PREFACE TO SELECTED INFORMATION DIRECTIVES

CIO Transmittal No.: 15-010	CIO Approval Date: 06/12/2015

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

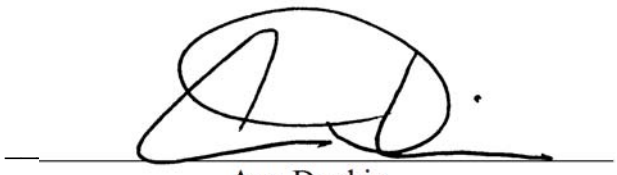
CHIEF INFORMATION OFFICER MEMORANDUM

SUBJECT: Chief Technology Officer (CTO) Responsibilities in Selected Information Directives

Re-assigned CTO responsibilities

Effective immediately, CTO responsibilities detailed in the selected information directives (i.e., Information Policies, Procedures, Standards, and Guidance) listed in Appendix A are re-assigned to the OEI Office of Technology, Operations, and Planning (OTOP) Director and the Senior Agency Information Security Officer (SAISO) as detailed. The re-assignment does not change any requirements in the selected information directives.

The OEI Information Directives Program Manager is directed to attach this memorandum and Appendix A as a Preface to each of the Information Directives listed. OEI will then update the Roles and Responsibilities section of each Information Directive in accordance with the normal review and update cycle.



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

APPENDIX A

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2104.1 Software Management and Piracy Policy	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy and manage enterprise software licenses.	OTOP Director
CIO 2104-P-01.0 Software Management and Piracy Procedure	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy, manage enterprise software licenses, and provide covered users within their office with training and awareness on the Software Management and Piracy Policy through the annual Cybersecurity Awareness Training.	OTOP Director
CIO 2121.1 System Life Cycle Management (SLCM) Policy	Establish and publish procedures, technical operational procedures and standards (TOPS), and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2121-P-03.0 SLCM Procedure	Establish and publish procedures, TOPS, and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2122.1 Enterprise Architecture (EA) Policy	Issue procedures, guidance, and technical standards associated with the EA with a specific focus on the technology architecture, chair the Quality Technology Subcommittee (QTS), and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-01.1 EA Governance Procedures	Issue procedures, guidance, and technical standards associated with the EA, with a specific focus on the technology architecture, chair the QTS, and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-03.0 Information Technology Infrastructure Standard Procedure	Recommend to the CIO a specific IT standard, product or specification to be added to the official Agency IT Standards Profile with consultation from the Quality Information Council (QIC) and the QTS, and develop and maintain the Agency's Technology Architecture.	OTOP Director
2122-S-02.0 Personal Computer Configuration and Management Standard	Review and approve requests for waivers in regard to this standard.	OTOP Director
CIO 2123.1 Configuration Management Policy	Provide procedures, standards, and guidance to senior level managers in support of the Agency's Configuration Management Policy; institute change management processes; and provide a change management database.	OTOP Director

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2150-P-01.1 Information Security - Interim Access Control Procedures	Approve all methods of dial-up access, approve all wireless connections, establish, document, authorize, and monitor all methods of remote access to an information system; delegate to Regions and other entities, as appropriate; and address co-management responsibilities for the Agency Security Architecture.	OTOP Director
CIO 2150-P-08.1 Information Security - Interim Incident Response Procedures	Determine Operational Status Categories during Alerts and Risks (OSCAR) 5 level (page 7).	SAISO
	Be available when the Computer Security Incident Response Capability (CSIRC) must report and coordinate incidents (page 16). Be available to meet with the Director of Cyber Security Staff (CSS) when senior managers are informed of incidents, occurrences and their status (page 18).	OTOP Director
CIO 2150-P-14.1 Information Security - Interim Risk Assessment Procedures	Approve the use of and, as appropriate, acquire and deploy enterprise vulnerability management technology. Consult with the SAISO to determine the coverage and compliance of enterprise vulnerability management technology with respect to federal and Agency requirements, including use of these tools to meet assessment requirements of other control families in NIST 800-53A, Revision 1, and to ensure the most cost effective, complete and accurate results.	OTOP Director
CIO 2150-P-15.1 Information Security - Interim System Services Acquisition Procedures	For the procurement of external information system services where a sufficient level of trust cannot be established, be available to confer regarding risks associated with the network and the Agency.	OTOP Director
CIO 2150-P-16.1 Information Security - Interim System and Communications Protection Procedures	Approve use of mobile VoIP-enabled units.	OTOP Director
CIO 2150.4 Mobile Computing Policy	Oversee policy and procedure implementation regarding use of mobile computing technologies. Approve mobile computing technology and device deployment.	OTOP Director
CIO 2150-P-01.1 Mobile Computing Management Procedures	Oversee policy and the implementation of the procedures. Approve enterprise mobile device types to be deployed. Review and approve requests for waivers in regards to the procedures.	OTOP Director

EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-16.1	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 SYSTEM AND COMMUNICATIONS PROTECTION PROCEDURES
V3.1
JULY 16, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the System and Communications Protection 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 EPA's operations and assets.

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 system and communication protection family of controls found in NIST SP 800-53, Revision 3.

EPA Classification No.:	CIO-2150.3-P-16.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

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)
- Rehabilitation Act of 1973, Section 508 (as amended) (29 USC § 794 (d))
- Office of Management and Budget (OMB) Memorandum M-00-13, "*Privacy Policies and Data Collection on Federal Web Sites*," June 2000
- OMB Memorandum M-05-24, "*Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*," August 2005
- OMB Memorandum M-06-16, "*Protection of Sensitive Agency Information*," June 2006
- OMB Memorandum M-08-05, "*Implementation of Trusted Internet Connections (TIC*,*)*" November 2007
- OMB Memorandum M-08-16, "*Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*," April 2008
- OMB Memorandum M-08-23, "*Securing the Federal Government's Domain Name System Infrastructure*," August 2008
- OMB Memorandum M-08-27, "*Guidance for Trusted Internet Connection (TIC) Compliance*," September 2008
- OMB Memorandum M-09-32, "*Update on the Trusted Internet Connections Initiative*," September 2009
- OMB Circular A-130, "*Management of Federal Information Resources*," Appendix III, "*Security of Federal Automated Information Resources*", November 2000
- Federal Information Processing Standards (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

6. PROCEDURES

SC-2 – Application Partitioning

For moderate and high information systems

a. The information system must be designed and configured to separate user functionality (including user interface services) from information system management functionality (e.g., functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access).

Note: An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

b. The information system must be designed and configured to either physically or logically separate user functionality from information system management functionality.
    i. Separation must be accomplished by using one of the following methods or a combination of methods, as applicable:
        - Different computers
        - Different partitions
        - Different central processing units
        - Different instances of the operating system
        - Different network addresses
        - Other methods as appropriate

c. The following must be complied with for designing, implementing, and managing web-based applications:
    i. Web content must be installed on a dedicated physical disk or logical partition that is separate from the storage locations for the operating system and web server application.
    ii. A complete web content access matrix must be defined that identifies which folders and files within the web server's document directories should be restricted and which should be accessible and by whom.
    iii. Access to a specific web content file directory tree must be restricted by:
        - Establishing related subdirectories exclusively for web server content files, including graphics but excluding scripts and other programs.
        - Defining a single directory tree exclusively for all external scripts or programs executed as part of web content such as Common Gateway Interface (CGI), Active Server Pages (ASP), or PHP: Hypertext Preprocessor (PHP).
        - Disabling the execution of scripts that are not exclusively under the control of administrative accounts by creating and controlling access

to a separate directory intended to contain authorized scripts.

- Disabling the use of hard or symbolic links.

iv. The functionality of one process or service given to one application must not enable the same functionality for another application (e.g., access to a back-end database).

v. A limit on hard drive space must be placed on resources dedicated for uploads from users to servers.

- Uploads must be placed on a separate partition to provide stronger assurance that the hard drive space limit cannot be exceeded.

vi. Log files must be stored in a location that is sized appropriately and must be stored on a separate partition or computer.

- Refer to *Information Security – Interim Audit and Accountability Procedures* for further information on audit log storage.

vii. On servers that use certificates, the original certificate must be stored in a folder or partition that is:

- Accessible by only authorized web or system administrators
- Secured by appropriate authentication mechanisms

viii. On servers that use certificates, a file integrity checker must be run on the server to monitor for any changes to the certificate.

d. The information system must be configured to prevent users from performing any functions that are not explicitly authorized for their roles.

i. Refer to *Information Security – Interim Access Control Procedures* for requirements on authorization and access enforcement.

