EPA INFORMATION POLICY

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO 2150.0	CIO Approval Date:	11/27/07
CIO Transmittal No.:	08-005	Review Date:	11/2010

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

Agency Network Security Policy

1 PURPOSE This Policy –

1.1 establishes a security policy for the Environmental Protection Agency's (EPA's) national data communications network (EPA network). See Section 9 for a list of definitions.

1.2 establishes principles to ensure a secure network infrastructure that integrates confidentiality, availability, and integrity into the infrastructure design, implementation, and maintenance; in order to:

1.1.1 protect the Agency's infrastructure and critical information assets from internal and external threats arising from connections to the EPA network and the Internet.

1.1.2 ensure that information technology (IT) resources attached to the EPA network are consistent with, and supportive of, a secure network IT infrastructure design.

1.1.3 protect EPA IT resources from malicious threats or unauthorized use, as well as unintentional misuse by authorized persons.

1.1.4 support the Agency in delivering reliable, high quality data in order for EPA to fulfill its mission of protecting human health and the environment.

1.1.5 maintain the appropriate level of security to support the ability of the Agency to conduct its work.

1.3 establishes the Senior Agency Information Security Officer (SAISO) as mandated by (44 USC 3544(a)(3)(A)), *Federal Information Security Management Act of 2002*.

1.4 Roles and responsibilities of the Director of the Office of Technology Operations and Planning (OTOP) includes a revised title of Chief Technology Officer (CTO).

2 SCOPE AND APPLICABILITY

2.1 All EPA employees, contractors, grantees and all users of the EPA network.

2.2 All traffic to and from the Internet and across data lines managed by the public telephone networks is governed by this policy. All access points (e.g., modems, Internet connections, workstations) are subject to this policy.

3 AUDIENCE

3.1 All EPA employees, contractors, and all users of the EPA network.

4 BACKGROUND

4.1 Historically, the EPA network operated as an open network comprised of centralized and distributed systems. While this structure was well-suited for the dissemination of public information, promotion of scientific collaboration, and provision of seamless, consistent connectivity, the Agency faces new and increasing potential threats both internally and externally arising from its use of the Internet as a major information dissemination tool.

4.2 This policy does not stand alone and must be used in conjunction with:

- Federal Information Processing Standards (FIPS)
- Directive 2195A1, EPA's *Information Security Manual*
- National Institute for Standards and Technology (NIST) Special Publications
- Agency IT resource procedures, standards and guidance (see sections 7 and 11)

4.3 Increased interconnectivity and implementing newer technologies for IT resources means the security posture of one resource can have significant impact on one or more connected resources. Therefore, to secure EPA's network infrastructure, controls must be put in place to build a secure network infrastructure and to protect all information resources connected to it.

5 AUTHORITY

5.1 *Clinger-Cohen Act of 1996* (40 U.S.C. 1401(3))

5.2 *Computer Fraud and Abuse Act of 1986* (18 USC 1030 et seq.)

5.3 *Electronic Communications Privacy Act of 1986* (18 USC 2510 et seq., 2701 et seq., 3121 et seq.)

5.4 *E-Government Act of 2002* (H.R. 2458/S. 803) (Title III, Federal Information Security Management Act)

5.5 *OMB Circular A-130*, “Management of Federal Information Resources,” Revised Nov. 30, 2000, Transmittal Memorandum No. 4

5.6 *Paper Work Reduction Act of 1995* (44 USC 3501-3519)

5.7 *Privacy Act of 1974* (5 USC 552a, as amended)

5.8 EPA Delegations of Authority, “General, Administrative, and Miscellaneous,” 1-19: Directives; 1-84: Information Resources Management.

5.9 Homeland Security Presidential Directive 12 (HSPD-12), “Policy for a Common Identification Standard for Federal employees and Contractors.”

6 POLICY

6.1 General

6.1.1 Network access and system interconnection points shall implement protection mechanisms to ensure adequate network security and controls to regulate the type and direction (in/out) of permissible network activities.

6.1.2 Network security is managed as a mission-critical activity in accordance with risk management principles and implemented as an Agency-wide security program.

6.1.2.1 All Agency contracts and procurements must be compliant with the Agency’s information security policies.

6.1.2.2 The Agency must monitor contractor compliance with information security responsibilities as specified in Agency contracts. Violations will be reported as appropriate to the Contracting Officer, OEI official, and/or Inspector General. Specific violations involving National Security Information will be reported to the Director, Security Management Division (SMD), in the Office of Administrative Services (OAS), Office of Administration and Resources Management (OARM), the Inspector General (IG), and the Contracting Officer.

