheduled, unscheduled, and emergency maintenance on the information system.
    i. Email notification is preferable for external users.
    ii. Notification via the web for external users must consider the extent of information and detail of information disclosed;
        - For example, naming servers in the notification may provide information for social engineering threats.
    iii. Help desk personnel must be notified and reminded not to provide unauthorized information unless the identity of the user can be confirmed.
    iv. The following must be addressed in the notification.
        - The expected start and finish time of the maintenance.
        - The purpose of the maintenance activity.
        - The specific information systems or subcomponents that may be impacted by the maintenance.

- Any actions required of the impacted users in coordination with the maintenance effort.
- Contact information should a user have any questions or concerns related to the maintenance effort.

h. An updated notification must be sent should the expected start or finish time or any other parameter of the maintenance change.

i. The System Owner (SO) and the party that requested the maintenance, if applicable, must be notified when maintenance is completed.

j. Following maintenance or repair actions, the security features must be checked to verify that they are still functioning properly.

For moderate and high information systems

k. Maintenance records for the information system must include the following:

i. Date and time of maintenance.

ii. Name of individual(s) performing the maintenance.

iii. Name of escort, if applicable.

iv. Description of maintenance performed.

v. List of equipment removed or replaced (including identification numbers, if applicable).

l. Maintenance records of the aforementioned items must be kept on file.

For high information systems

m. Automated mechanisms must be employed 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.

MA-3 – Maintenance Tools

For moderate and high information systems

a. The use of information system maintenance tools must be 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 of the approved maintenance tool must be 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 must be given by the SO.

ii. The SO's written approval must then be included as an attachment to the Maintenance Plan after the fact.

iii. Once the maintenance is completed, one of the following actions is required:

- The tool must be formally documented and added to the list in the Maintenance Plan.
- The tool must be removed from the information system and no longer used.

c. Any maintenance ports, services, and protocols that according to configuration standards must be disabled, but must be used by approved maintenance tools, are only permitted to be enabled during maintenance.

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

d. The approved tools must be maintained on an ongoing basis.

i. A maintenance schedule must include the maintenance of the information system's maintenance tools and the schedule must be documented in the Maintenance Plan.

ii. Maintenance tools must receive vendor recommended maintenance, and the maintenance must be documented with other information system maintenance records.

iii. If maintenance tools are supported by vendor or third party agreements, the agreements must include SLAs appropriate for the information system.

e. All maintenance tools carried into a facility by maintenance personnel must be inspected for obvious improper modifications.

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

f. All media containing diagnostic and test programs (e.g., software or firmware used for system maintenance or diagnostics) must be checked for malicious code before the media are used in the information system.

For high information systems

g. At least one of the following must be used to prevent the unauthorized removal of maintenance equipment:

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

ii. Sanitizing or destroying the equipment

- Refer to *Information Security – Interim 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-4 – Non-Local Maintenance

a. Non-local maintenance and diagnostic activities performed on the information system must be authorized, logged, monitored, and controlled.

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. The use of non-local maintenance and diagnostic tools must be consistent with EPA policy and requirements and documented in the information system's SSP.
    i. Non-locally executed maintenance and diagnostic activities must not bypass information technology security controls or violate EPA policy or requirements.
c. Strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions must be employed.
    i. Identification and authentication techniques must be consistent with the network access requirements of IA-2 found in *Information Security – Interim Identification and Authentication Procedures*.
d. Maintenance records must be maintained 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. Access information such as passwords or port information must be communicated out of band by secure means (e.g., encrypted communications, phone).
f. When maintenance is to be conducted externally by a non-EPA third party, the information system personnel shall accomplish the following:
    i. Set up the required connection features.
    ii. 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).
    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. Any maintenance ports, services, and protocols that according to configuration standards must be disabled, but must be used during non-local maintenance, are only permitted to be enabled during maintenance.
    i. Refer to *Information Security – Interim Configuration Management Procedures* for requirements on ports, services, and protocols.
h. When non-local maintenance and diagnostic activities are completed, the following must be adhered to and verified:
    i. All sessions and network connections invoked in the performance of the

activity must be terminated.

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

iii. All temporary access must be disabled.

For moderate and high information systems

i. Non-local maintenance and diagnostic sessions must be audited and the designated information system personnel shall review the maintenance records of the sessions.

j. Installation and use of non-local maintenance and diagnostic connections must be documented in the information system's SSP.

For high information systems

k. Non-local maintenance or diagnostic services must be performed from an information system that implements the same level of security (or higher) as that implemented on the information system being serviced.

i. If the above condition cannot be met, then the component to be serviced must 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, and it must 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.

- Refer to *Information Security – Interim Media Protection Procedures* for requirements on sanitization.

MA-5 – Maintenance Personnel

a. A process for maintenance personnel authorization must be established.

b. Only authorized personnel shall perform maintenance on the information system.

c. A current list of authorized maintenance organizations or personnel must be maintained.

d. Personnel performing maintenance on the information system must have the required access authorizations.

i. When maintenance personnel do not possess the required access authorizations, EPA personnel with the required access authorizations and technical competence deemed necessary must be designated to supervise information system maintenance.