SC-3 – Security Function Isolation

For high information systems

a. The information system must be configured to isolate security functions from non-security functions by means of isolation boundaries (implemented via partitions and domains) that control access to and protect the integrity of the hardware, software, and firmware that perform those security functions.

b. The information system must be configured to maintain a separate execution domain (e.g., address space) for each executing process.

SC-4 – Information in Shared Resources

Note: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

For moderate and high information systems

a. The information system must be configured to prevent unauthorized and unintended information transfer via shared system resources.

Note: The control of information in shared resources is also referred to as object reuse.

b. When configuring a host operating system, the following must be complied with:
    i. Temporary files created by the server application must be restricted to a specified and appropriately protected subdirectory, when possible.
    ii. Access to any temporary files created by the server application must be limited to the service processes that created the files, when possible.

c. Any previous information content of the information system must be made unavailable upon the allocation of the resource to all subjects, and this must be carried out through the implementation of safeguards, including but not limited to the following:
    i. Temporary pages must not be indexed.

d. The information system object reuse features must be configured to delete information when no longer needed.
    i. Cookies placed onto users' systems must not contain sensitive or Personally Identifiable Information (PII).
    ii. The information system must overwrite sensitive data in memory after the use of the data.
        - Sensitive information includes passwords, secret keys, session keys, private keys, or any other highly sensitive data such as PII or medical records.
    iii. At the end of a session, the information system must delete all temporary files created during the session.
    iv. Before shutdown, the application must delete or erase all temporary files, cache, data, and other objects it created during its execution.
    v. On a weekly basis, the information system must search and delete Word, Outlook, and Internet Explorer temporary files.

e. The information system must not generate core dumps when the information system fails.

f. Information on backup and storage media (e.g., memory, disk drives, removable media including tapes, flash drives, optical disks) must be protected as follows:
    i. The media must be cleared and purged before reuse or before using for other purposes by using Agency-approved and validated overwriting technologies/methods/tools.
    ii. The media must be destroyed by using Agency-approved and validated technologies/methods/tools.
    iii. NIST SP 800-66 Revision 1, NIST SP 800-88, OMB M-06-16, and *Information Security – Interim Media Protection Procedures* must be used as a procedure.

g. Printers and copiers must be configured to not recall data from memory or disks

after printing processes.

Note: This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

SC-5 – Denial of Service Protection

a. The information systems, firewalls, and routers must be configured to protect against or limit the effects of the following types of Denial of Service (DoS) attacks, as applicable:
    i. Internet Control Message Protocol (ICMP) flood:
        - Smurf attack
        - Ping of death
        - Ping flood
    ii. Teardrop attack
    iii. Peer-to-peer attacks
    iv. Permanent DoS attack (i.e., phlashing)
    v. Application level floods:
        - Internet Relay Chat (IRC) floods
        - Banana attack
        - Buffer overflow
    vi. Nuke
    vii. Distributed DoS attack
    viii. Reflected attack
    ix. Unintentional attack
    x. DoS Level II
b. The following methods to guard against, limit, reduce the susceptibility to, and/or detect DoS attacks must be considered and used as appropriate:
    i. Properly configuring the information system according to agency standards
        - Refer to *Information Security – Interim Configuration Management Procedures* for requirements on configuration standards.
    ii. Configuring switches and routers to disable forwarding packets to broadcast addresses
    iii. Configuring the routers to filter traffic
    iv. Employing and properly configuring Intrusion Detection and Prevention Systems (IDPS)

v. Using appropriate tools to detect changes in configuration information or other files

vi. Installing patches

vii. Monitoring the application level of the information system

viii. Reviewing server capacity

ix. Monitoring for suspicious amount of data transferred to or from servers within a prescribed period of time

x. Reviewing appropriate bandwidth

xi. Implementing a separate route or circuit for service redundancy

c. EPA shall work with its telecommunications service providers to implement techniques such as traffic rate limiting, which limits the amount of nonessential traffic (e.g., ICMP traffic) crossing the EPA edge area.

SC-7 – Boundary Protection

a. The information system must be configured to monitor and control communications:

   i. At the external boundary of the system

   ii. At key internal boundaries within the system

b. The information system must connect only to external networks or information systems, through managed interfaces approved by the Office of Technology Operations and Planning (OTOP).

   i. These managed interfaces must consist of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in accordance with an effective, security architecture.

      - For example, the architecture may consist of firewalls protecting routers and application gateways residing on a protected sub-network commonly referred to as a demilitarized zone or DMZ.

   ii. Connections must be consistent with EPA's enterprise technology and security architecture.

   iii. Connections must be consistent with federal regulations.

      - Refer to OMB M-08-27 for guidance on TIC.

Note: Prohibiting external traffic that appears to be spoofing an internal address as the source is an example of restricting and prohibiting communications.

c. EPA shall consider the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services.

   i. When commercial telecommunications services are employed, either one or both of the following must be complied with:

- Appropriate compensating security controls must be implemented.
- The additional risk must be explicitly accepted.

Note: Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions.

d. Boundary/edge devices (e.g., firewalls, routers) must be configured to protect and control access to Agency information resources.
    i. Incoming network traffic must be inspected and requests that do not comply with applicable policy must be denied.
    ii. External web traffic must be restricted only to organizational web servers within managed interfaces.
    iii. Traffic from outside a designated boundary that claims to be from within the designated boundary must be blocked.
        - This applies to any traffic from the external network that has a source address that should reside on the internal network.
    iv. Web requests that are not from an authorized internal web proxy must not be passed to the Internet.
e. Tight constraints must be maintained on trust levels within EPA networks.
    i. Information systems outside of the agency firewall must never be absolutely trusted by systems inside the firewall.
f. Information systems must detect and block unauthorized scanning activity that originates outside of its network, within its network, and between information systems.
g. The following must be complied with when securing network device management technologies/tools:
    i. There must be sufficient capacity to collect, store, and view system logging information from all critical Agency infrastructure devices.
        - Refer to *Information Security – Interim Audit and Accountability Procedures* for requirements regarding logging.
    ii. Data and alerts from specialized applications (e.g., IDPS) must be logged to separate management hosts that are better equipped to handle time-critical alarms.
    iii. To ensure that log messages are time-synchronized to each other, clocks on hosts and network devices must be synchronized using Network Time Protocol (NTP) or other approved services.
        - Times must be based on an authoritative external source such as NIST http://tf.nist.gov/timefreq/service/time-computer.html or the

Naval Observatory http://tycho.usno.navy.mil/ntp.html.

- Refer to *Information Security – Interim Audit and Accountability Procedures* for requirements regarding time stamps.

iv. Management channels that need to be active at all times, such as Simple Network Management Protocol (SNMP), must be used with utmost caution due to the inherent vulnerabilities.

- Where SNMP is in use, access to devices must be read-only.

h. The following must be complied with when securing routers:

i. Router configurations and associated documentation must be treated as confidentially sensitive information and must be available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel).

ii. All forms of router access, including SNMP and Hypertext Transfer Protocol (HTTP), must be restricted in accordance with the manufacturer's recommendation.

iii. All passwords must be encrypted.

iv. Secure Shell (SSH) must be used to access a router interface in order to defeat packet sniffers.

- Telnet is prohibited from use.

v. All routers must employ system use notification messages and be in compliance with procedures and standards found in *Information Security – Interim Access Control Procedures.*

vi. Suitable forms of logging must be employed and must be in compliance with *Information Security – Interim Audit and Accountability Procedures*.

- Examples of logging are system logging; Authentication, Authorization, and Accounting (AAA); and SNMP trap logging.

vii. Internet Protocol (IP) routing must be secured with anti-spoofing, route advertisement authentication, and related measures.

viii. Unnecessary services such as finger, Cisco Discovery Protocol (CDP), File Transfer Protocol (FTP), and Trivial File Transfer Protocol (TFTP) must be disabled.

ix. Router software (i.e., operating system) must be kept up-to-date and patches must be applied in compliance with procedures and standards found in *Information Security – Interim System and Information Integrity Procedures*.

i. The following must be complied with when securing network switches:

i. Procedures for carrying out change control and configuration analysis must be in place for switches.

- Refer to *Information Security – Interim Configuration Management Procedures* for requirements on change control.

ii. Unused switch ports must be disabled to prevent hackers from connecting to unused ports and communicating with the rest of the network.

iii. For ports that require trunking, a dedicated Virtual Local Area Network (VLAN) identifier must be used.

iv. Switches must be configured in high-security mode to defeat Address Resolution Protocol (ARP) spoofing and ARP poisoning attacks.

v. Switches must be configured to send all traffic to network-based IDPS on the public web server network segment or to other network segments guarded by an IDPS.

j. The following must be complied with when securing networked hosts:

i. Unused or unneeded services and applications on hosts must be disabled.

ii. All remote access to hosts must occur over secure channels.