6.1.3 Network security is implemented by controlling network access to all entry and exit points, maintaining network-attached resources, monitoring selected activities on the network in accordance with the Enterprise Architecture, and implementing other necessary controls. Network protection measures must be taken to ensure that only authorized and authenticated users access EPA data and IT resources.

6.1.4 Security provisions governing the EPA network are effective 24 hours per day, seven days per week in order to support continuous business operations.

6.1.5 Network procedures, technical operations, standards, and guidance for implementation of this policy shall be consistent with Agency and Federal standards, NIST requirements and guidance, Federally recognized central computer incident response/emergency response capability advisories, and documented industry standards and best practices as they are applicable to the Agency.

6.1.6 The EPA CTO issues such network procedures, technical operations, standards, and guidance for implementing this policy (hereafter referred to as “Federal and Agency security standards and requirements”).

6.2 Network Access Points

6.2.1 Network security for the Agency must be managed for all access points.

6.2.2 All Information transfer transactions that traverse EPA network access points must be directed through an Agency perimeter security defense mechanism to devices which are:

6.2.2.1 approved and registered with the CTO.

6.2.2.2 operated and maintained in conformance with Federal computer security advisories and recommendations.

6.2.2.3 configured, operated and maintained in compliance with Federal and Agency security standards and requirements.

6.2.3 Transactions that require user authentication and/or information sensitivity[1] protection must be conducted in a secure manner consistent with Federal and Agency security standards and requirements.

6.2.4 Agency perimeter security defense mechanisms must be managed and configured to deny all traffic or transmissions except as explicitly authorized.

6.2.5 Remote access to the EPA network and its IT resources must be provided through a centrally managed infrastructure designed to minimize and control risk. Remote access must also be consistent with business operational requirements and Federal and Agency security standards and requirements.

[1] Information sensitivity is defined as the level of impact on an organization or individual if there is a breach of confidentiality, availability and integrity. Impact levels are defined in FIPS 199.

6.3 Network-Attached Resources

6.3.1 Information systems must log, at minimum, all login or authentication events (including all successful and failed access attempts) and all system administration events as defined in applicable configuration documents.

6.3.2 Configurations and settings of network-attached resources must:

6.3.2.1 be tested by the responsible information system manager prior to implementation in accordance with Federal and Agency security standards and requirements.

6.3.2.2 be documented.

6.3.2.3 conform to Federal and Agency security standards and requirements, published security vulnerabilities and security best practices.

6.3.2.4 apply software patches or upgrades consistent with Agency-approved standards.

6.3.3 All EPA IT resources must be documented, monitored, tested, evaluated, and verified during its system life cycle to ensure adequate security in accordance with information sensitivity and other Federal and Agency security standards and requirements.

6.3.4 All IT resources scheduled for disposal must be adequately sanitized of all data, software, and files to protect the confidentiality of Agency information and licensing agreements.

6.3.5 Appropriate security controls are applied to all IT information system media (paper and electronic) when such media are being transported, transferred, or removed from areas under Agency control, in accordance with Federal and Agency security standards and requirements.

6.4 Physical Facilities

6.4.1 Agency IT resources must be maintained in accordance with minimum physical security requirements established in Federal regulations and standards, EPA policy, and industry best practices (http://csrc.nist.gov/fasp) to ensure adequate confidentiality, availability, and integrity of both the resources and information stored on or transmitted through the EPA network.

6.5 Personnel

6.5.1 IT positions and related functions must have an appropriate level of background screening consistent with Agency personnel and information security requirements and procedures. The level of screening will be determined by the sensitivity of the position and level of public trust. All systems administrative staff (Federal, contractor, and grantee) must have adequate background checks.

6.5.2 Information resource access privileges shall be coordinated with staff personnel actions. Any access authorizations for staff, including contractor staff, departing the Agency or moving to another function/organization within the Agency must be promptly disabled and, if appropriate, transferred.

6.5.3 Annual security awareness training must be completed by all personnel.

6.5.4 Personnel with significant network security roles and responsibilities shall complete sufficient information system security training and continuing education to ensure compliance with this policy.

6.6 Risk Management

6.6.1 Risk assessments must be conducted and updated by general support systems and major application managers at least every three years or whenever a substantive change in processing occurs. The assessment must form the basis for security plans – including their authorization and re-authorization – and associated training and awareness programs.