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

e. Before accessing an EPA information system, all third-party maintenance personnel must have:

i. Individually signed a non-disclosure form.

ii. Provided valid identification.

iii. 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.

- Refer to *Information Security – Interim Personnel Security Procedures* for requirements on screening.

f. Personnel who are to perform routine maintenance must be both expected (i.e., there must be a schedule or notification) and pre-approved.
    i. When emergency maintenance is needed, the personnel must still be pre-approved.
        - 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 must be based on a prior assessment of risk.
g. 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.
    i. Refer to *Information Security – Interim System and Services Acquisition Procedures* for requirements on SOWs and contracts.

MA-6 – Timely Maintenance

For moderate and high information systems

a. Timely maintenance provisions (i.e., SLAs or equivalent language) must be included in all maintenance agreements for the information system.
    i. The timely maintenance provisions must 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 timely maintenance provisions must be expressed in terms of the timeframe from notification of the failure, emergency, or need for unscheduled maintenance.
    iii. The provisions must address the timeframe for dispatching technicians.
    iv. The maintenance agreements must define the security-critical information system components and/or key information technology components for which spare parts or replacement parts must be made available.

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

- 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 must be specified.

- The provisions must address both the availability and the delivery of spare or replacement parts.

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

7. RELATED DOCUMENTS

- NIST SP 800-35, *Guide to Information Technology Security Services*, October 2003
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009
- NIST SP 800-63, Version 1.0.2, *Electronic Authentication Guideline*, April 2006
- NIST SP 800-88, *Guidelines for Media Sanitization*, September 2006

8. ROLES AND RESPONSIBILITIES

Contracting Officer or Contracting Officer Technical Representative (COTR)

a. The Contracting Officer or COTR has the following responsibilities with respect to maintenance:

i. 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.

ii. Ensure that maintenance personnel screening and access requirements are detailed in the SOW or contract covering the information system's maintenance.

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

Information System Personnel

a. Information system personnel have the following responsibilities with respect to maintenance:

i. When maintenance is to be conducted non-locally by a non-EPA third party:

- 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.

ii. Change the password following each non-local maintenance service, if password-based authentication is used.

iii. After maintenance is completed, verify that security features are still functioning properly.

System Owner (SO)

a. The SO have the following responsibilities with respect to maintenance:
   i. Give written approval to use a maintenance tool that is not contained in the maintenance plan prior to using that tool.
   ii. Make the determination to allow the maintenance tool to be used.
   iii. Plan, budget, develop, and implement maintenance agreements for their information systems.
      - Ensure adequate controls over maintenance activities.
      - Monitor controls over maintenance.
   iv. Develop appropriate contract language and SLAs for their information systems consistent with EPA and federal policies, procedures, and BIAs.

Information System Security Officer (ISSO)

a. The ISSO has the following responsibilities with respect to maintenance:
   i. Ensure adequate controls are addressed and documentation and records are reviewed and kept in accordance with established requirements.
   ii. Review acquisition, agreement, and SLA documentation for necessary maintenance language and requirements.

EPA Personnel

a. EPA personnel have the following responsibilities with respect to maintenance:
   i. Supervise and escort maintenance personnel at all times while maintenance activities are being performed on the information system.
   ii. Question and verify the identity of unfamiliar maintenance personnel.
   iii. Contact the help desk security regarding any suspicious activity.

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.
- Non-local Maintenance - 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.
- 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" means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.

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, OTOP shall coordinate to maintain central repository of all waivers.

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy and procedures are available on OEI's Policy Resources website.

http://intranet.epa.gov/oei/imitpolicy/policies.htm

Related standards and guidelines are available on OEI's website.

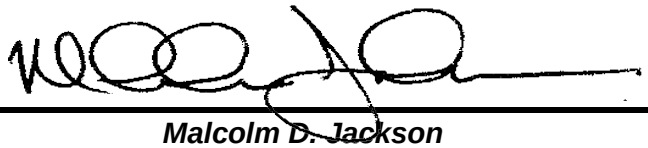
12. MATERIAL SUPERSEDED

EPA Classification No.:	CIO-2150.3-P-09.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

NA

13. ADDITIONAL INFORMATION

NA



Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

BIA	Business Impact Assessment
CIO	Chief Information Officer
COTR	Contracting Officer Technical Representative
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ISSO	Information System Security Officer
NACI	National Agency Check Inquiries
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POC	Point of Contact
SLA	Service Level Agreement
SO	System Owner
SOW	Statement of Work
SP	Special Publication
SSP	System Security Plan

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.7	2/6/2008	Initial draft	Heather Flager	Procedures-MA-Draft_TO62_020_1
1.0	6/24/2009	Incorporated EPA comments	Heather Flager	Procedures-MA-Final_TO62_020_2
1.5	6/29/2010	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_MA_Draft.TO-062_050_1.0
1.6	7/14/2010	TISS Final Draft Review	Charleen Johnson	Procedures_MA_Draft.TO-062_050_1.0
1.7	5/1/2012	SAISO Final Review	David Stepp	Procedures_MA_Draft.TO-062_250_1.0
1.8	7/18/2012	Document Review	LaToya Gordon	Procedures_MA_Draft.TO-062_250_1.0