- Secure channels include encrypted network connections using SSH or Internet Protocol Security (IPsec).

iii. Network connections must be configured to prevent removal or relocation of a host except by authorized personnel and in conformance with configuration management and change control processes.

- Refer to *Information Security – Interim Configuration Management Procedures* for requirements on change control.

iv. All networked hosts must be scanned for viruses.

- Refer to *Information Security – Interim System and Information Integrity Procedures* for requirements on malicious code protection.

v. At a minimum, IDPS technology must be deployed for hosts that use end-to-end encrypted communications.

k. The following must be complied with when securing IDPS:

i. Network Intrusion Detection System (NIDS) and/or Host Intrusion Detection System (HIDS) must be used as appropriate for the protection of agency assets.

ii. The IDPS engines must be tuned and maintained by security personnel to maximize effectiveness of detection and minimize the occurrence of false positives and false negatives.

iii. IDPS databases must be continuously updated with the latest attack signature information.

iv. Outsourced solutions must be carefully evaluated to ensure that agency security and performance requirements are met.

- Refer to *Information Security – Interim System and Services Acquisition Procedures* for requirements on outsourced services.

l. The following must be complied with regarding firewall management:

i. Firewall configurations and associated documentation must be treated as confidentially sensitive information and must be available to only authorized personnel (e.g., authorized administrators, auditors, security oversight personnel).

ii. An effective set of procedures must be in place to distribute firewall update bulletins and security patches.

- Refer to *Information Security – Interim System and Information Integrity Procedures* for requirements on flaw remediation and security alerts and advisories.

iii. Firewall patches must be installed as soon as possible after the respective vendors release them and the patches are tested.

- Refer to *Information Security – Interim System and Information Integrity Procedures* for requirements on flaw remediation.

iv. Unneeded services (e.g., telnet) must be disabled on the firewall.

v. The firewall must have at least two network interfaces (i.e., dual-homed), one for the private network it is intended to protect and one for the external network to which it is exposed.

vi. The following testing must be performed annually on firewalls and management consoles:

- Penetration testing against the firewall
- Verification that the firewall is properly configured and patched and validation that the firewall is operating as intended
  - This is sometimes referred to as Independent Verification and Validation (IV&V).

m. NIST SP 800-41, Revision 1 must be used as guidance on firewalls and firewall policy.

n. NIST SP 800-54 must be used as guidance on routers.

o. NIST SP 800-77 must be used as guidance on Virtual Private Networks (VPNs).

p. NIST SP 800-94 must be used as guidance on IDPS.

For moderate and high information systems

q. Publicly accessible information system components (e.g., public web servers) must be physically allocated to separate sub-networks with separate, physical network interfaces.

r. Public access into the organization's internal networks must be prevented by the information system except as appropriately mediated by managed interfaces employing boundary protection devices.

s. The number of access points to the information system must be limited to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

Note: The TIC initiative is an example of limiting the number of managed network access points.

t. A managed interface must be implemented for each external telecommunication service.
    i. Security controls must be employed as needed to protect the confidentiality and integrity of the information being transmitted.

u. A traffic flow policy must be established for each managed interface.
    i. Each exception to the traffic flow policy must be documented with a supporting mission/business need and the duration of that need.
    ii. Exceptions to the traffic flow policy must be reviewed quarterly.
    iii. Traffic flow policy exceptions that are no longer supported by an explicit mission/business need must be removed.

v. The information system must be configured at managed interfaces to deny network traffic by default and allow network traffic by exception (i.e., deny all, permit by exception).

w. The information system must be configured to prevent remote devices (e.g., notebooks/laptop computers) that have established a non-remote (e.g., VPN) connection with the system from communicating outside of that communications path with resources in external networks.
    i. Remote devices must be configured via settings that are not configurable by the user of that device to prevent “split tunneling”.

Note: Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communication paths such as split tunneling would be, in effect, allowing unauthorized external connections into the system.

For high information systems

x. The unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary must be prevented when there is an operational failure of the boundary protection mechanisms.

y. The information system must be configured to route approved and defined internal communications traffic to approved and defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.
    i. Proxy servers must support logging of individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and IP addresses.

ii. Proxy servers must be configurable with organization-defined lists of authorized and unauthorized websites.

SC-8 – Transmission Integrity

Note: This control applies to communications across internal and external networks.

For moderate and high integrity information systems

a. The information system must be configured to protect the integrity of transmitted information.

b. If commodity commercial transmission services rather than a fully dedicated transmission service are used and it is infeasible or impractical to obtain from the service provider the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles (see *Information Security – Interim System and Services Acquisition Procedures*), then one or both of the following must be complied with:

   i. Appropriate compensating security controls must be implemented.

   ii. The additional risk must be explicitly accepted.

c. The following types of transmission require enhanced protection (e.g., cryptography mechanisms) when integrity is an important consideration:

   i. Internal traffic within the information system and applications

   ii. Internal traffic between two or more EPA information systems

   iii. External traffic to or across the Internet

   iv. Remote access

   v. Email

   vi. FTP transmissions

   vii. Web services

   viii. Voice over Internet Protocol (VoIP)

   ix. Audio and video

   x. Wireless client to host communications

d. All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol that includes:

   i. Secure Sockets Layer (SSL) version 3.0

   ii. Transport Layer Security (TLS)

e. Instant messaging technologies, where allowed, must not be used to transmit any type of confidentially sensitive non-public data.

f. NIST SP 800-52 must be used as guidance on protecting transmission integrity

using TLS.

g. NIST SP 800-77 must be used as guidance on protecting transmission integrity using IPsec.

h. NIST SP 800-81 must be used as guidance on Domain Name System (DNS) message authentication and integrity verification.

i. NIST SP 800-113 must be used as guidance on SSL VPNs.

j. Cryptographic mechanisms must be employed to ensure changes to information during transmission are recognized, unless the transmission is protected by alternative physical measures (e.g., protective distribution systems).

Note: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003 contain guidance on the use of protective distribution systems, which are physical measures to protect transmitted information.

SC-9 – Transmission Confidentiality

Note: This control applies to communications across internal and external networks.

For moderate and high confidentiality information systems

a. The information system must be configured to protect the confidentiality of transmitted information.

b. Information of a non-public, confidentially sensitive nature (e.g., sensitive PII, trade secret information, confidentially sensitive business information, etc.) must be adequately protected from unauthorized disclosure at rest and in transit and must not be transmitted unprotected (e.g., not visible as clear text) over unsecured networks (e.g., the Internet).

c. If commodity commercial transmission services rather than a fully dedicated transmission service are used and it is infeasible or impractical to obtain from the service provider the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles (see *Information Security – Interim System and Services Acquisition Procedures*), then one or both of the following must be complied with:

    i. Appropriate compensating security controls must be implemented.

    ii. The additional risk must be explicitly accepted.

d. The following types of transmission require enhanced protection (e.g., cryptographic mechanisms) when confidentiality is an important consideration:

    i. Internal traffic within the information system and applications

    ii. Internal traffic between two or more EPA information systems

    iii. External traffic to or across the Internet

    iv. Remote access

    v. Email

vi. FTP transmissions

vii. Web services

viii. VoIP

ix. Audio and video

x. Wireless client to host communications

e. Confidentially sensitive data must be encrypted before being transmitted over any non-protected communication method.

f. All communications that transfer confidentially sensitive data between web clients and web servers must employ the most current secure transport protocol which includes:

i. SSL version 3.0 or higher where required for communication with the public

ii. TLS

g. Instant messaging must not be used to transmit any type of confidentially sensitive data.

h. Email must not be used to transmit confidentially sensitive, non-public data, unless the information is encrypted.

i. NIST SP 800-52 must be used as guidance on protecting transmission confidentiality using TLS.

j. NIST SP 800-77 must be used as guidance on protecting transmission confidentiality using IPsec.

k. NIST SP 800-113 must be used as guidance on SSL VPNs.

l. Cryptographic mechanisms must be employed to prevent unauthorized disclosure of information during transmission, unless the transmission is protected by alternative physical measures.

Note: NSTISSI 7003 contains guidance on the use of protective distribution systems, which are physical measures to protect transmitted information.

SC-10 – Network Disconnect

Note: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

For moderate and high information systems

a. The information system or communicating component must terminate the network connection associated with a communications session at the end of the session.

b. The information system must be configured to disconnect inactive remote VPN

sessions according to the following criteria:

i. After 30 minutes of inactivity if PII is accessible through the connection

ii. After 60 minutes of inactivity if PII is not accessible through the connection

c. The information system must be configured to disconnect inactive local connections after six (6) hours of inactivity.

d. The information system's network disconnect capability must be configured to warn the user that a disconnection is about to occur following a period of inactivity.

e. After the network connection has been terminated, the information system must require re-authentication before allowing access to the system again.

SC-12 – Cryptographic Key Establishment and Management

a. Cryptographic keys must be established and managed by using manual procedures or automated mechanisms with supporting manual procedures, when cryptographic protection is required and the information system is not covered by an enterprise solution.

Note: In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

b. If cryptographic protection is required, the information system must use one of the following approved forms of encryption:

i. Products and modules that have been validated by NIST as compliant with FIPS 140-2 and are listed on the current validated products list at http://csrc.nist.gov/groups/STM/cmvp/validation.html.

Note: Products that have been tested and validated by a Cryptographic Module Testing (CMT) laboratory are members of the National Voluntary Laboratory Accreditation Program (NVLAP).

ii. Products and modules that have been validated or certified for protecting National Security Information by the National Security Agency or the Defense Information Systems Agency.

iii. Encryption technology developed by contractors or as freeware, provided that:

- Commercial products are unavailable, incompatible, or their use is not cost effective.
- A full life cycle cost benefit analysis has been conducted which demonstrates cost efficiencies over use of a commercial product and considers the cost of maintaining NIST validations.
- The encryption technology complies with NIST validation requirements and will support encryption validation requirements throughout the product's usage life cycle.

c. When selecting a NIST-validated product, the module validation lists from http://csrc.nist.gov/groups/STM/cmvp/validation.html must be reviewed to locate the selected and validated cryptographic module.

   i. The vendor of the specified product needs to provide the validation certificate number, and that the number is used to locate and review the module.

   ii. If the selected module is not on the list or its certificate has been revoked, it is prohibited from use and must not be used to demonstrate compliance with FIPS 140-2.

   iii. NIST's website may be used to assist to select another module, as the site displays which modules have validation certificates and are available from the vendor for procurement.

d. The selected cryptographic module must be installed and configured in accordance with the security policy from the NIST validation website in order to be considered FIPS 140-2 compliant.

e. NIST SP 800-56A and NIST SP 800-56B must be referenced as procedures, on establishing cryptographic keys.

f. NIST SP 800-57 must be referenced as guidance on managing cryptographic keys.

For high information systems

g. Availability of information must be maintained in the event of the loss of cryptographic keys by users

SC-13 – Use of Cryptography

a. The information system must implement required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

   i. The federal standard that must be met for employing cryptography in information systems is FIPS 140-2 (as amended).

   ii. Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked.

   iii. Revocations of certificates and other actions as well as additional information on the use of validated cryptography can be found on NIST's website at http://csrc.nist.gov/groups/STM/cmvp/notices.html.

   iv. NIST's validation website must be checked at least annually or when planning upgrades to ensure that product validations have not been revoked and usage is still valid.

   v. Transition plans or requirements for cryptography must be factored into information system budgets and planning.

      - Refer to *Information Security – Interim System and Services*

Acquisition Procedures for requirements on life cycle support and allocation of resources.

b. All data on mobile computers/devices shall be encrypted unless the data is determined to be non-sensitive, in writing, by the EPA Deputy Administrator or an individual he/she may designate in writing;
    i. Refer to *Information Security – Interim Access Control Procedures* for guidance on mobile devices.
    ii. Refer to *Information Security – Interim Media Protection Procedures* for guidance on transporting PII.
c. All sensitive data that is transported or transmitted outside of Agency premises (e.g., backup tapes, disaster recovery/continuity of operations backups, archives, electronic transmissions) must be encrypted in accordance with FIPS 140-2.
    i. Refer to *Information Security – Interim Media Protection Procedures* for guidance on transported and transmitted sensitive PII.
d. NIST SP 800-56A and NIST SP 800-56B must be referenced as guidance on establishing cryptographic keys.
e. NIST SP 800-57 must be referenced as guidance on managing cryptographic keys.

SC-14 – Public Access Protections

Note: The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

a. The information system must protect the integrity and availability of publicly available information and applications.
b. The information system architecture must be designed so that publicly available servers are hosted in a DMZ.
c. The information system must be configured to enforce the following:
    i. Prevent unauthorized users from changing or deleting any established reference links, or associations, or other relationships between data elements.
    ii. Restrict system-related data against modification by public users, unless that data is intended to be altered by the public.
    iii. Prevent the modification of any data elements that are designated as read-only.
        - The information system must also issue a warning reminder to the user that they are not authorized to move, change, or delete read-only data.
    iv. Protect the browser or other client application session cookies from tampering.

v. Protect user identity information stored on the browser or client platform from disclosure and tampering.

vi. Prevent users from accessing the file system directory indicated by a path name.

d. Routine system updates must be performed on all publicly accessible system components to maintain appropriate and security-required patch levels.

i. Refer to *Information Security – Interim System and Information Integrity Procedures* for requirements regarding flaw remediation.

e. Scripts must be secured, reviewed, and tested against exploits that might allow direct access to the underlying operating system or other compromises of the application.

f. Where the application promotes or permits public access, authorization must be obtained to ensure that only the appropriate types of information are made available to the public.

i. The necessary authorization must be obtained from the Information Owner (IO) and System Owner (SO) of the general support system that will be providing access to the public.

g. Web server security checklists in Appendix E of NIST SP 800-44, Version 2 must be used for the following:

i. Planning and managing the web server

ii. Implementing a secure network infrastructure

iii. Securing the web server operating system and testing that security

iv. Securing the web server software, using proper configuration

v. Managing and securing web content

vi. Configuring authentication and encryption technologies and protecting against attacks

vii. Administering the web server, including testing security and recovering from incidents

h. The Configuration Management Plan and other configuration documentation for the web server must incorporate the information from the NIST web server security checklists.

i. Items on the checklists that are not used must be documented and justified in the Configuration Management Plan.

ii. Refer to *Information Security – Interim Configuration Management Procedures* for requirements on developing a Configuration Management Plan.

i. NIST SP 800-95 must be used as guidance on securing web services.

SC-15 – Collaborative Computing Devices

a. Remote activation of collaborative computing devices (e.g., networked white boards, cameras, microphones) is prohibited.

b. The information system must provide an explicit indication to the users physically present at the devices that collaborative computing devices are in use.

    i. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

SC-17 – Public Key Infrastructure Certificates

Note: This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations (e.g., application-specific time services).

For moderate and high information systems

a. Public key certificates (e.g., those certificates requiring visibility external to EPA) must be issued in accordance with EPA Order 3200 or a certification authority cross-certified with the Federal Bridge Certification Authority.

b. For user certificates, EPA shall use certificates from an approved, shared service provider, as required by OMB M-05-24.

c. Certificates for internal system operations (e.g., application-specific time services, desktops, internal servers) must use EPA Active Directory certificates or others approved by OTOP.

    i. These certificates must be implemented under a documented and approved certificate policy and certification practice statement prior to issuance.

    ii. EPA shall provide oversight in the creation of Public Key Infrastructure (PKI) framework and services that provide the generation, production, distribution, control, revocation, recovery, and tracking of PKI certificates and their corresponding private keys for EPA.

d. Registration to receive a public key certificate must include authorization by a supervisor or a responsible official.

e. Public key certificates must be issued by using a secure process that both verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

f. NIST SP 800-32 must be used as guidance on public key technology.

g. NIST SP 800-63, Version 1.0.2 must be used as guidance on remote electronic authentication.

SC-18 – Mobile Code

For moderate and high information systems

a. EPA shall define acceptable and unacceptable mobile code and mobile code technologies.

Note: Mobile code technologies include, for example, Java, JavaScript, ActiveX, Portable Document Format (PDF) files, Postscript, Shockwave movies, Flash animations, and VBScript. A related term is "active content," which may refer to program code embedded in a web page or to plug-in applications intended for use in the web browser.

b. Employment of mobile code within organizational information systems must be based on the potential for the code to cause damage to the system if used maliciously.

c. EPA shall establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

    i. Usage restrictions and implementation guidance apply to both of the following:

        - The selection and use of mobile code installed on organizational servers
        - Mobile code downloaded and executed on individual workstations

d. EPA's usage restrictions must apply to all categories of mobile code technologies.

    i. Refer to *Appendix B* for information on *Categories of Mobile Code Technologies.*

        - Category 1 – high risk
        - Category 2 – medium risk
        - Category 3 – low risk
        - Emerging mobile code technologies

    ii. The following usage restrictions apply to all EPA information systems using Category 1/high risk mobile code technologies:

        - Category 1 mobile code must be signed with an EPA-approved PKI code-signing certificate or an alternate commercial signing product that has been approved by OTOP.
        - Category 1 mobile code must be obtained from a trusted source.
        - To the extent possible, all agency information systems capable of executing mobile code must be configured to disable the execution of unsigned Category 1 mobile code obtained from outside the agency-managed boundary.

    iii. The following standards apply to all EPA information systems using Category 2/ medium risk mobile code technologies:

        - Category 2 mobile code may be used if it is obtained from a trusted source over an assured channel (i.e., TLS/SSL VPN, IPsec, or other approved by OTOP).
        - Unsigned Category 2 code, whether or not obtained from a trusted source over an assured channel, may be used if it executes in a constrained environment without access to local system and network

resources (e.g., file system, Windows registry, or network connections other than to its originating host).

- Where possible, web browsers and other mobile code-enabled products must be configured to prompt the user prior to the execution of Category 2 code.
- Where possible, protections against malicious Category 2 technologies must be employed at end user systems and at system boundaries.

iv. The following standards apply to all EPA information systems using Category 3/low risk mobile code technologies:

- Category 3 mobile code technologies may be used in agency information systems.

v. Emerging mobile code technologies must not be used unless otherwise approved.

- The download and execution of mobile code using emerging technologies must be blocked by all means available at the network boundary, workstation, host, and within applications.

Note: Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet been reviewed for categorization.

e. Risk category assignments and usage restrictions for commonly used mobile code technologies must be documented and maintained in a mobile code risk category assignments list.

i. Mobile code technologies used on each information system must be documented as follows:

- The type of code and risk category for each
- Business need for the mobile code
- Mobile code scope of use including:
  - Isolated (i.e., within the accreditation boundary)
  - Internal (i.e., within EPA's network)
  - External (i.e., crosses EPA's managed network boundary)
- Controls used to restrict the scope of use
- The information system name

ii. The list of mobile code technologies used must be forwarded to the Information Security Officer (ISO) and each organization must consolidate the lists and forward them to the Senior Agency Information Security Officer (SAISO).

- The ISO lists must include recommendations for use or restriction of mobile code included on the list.
- An initial list must be forwarded to the SAISO within six months of

approval of this procedure.

iii. The SAISO shall review, approve, and aggregate individual lists to a consolidated agency list and then publish the consolidated list.

iv. Subsequent additions or changes must be forwarded from SOs during the information system life cycle to allow for selecting, testing, and approving an alternative mobile code technology, should implementation be denied for an item on the forwarded list.

v. The SAISO shall update the consolidated agency list annually.

f. EPA shall develop and publish guidelines on how needed plug-ins and other mobile software code are to be approved and obtained from software manufacturers, evaluated, and distributed by EPA.

g. The use of mobile code within the information system must be authorized only based upon a determination of risk acceptability.

i. The mobile code technology currently in use or to be used in an EPA information system must:

- Undergo a risk assessment.
- Be assigned to a risk category per requirements in *Appendix B*.

ii. In most cases the authorization will be made by the Senior Information Official (SIO) upon accreditation of an information system that relies on mobile code.

- If a mobile code technology is added or replaced by a different technology, at a minimum the System Security Plan (SSP) must be updated; a re-certification and re-accreditation may also be required.

h. Use of mobile code within the information system must be controlled, based on its potential to cause damage to EPA information, information systems, and operations if used maliciously.

Note: Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.

i. All software must be obtained through approved distribution channels, particularly through internal distribution channels set up by EPA for this purpose.

ii. The installation of mobile code applications must be limited.

- The fine print must be read before approving the software.
- Unapproved application software and plug-ins must not be downloaded and installed.
- Applications that are no longer used or needed must be deleted.

iii. All mobile code-enabled software residing on workstations and servers must be configured in compliance with the EPA Standard Configuration

Documents (SCDs).

- The Microsoft® Java implementation must be restricted as much as possible through browser settings and implementations must be required, approved, and only allowed to run at a restricted level.
- ActiveX controls must be configured as restrictive as possible to permit "official business" only.
- Third-party extensions must only be allowed for applications that are approved for use within EPA's network.
  - That is, the scope of use is "internal" and external use (crossing EPA's managed network boundary) is not allowed.

iv. Unneeded functionality must be disabled in the security settings of desktop applications unless needed for "official business."

v. When required to conduct official business, all mobile code technologies that are permitted to be used in EPA information systems under this procedure must pass through EPA information system boundary protection mechanisms.

- Refer to *SC-7 Boundary Protection* for further information.

vi. Information systems must be current with the latest software upgrades and patches that address security vulnerabilities in desktop applications, such as web browsers, readers, and email, and other critical software.

- Refer to *Information Security – Interim System and Information Integrity Procedures* for requirements on flaw remediation and malicious code protection.

vii. The EPA help desk must be contacted to report an incident when discovering evidence of an intrusion or suspicion of infection from malicious active code.

- Refer to *Information Security – Interim Incident Response Procedures* for requirements on incident reporting.

i. All users shall take appropriate precautions with respect to mobile code and active content, including but not limited to the following:

i. An isolated system and safe browser settings must be used when visiting untrusted websites.

- Visiting untrusted websites must be only for official business.

ii. Electronic documents containing active content must not be perused and software must not be downloaded from untrusted sources.

- ActiveX code must be enabled only from trusted websites that require its use.

iii. Risks and benefits must be carefully considered before creating and/or distributing documents that include active content.

j. The use of mobile code with email must be severely restricted.

i. JavaScript and any other active content processing capabilities within email desktop applications that are capable of handling Hypertext Markup Language (HTML) or other markup language-encoded messages must be disabled.

ii. Whenever possible, the automatic execution of all categories of unauthorized, unapproved mobile code in email bodies and attachments must be disabled.

iii. Whenever possible, desktop software must be configured to prompt the user with a warning prior to opening email attachments that may contain mobile code.

iv. Active content documents must not be opened and email attachments must not be executed without the recipient first verifying them with the sender.

- Users must be especially wary of attachments to electronic chain mails forwarded from or through friends.

k. Use of mobile code must be monitored.

i. EPA's Computer Security Incident Response Capability (CSIRC) must be kept informed of latest security advisories from the United States Computer Emergency Readiness Team (US-CERT) and the Computer Emergency Response Team Coordination Center (CERT-CC).

- Security mailing lists must be subscribed to and warnings and patches must be distributed as necessary.

ii. Products must be periodically cross-checked against published lists of known vulnerabilities, such as the NIST National Vulnerability Database (NVD), that provide pointers to solution resources and patch information.

iii. All EPA-owned and EPA-controlled servers must be monitored to detect the presence of prohibited mobile code.

- Any discovered prohibited mobile code must be removed.

iv. Approved mobile code-enabled software residing on workstations and servers must be monitored.

v. Information systems must be audited on a regular basis to ensure the restrictive settings are implemented correctly and remain effective.

vi. Anti-malware software, firewalls, active content filters, and dynamic behavior monitors must be implemented in accordance with standard configurations.

- These products must be upgraded to the latest version, patches, and signature files.

vii. Information systems and networks must be regularly audited and defects must be quickly remedied, and configuration variances, etc., must be documented.

- Misconfigurations must be corrected immediately.

l. NIST SP 800-28, Version 2 must be used for additional guidance regarding active

content and mobile code.

SC-19 – Voice Over Internet Protocol

For moderate and high information systems

a. EPA shall establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if maliciously used.

b. The SO shall authorize, monitor, and control the use of VoIP within the information system.

c. The following must be adhered to regarding planning and managing the integration of voice and data in a single physical network:

   i. Voice and data traffic must be separated on logically different networks, if feasible.

   ii. On IPv4 networks that are to carry voice traffic, different subnets with separate Request for Comment (RFC) 1918 address blocks must be used for voice and data traffic, with separate Dynamic Host Configuration Protocol (DHCP) servers for each kind of traffic.

   iii. The voice gateway that interfaces with the Public Switched Telephone Network (PSTN) must not allow H.323, Session Initiation Protocol (SIP), and other VoIP protocols onto the data network.

   iv. Strong authentication and access control must be employed on the voice gateway.

      - Refer to *Information Security – Interim Access Control Procedures* for requirements on access control.
      - Refer to *Information Security – Interim Identification and Authentication Procedures* for requirements on authentication.

   v. IPsec or SSH must be used for all remote management and auditing access.

      - If practical, IP Private Branch Exchange (PBX) access from a physically secure system must be used rather than remote management.

   vi. IP phones with the strongest possible encryption algorithm must be used to implement end-to-end encryption of voice traffic.

      - Strong encryption is provided by algorithms such as Advanced Encryption Standard (AES).

   vii. If end-to-end encryption is not possible for performance reasons, IPsec tunneling at the router or other gateway must be used.

   viii. Any use of “softphones” (i.e., software programs running on a workstation to make Internet-based phone calls) is prohibited.

      - The exception is when the softphones are used to achieve Section 508 compliance and therefore, are used on a dedicated appliance

that is restricted and limited to phone capability.

- The softphones must be accessible only to the VoIP network, if no other alternatives are available.

d. All VoIP systems must provide complete and accurate information to emergency call ("911") centers, unless a separate phone system is available for emergency calls.

   i. EPA shall carefully evaluate 911 service issues in planning for VoIP deployment.

      - Service issues include, for example, emergency operators being unable, in some cases, to locate a caller who is using a VoIP phone number.

Note: VoIP's packet-switched technology complicates the provision of 911 services, which normally provides the caller's location to the 911 dispatch office.

e. VoIP servers and gateways/switches must be physically safeguarded.

   i. As the first line of defense, barriers, locks, access controls, and guards must be used.

   ii. Countermeasures must be in place to protect against the insertion of sniffers and other network monitoring devices.

      - Refer to *Information Security – Interim Physical and Environmental Protection Procedures* for requirements on physical access control.

Note: Anyone with physical access to the agency network could potentially tap into telephone conversations or determine, through traffic analysis, which parties are communicating.

f. The adequacy of backup power for VoIP must be carefully assessed, using the following criteria:

   i. Agency VoIP switches as well as each desktop phone must be part of the assessment of backup power adequacy.

   ii. The cost of providing electrical power must include the cost of maintaining the uninterruptible power supply (UPS) battery charge, periodic maintenance costs for backup power generation systems, and cost of UPS battery replacement.

   iii. If electrical/backup power is required for more than a few hours, electrical generators must be used.

      - Operational costs for generators must include fuel, fuel storage facilities, generator inspection and testing, and cost of fuel disposal at end of storage life.

g. The type of security mechanisms deployed on agency data networks must be considered when deploying VoIP:

i. Since firewalls have difficulty filtering VoIP signaling traffic, VoIP-ready firewalls must be employed.

ii. Preference must be given to stateful firewalls that can process H.323 and SIP and can open and close User Datagram Protocol (UDP) ports.

- Most VoIP traffic travels across UDP ports.

iii. Alternatively, VPNs can be used to tunnel through the firewall.

iv. Using a firewall to physically broker between physically segmented traffic (i.e., one network for voice and one for data) is not recommended, since it would defeat the cost benefits of using the same physical network for voice and data.

v. Where Network Address Translation (NAT) is in use, agency network architects must confront and address the problems associated with NAT traversal and VoIP traffic.

- The router configured for NAT may be able to handle the signaling traffic, but it has no way of knowing that the audio (voice) traffic is related to the signaling. As a result, the audio traffic is not translated properly between the address spaces. Therefore, the range of industry answers to NAT traversal must be carefully evaluated and then benefits weighed against security concerns.

vi. IPsec VPN technology must be used on the VoIP system for purposes of authentication, authorization, and privacy (when encryption is enabled).

vii. VoIP also poses challenges to IDPS that must be met with the help of best-available industry solutions.

h. Quality of Service (QoS) considerations must be addressed with respect to security controls on an integrated voice-data network.

Note: Due to the time-critical nature of VoIP traffic and its low tolerance for disruption and packet loss, security controls on the integrated network can have a negative impact on QoS.

i. To prevent jitter (i.e., non-uniform or variations in delivery of packets) devices that support QoS and improve bandwidth efficiency must be employed.

ii. Bandwidth allocation must be treated as essential to VoIP quality.

- Voice is extremely intolerant of packet loss, which is often caused by bandwidth congestion.

iii. The selection and implementation of security mechanisms on the VoIP network must not lose sight of the potential for latency (i.e., the amount of time needed to deliver a packet).

- Latency in voice is less tolerated than latency in data transmission.
- Traditional firewall/NAT traversal, as well as encryption/decryption,

adds delays.

i. Mobile VoIP-enabled units must comply with the following requirements:

   i. Their use must be approved by the Chief Technology Officer (CTO).

   ii. Mobile VoIP-enabled units must comply with the either the Wireless Fidelity (WiFi) Protected Access (WPA) security protocol or its successor, WPA2.

      - Where an agency office or region has a mission need for integrating wireless devices with a VoIP system, WPA protection must be employed instead of 802.11 Wired Equivalency Privacy (WEP), which offers little or no protection.
      - Higher-level cryptographic protocols such as TLS with FIPS 140-2 validated modules must be used, when indicated by an assessment of the risks.

j. NIST SP 800-58 must be used as guidance regarding security considerations for VoIP technologies employed in the information system.

SC-20 – Secure Name/Address Resolution Service (Authoritative Source)

a. The information system must provide additional data origin and integrity artifacts (e.g., digital signatures, cryptographic keys) along with the authoritative data (e.g., DNS resource records) the system returns in response to name/address resolution queries.

   i. This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

b. Mechanisms to ensure that name/address resolution service provides additional data origin, integrity artifacts, and authoritative data in response to queries must include all of the following:

   i. Digital signatures.

   ii. Digital certificates

   iii. Digital time stamping

   iv. Domain Name System Security Extensions (DNSSEC)

   v. Approved encryption requirements and technology:

      - FIPS 140-2
      - Use of AES 128 bit or higher

c. A list must be maintained of the individuals authorized to administer each zone and name server.

   i. The list must indicate each zone and name server for which an individual has responsibility.

d. The DNS server software must execute only on agency-approved and hardened operating systems.

e. The information system's DNS server software and related portions of the underlying operating system must be configured to guard against adverse attacks to circumvent the DNS.

i. Mitigation actions must include the following:

- Configure the information system to ensure that hosts outside a boundary cannot directly query or request a zone transfer from a DNS that resides on the internal network (i.e., not in a DMZ).
- Disable dynamic updates unless the DNS software is configured to require that all dynamic updates be cryptographically authenticated.
- Review DNS logs daily or employ a near real-time log analysis or network management tool that immediately alerts an administrator of critical DNS system messages.
- Configure the DNS software to log, at a minimum, success and failure of the following events:
  - Start and stop of the name server service or daemon
  - Zone transfers
  - Zone update notifications
  - Dynamic updates

ii. Back up DNS configuration and resource record data daily.

f. The aforementioned identified mechanisms must be re-evaluated annually to ensure that the mechanisms continue to meet the security needs of the information system.

g. The information system, when operating as part of a distributed, hierarchical namespace, must provide the means to indicate the security status of child subspaces and (if the child supports secure resolution service) enable verification of a chain of trust among parent and child domains.

Note: An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS.

h. NIST SP 800-81 must be used as guidance regarding secure domain name system deployment.

SC-21 – Secure Name/Address Resolution Service (Recursive or Caching Resolver)

For high information systems

a. The information system (e.g., recursive resolving or caching DNS server) must also perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources (e.g., authoritative DNS servers) when requested by client systems.

b. A caching name server must be configured to accept recursive queries only from the IP addresses and address ranges of known, supported clients.

c. Recursion on an authoritative name server is prohibited.

d. NIST SP 800-81 must be used as guidance on secure domain name system deployment.

SC-22 – Architecture and Provisioning for Name/Address Resolution Service

For moderate and high information systems

a. The information systems that collectively provide name/address resolution service (e.g., DNS) for EPA must be configured to be fault-tolerant and must implement internal/external role separation.

Note: A DNS server is an example of an information system that provides name/address resolution service.

b. At least two DNS servers must be configured.

   i. One DNS server must be configured as the primary and the other as a secondary (or as a redundant) server.

   ii. The two DNS servers must be located in at least two different network subnets and they must be geographically separated.

   iii. The secondary (i.e., redundant primary) server must be configured to provide:

      - Redundancy
      - Load balancing
      - Distributed access

c. The alternate or backup DNS service (e.g., for contingency or disaster recovery situations) must be provided from at least one independent site, such as by the Internet Service Provider (ISP) or by another federal agency through a cooperative agreement.

d. Authoritative DNS servers must be established in regards to role separation.

   i. DNS servers with an internal role must only process name/address resolution requests from within the organization (i.e., internal clients).

   ii. DNS servers with an external role must only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet).

   iii. The set of clients that can access an authoritative DNS server in a particular role must be specified by EPA (e.g., by address ranges, explicit lists).

e. NIST SP 800-81 must be used as guidance on secure domain name system deployment.

SC-23 – Session Authenticity

For moderate and high information systems

a. The information system must provide mechanisms to protect the authenticity of communications sessions.

Note: This control focuses on communications protection at the session versus packet level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

b. The SO shall select and implement protection mechanisms to ensure adequate protection of data integrity, confidentiality, and session authenticity in transmission;

   i. Mechanisms include but are not limited to the following:
      - Security services based on IPsec
      - VPNs
      - TLS
      - DNS
      - SSH
      - SSL
      - Digital signatures
      - Digital certificates
      - Digital time stamping
      - Approved encryption requirements and technology:
        - FIPS 140-2
        - Use of AES 128 bit or higher

c. NIST SP 800-52 must be used as guidance on the use of TLS mechanisms.

d. NIST SP 800-77 must be used as guidance on the deployment of IPsec VPNs and other methods of protecting communications sessions.

e. NIST SP 800-95 must be used as guidance on securing web services.

f. NIST SP 800-113 must be used as guidance on SSL VPNs.

SC-24 – Fail In Known State

For high information systems

a. The information system must fail to a known secure state for all failures preserving the confidentially, integrity, or availability of system information and failure cause information.

Note: Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the

information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.

SC-28 – Protection of Information at Rest

Note: This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information.

For moderate and high information systems

a. The information system must protect the confidentiality and integrity of information at rest (i.e., the state of information when it is located on a secondary storage device within an information system).
    i. User and system information at rest in non-mobile devices must be protected.

Note: Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.

b. NIST SP 800-56A and NIST SP 800-56B must be referenced as guidance on establishing cryptographic keys.

c. NIST SP 800-57 must be referenced as guidance on managing cryptographic keys.

d. NIST SP 800-111 must be used as guidance on storage encryption technologies for end user devices.

SC-32 – Information System Partitioning

For moderate and high information systems

a. The information system must be partitioned into components residing in separate physical domains (or environments) as deemed necessary.
    i. Network access and information flow among partitioned information system components must be restricted or prohibited by managed interfaces.
    ii. An assessment of risk must guide the partitioning of information system components into separate physical domains (or environments).
    iii. The security categorization must guide the selection of appropriate candidates for domain partitioning.

7. RELATED DOCUMENTS

- NIST Cryptographic Module Validation Lists – http://csrc.nist.gov/groups/STM/cmvp/validation.html
- NIST National Vulnerability Database (NVD) – http://nvd.nist.gov/
- NIST SP 800-28*, Version 2, Guidelines on Active Content and Mobile Code,* March 2008
- NIST SP 800-32*, Introduction to Public Key Technology and the Federal PKI Infrastructure,* February 2001
- NIST SP 800-41, Revision 1, *Guidelines to Firewalls and Firewall Policy*, September 2009
- NIST SP 800-44, Version 2*, Guidelines on Securing Public Web Servers,* September 2007
- NIST SP 800-52*, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations,* June 2005
- NIST SP 800-53, Revision 3*, Recommended Security Controls for Federal Information Systems and Organizations,* August 2009
- NIST SP 800-54, *Border Gateway Protocol Security*, July 2007
- NIST SP 800-56A*, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,* March 2007
- NIST SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography,* August 2009
- NIST SP 800-57*, Recommendation on Key Management,* March 2007
- NIST SP 800-58*, Security Considerations for Voice Over IP Systems,* January 2005
- NIST SP 800-63*, Version 1.0.2, Electronic Authentication Guideline,* April 2006
- NIST SP 800-66*, Revision 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,* October 2008
- NIST SP 800-77*, Guide to IPsec VPNs,* December 2005
- NIST SP 800-81*, Secure Domain Name System (DNS) Deployment Guide,* May 2006
- NIST SP 800-88*, Guidelines for Media Sanitization,* September 2006
- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007
- NIST SP 800-95*, Guide to Secure Web Services,* August 2007
- NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, November 2007
- NIST SP 800-113, *Guide to SSL VPNs*, July 2008
- NSTISSI No. 7003*, Protective Distribution Systems (PDS), December* 1996

8. ROLES AND RESPONSIBILITIES

Senior Information Official (SIO)

a. The SIO has the following responsibilities with respect to system and communications protection:
    i. Understand risks and authorize the use of mobile code and mobile code technologies as permitted.
    ii. Support OTOP in the implementation and management of the system and communications protection infrastructure as required.

Senior Agency Information Security Officer (SAISO)

a. The SAISO has the following responsibilities with respect to system and communications protection:
    i. Maintain and annually update a list of permitted and not permitted mobile code and mobile code technologies for the Agency.

Chief Technology Officer (CTO)

a. The CTO has the following responsibilities with respect to system and communications protection:
    i. Approve use of mobile VoIP-enabled units.

Information Security Officer (ISO)

a. The ISO has the following responsibilities with respect to system and communications protection:
    i. Maintain and annually update a list of permitted mobile code and mobile code technologies for their program or Regional office and forward the information to the SAISO.

Office of Technology Operations and Planning (OTOP), Office of Environmental Information (OEI)

a. The OTOP, OEI has the following responsibilities with respect to system and communications protection:
    i. Analyze, plan, and implement partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access and information flow among partitioned information system components in accordance with an organizational assessment of risk.
    ii. Oversee and manage the creation of PKI framework and services that provide the generation, production, distribution, control, revocation, recovery, and tracking of PKI certificates and their corresponding private keys for EPA.
    iii. Coordinate with Office of Administration and Resources Management (OARM) regarding the implementation of PKI in Smart Cards under HSPD 12.

iv. Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if maliciously used.

v. Establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if maliciously used.

vi. Plan, manage, implement and oversee Secure Name/Address Resolution Services and secure DNS (DNSSEC) for EPA.

vii. Establish an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher.

Office of Administration and Resources Management (OARM)

a. OARM has the following responsibilities with respect to system and communications protection:

   i. Coordinate with OTOP, OEI regarding the implementation of PKI in smart cards under HSPD 12.

System Owner (SO)

a. The SO has the following responsibilities with respect to system and communications protection:

   i. Consider the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services.

   ii. Implement configuration practices to manage internal and external devices.

   iii. Prevent public access into the organization's internal networks except as appropriately allocated and mediated.

   iv. Limit the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

   v. Implement a managed interface for each external telecommunication service, implementing security controls as needed to protect the confidentiality and integrity of the information being transmitted.

   vi. Prevent the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

   vii. Employ appropriate and authorized mechanisms with supporting procedures for use of cryptography.

   viii. Use certificates from an approved, shared service provider, as required by OMB M-05-24.

   ix. Authorize, monitor, and control the use of mobile code within the information system.

   x. Ensure emerging mobile code technologies are not used unless otherwise approved.

xi. Prohibit the use of mobile code, as required.

xii. Authorize, monitor, and control the use of VoIP within the information system.

xiii. Select and implement protection mechanisms to ensure adequate protection of data integrity, confidentiality, and session authenticity in transmission of communications sessions.

xiv. Ensure the confidentiality and integrity of information at rest is protected.

xv. Configure the information system and components of the information system to fail to a known state.

Users/Individuals

a. Users/individuals have the following responsibilities with respect to system and communications protection:

i. Use an isolated system and safe browser settings when visiting untrusted Web sites.

ii. Do not visit untrusted web sites except for official business.

iii. Avoid viewing and downloading active content from untrusted sources.

iv. Carefully consider risks and benefits before creating and/or distributing documents that contain active content.

9. DEFINITIONS

- Active Content – electronic documents and other objects that can carry out or trigger actions automatically on a computer platform without the intervention of a user.
- Boundary Protection – monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
- Boundary Protection Device – a device with appropriate mechanisms that (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system) and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels.
- Collaborative Computing – an interactive multimedia conferencing application that enables multiple parties to collaborate on textual and graphic documents. Through special software, each party to the call can contribute to such documents, working together with the other parties. During such a collaborative session, the original text document is saved, while each party contributes changes that are identifiable by contributor. When the parties agree to the collaborative edits and enhancements, the entire text file is refreshed and saved. Similarly, a design or a concept can be developed graphically and on a collaborative basis through white boarding, much as the parties would do on a physical whiteboard in a face-to-face meeting. Typically, each party to the conference has access to a special whiteboard pad and stylus, which is used to draw. Each party can modify the initial drawing, with each individual's contribution identified by separate color. Again, and once the group has agreed on the final graphic rendition, the graphic is saved and all screens are refreshed (*Webster's New World Telecom Dictionary*).
- Confidentiality – the preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- External Networks – networks outside the control of the organization.
- Information at Rest – the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system.
- Information System Management Functionality – functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged users' access.
- Integrity – to guard against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- Mobile Agent – a type of mobile code that is autonomous, intelligent and can migrate from machine to machine throughout a heterogeneous network, deciding when and where to migrate, and maintaining its state. Mobile agents initiate their own execution and migration from one platform to another without any user interaction. A supporting

mobile agent platform typically resides on a machine to receive migrating mobile agents at runtime. Mobile agents may be implemented as scripts, intermediate languages (e.g., Java), or binary executables (e.g., C++).

- Mobile Agent Technologies – software technologies that provide the mechanisms for the production and use of mobile agents (e.g., Tool command language [Tcl], Aglets).
- Mobile Code – software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
- Mobile Code Technologies – software technologies that provide the mechanism for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript, Java Virtual Machine, Java compiler, .NET Common Language Runtime, Windows Scripting Host, HTML Application Host). Examples of mobile code-enabled software include operating systems (i.e., Microsoft Windows), office applications (e.g., Microsoft Office, Corel Office), browsers (e.g., Internet Explorer, Netscape, Mozilla, Firefox), email clients (e.g., Outlook, Outlook Express, Mozilla, Netscape, Thunderbird, Eudora, Lotus Notes), mobile code runtime environments (e.g., Sun Java Virtual Machine, .NET Common Language Runtime, Adobe Reader, Macromedia Shockwave Director, Macromedia Flash, Postscript readers), and mobile agent systems.
- Object Reuse – control of information in shared resources.
- Protective Distribution System – wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
- Permitted Mobile Code – types of mobile code that is allowed to be used in accordance with this Procedure when the associated usage requirements are implemented. Permitted mobile code includes signed Category 1A mobile code, unsigned Category 2 mobile code that executes in a constrained execution environment, Category 2 mobile code obtained from a trusted source over an assured channel, Category 3 mobile code, and mobile code that downloads via email that does not execute automatically when the user opens the email body or attachment.
- Prohibited Mobile Code – types of mobile code that are prohibited from being used in EPA information systems in accordance with this procedure. Prohibited mobile code includes all unapproved Category 1X mobile code, unapproved and unsigned Category 1A mobile code, Category 2 mobile code that violates this Procedure's usage requirements, all emerging technologies mobile code, and all mobile code that downloads via an email body or email attachment that executes automatically when the user opens the email body or attachment.
- 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.
- Softphone – a software program running on a general-purpose computer, usually with a headset, that enables making telephone calls over the Internet or an intranet.
- 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 Information Security Manual, Directive 2195A1, 1999 Edition, Section 11.2.6

13. ADDITIONAL INFORMATION

NA

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

APPENDIX A: ACRONYMS

AAA	Authentication, Authorization, Accounting
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASP	Active Server Page
CDP	Cisco Discovery Protocol
CERT-CC	Computer Emergency Response Team Coordination Center
CGI	Common Gateway Interface
CIO	Chief Information Officer
CMT	Cryptographic Module Testing
CSIRC	Computer Security Incident Response Capability
CTO	Chief Technology Officer
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
DMZ	Demilitarized Zone
DS	Delegation Signer
ECMA	European Computer Manufacturers Association
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
HSPD	Homeland Security Presidential Directive
ICMP	Internet Control Message Protocol
IDPS	Intrusion Detection and Prevention Systems
IO	Information Owner
IP	Internet Protocol
IPsec	Internet Protocol Security
IRC	Internet Relay Chat
ISO	Information Security Officer
ISP	Internet Service Provider
IT	Information Technology
IV&V	Independent Verification and Validation
MS-DOS	Microsoft Disk Operating System
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NTP	Network Time Protocol
NVD	National Vulnerability Database
NVLAP	National Voluntary Laboratory Accreditation Program

OARM	Office of Administration and Resources Management
OEI	Office of Environmental Information
OMB	Office of Management and Budget
OTOP	Office of Technology Operations and Planning
PBX	Private Branch Exchange
PDF	Portable Document Format
PHP	PHP: Hypertext Preprocessor
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request for Comment
SAISO	Senior Agency Information Security Officer
SCD	Standard Configuration Document
SIO	Senior Information Official
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SO	System Owner
SOC	Statement of Capability
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	System Security Plan
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIC	Trusted Internet Connection
TLS	Transport Layer Security
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
VBA	Visual Basic for Applications
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalency Privacy
WiFi	Wireless Fidelity
WPA	WiFi Protected Access
WSH	Windows Scripting Host

APPENDIX B: CATEGORIES OF MOBILE CODE TECHNOLOGIES

Category 1/ High Risk

Category 1/high risk mobile code technologies exhibit a broad functionality, allowing unmediated access to workstation, server and remote system services and resources. These pose a significant risk to EPA information systems because they allow unlimited access to a user's computer. There are two subgroups of Category 1 mobile code technologies.

Category 1a

Category 1a technologies can differentiate between signed and unsigned mobile code. The technologies can also be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code. The following are assigned to Category 1a:

- ActiveX controls.
- Shockwave movies (e.g., dcr, .dxr, .dir files), including Xtras, that execute in the Shockwave for Director plug-in.

Category 1a mobile code technologies may be used at EPA when the requirements and restrictions described in *Section 6, Procedures,* are implemented.

Category 1x

Category 1x consists of mobile code technologies that are prohibited from being used in EPA information systems beyond the local information system's authorization boundary, or to or from external entities because they cannot implement the required restrictions described in *Section 6, Procedures*. They cannot differentiate between signed and unsigned mobile code nor can they be configured to block the execution of unsigned mobile code while enabling the execution of signed mobile code. The following are assigned to Category 1x:

- Mobile code scripts that execute in Windows Scripting Host (WSH) (e.g., JavaScript or VBScript downloaded via URL file reference or email attachments)
- Hypertext Mark-up Language (HTML) applications (e.g., .hta files) that download as mobile code
- Scrap objects (e.g., .shs and .shb files)
- Microsoft Disk Operating System (MS-DOS) batch scripts
- UNIX shell scripts
- Binary executables (e.g., .exe files) that download as mobile code

Category 2/ Medium Risk

Category 2/medium risk mobile code technologies have full functionality, allowing mediated or controlled access to workstations, server, and remote system services and resources. Category 2 technologies can pose a moderate security threat to EPA information systems because they offer limited control by the user on what the code is allowed to do. They may be used when the Category 2 restrictions described in Section 6, Procedures are implemented. The following are assigned to Category 2:

- Java applets and other Java mobile code

- Visual Basic for Applications (VBA) (e.g., Microsoft Office macros, also used by Corel Office)
- LotusScript (e.g., Lotus Notes scripts)
- PerfectScript (e.g., Corel Office macros)
- Postscript
- Mobile code executing in .NET Common Language Runtime (requires Internet Explorer v.6.0/Service Pack 2 or later)

Category 3/ Low Risk

Category 3/low risk mobile code technologies support limited functionality, with no capability for unmediated access to workstation, server, and remote system services and resources. Category 3 mobile code may be freely used without restrictions in EPA information systems. Category 3 technologies pose limited risk to EPA information systems because they are very restricted in the actions they can perform. The following are assigned to Category 3:

- JavaScript, including Jscript and European Computer Manufacturers Association (ECMA) Script variants, when executing in the browser
- VBScript, when executing in the browser (requires Internet Explorer v.6.0/Service Pack 2 or later).
- Portable Document Format (PDF)
- Flash animations (e.g., .swf and .spl files) that execute in the Shockwave Flash plug-in

Emerging Mobile Code Technologies

Emerging mobile code technologies refer to all mobile code technologies, systems, platforms, or languages whose capabilities and threat level have not yet undergone a risk assessment and therefore have not been assigned to one of the three risk categories described above. Because of the uncertain risk, the use of emerging mobile code technologies in EPA information systems is prohibited unless otherwise approved by the SAISO. All mobile agent systems and platforms are emerging technologies.

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.6	1/29/08	Initial draft	Heather Flager	Procedures-SC-Draft_TO62_020_1
2.0	6/29/09	Incorporated EPA comments	Heather Flager	Procedures-SC-Final_TO62_020_2
2.8	8/11/10	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_SC_Draft.TO-062_050_1.0
2.9	12/27/10	TISS Final Draft Review	Charleen Johnson	Procedures_SC_Draft.TO-062_050_1.0
3.0	5/2/12	SAISO Final Review	David Stepp	Procedures_SC_Draft.TO-062_050_1.0
3.1	7/16/2012	Document Review	LaToya Gordon	Procedures_SC_Draft.TO-062_050_1.0