6.6.2 Agency-wide risks not identified and accepted by the CTO must not be accepted by the owner of a general support system without consultation and written approval by the CIO or CTO. Agency Senior Managers may accept risks to local assets only (e.g., any resource or network not connected to the EPA network and in conformance with other EPA information security policies). Such acceptance must be communicated to the CTO and reviewed to ensure risks are localized.

6.7 Access Controls and Information Safeguards

6.7.1 Appropriate controls and safeguard techniques (such as identification, authentication, certification, authorization, and encryption) must be implemented to control access to the EPA network.

6.7.2 Identification and Authentication (I&A)

6.7.2.1 All users of Agency non-public information systems must be authenticated. The strength of authentication must be commensurate with the potential impact on EPA or the individual, should there be a breach of security of the information resource being protected.

6.7.2.2 User login IDs must be unique to each authorized user and passwords must be kept private.

6.7.3 Logical Access Control

6.7.3.1 Access privileges and controls must be based, at minimum, on the principles of “need-to-know” and “least privilege” in relation to functional requirements and system impact levels in accordance with Federal and Agency security standards and requirements.

6.7.3.2 Access privileges must be documented. Credentials and associated authentication methods, must be periodically reviewed, tested and verified.

6.7.3.3 Users external to EPA's network are provided direct access via the Internet only to designated "public access" servers.

6.7.3.4 Remote access to EPA servers is provided only to EPA employees and other authorized users via the Agency's remote access infrastructure (see Section 6.2.4).

6.7.3.5 All logins for system administrative purposes and for access to the Agency's information processing capabilities must be presented with a notice advising them of consequences for unauthorized use of government information technology resources, e.g., warning banner, when accessing EPA IT resources.

6.7.4 Information Safeguards

6.7.4.1 Appropriate information safeguards (such as encryption, data filtering, tagging, or segregation) will be implemented to ensure sensitive information including Personally Identifiable Information (PII) is protected from inappropriate disclosure, misuse, or other security breaches, in accordance with Federal and Agency security standards and requirements.

6.7.4.2 Agency ensures appropriate response in the event of a breach of sensitive PII consistent with Federal and Agency standards and requirements.

6.8 Monitoring

6.8.1 Continuous monitoring, automatic alerting, and auditing with corresponding tracking capabilities and reporting are required for EPA network access points as well as devices connected to the network. The Agency must also have procedures in place to ensure an adequate and timely response to unauthorized accesses and activities. The CIO has the authority to require the installation of monitoring or auditing agents on devices connected to the network.

6.8.2 EPA has a Computer Security Incident Response Capability (CSIRC) to respond to incidents affecting EPA's IT infrastructure.

6.8.3 The CSIRC establishes procedures to contain, minimize the impact, and communicate IT security vulnerabilities and incidents. It also identifies and prepares for actual and potential threats. Proactive measures are taken to reduce the risk of potential threats.

6.8.4 Internet emergency response advisories and other IT-related advisories and warnings from Federal and select industry organizations, as appropriate, must be analyzed and implemented in a timely fashion in accordance with CTO-established procedures and guidelines.

6.8.5 The Agency conducts penetration testing, auditing, and monitoring to ensure compliance with Federal and Agency security standards and requirements. All testing, auditing, and monitoring must be conducted with the advice of and in accordance with such standards and requirements and with the knowledge and consent of the CIO or CTO.

6.9 Security Architecture

6.9.1 A Security Architecture must be an integral component of the Agency's Enterprise Architecture (EA).

6.10 Contingency Planning

6.10.1 All EPA organizations must develop, implement and maintain a contingency planning capability to address disruptions of service.

6.10.2 The procedures for executing this capability must be documented. Continuity of Support Plans are required for general support systems. Contingency Plans are required for major applications.

6.10.3 These plans may be incorporated into the system security plans and must be reviewed annually and updated as necessary.

6.10.4 Personnel must be trained to identify weaknesses or gaps in the capability.

6.11 Certification and Accreditation

6.11.1 Agency general support systems and major applications must undergo Certification and Accreditation prior to connection to EPA networks.

6.11.2 Certification and Accreditation expires after 3 years or sooner if a major change occurs.

6.11.3 All system interconnections must receive written management authorization based on acceptable levels of risk[2].

7 RELATED DOCUMENTS

7.1 Directive 2195A1, EPA's *Information Security Manual.*

7.2 Directive 2190, EPA's *Privacy Act Manual*.

7.3 NIST Special Publications, **http://www.csrc.nist.gov/publications/nistpubs/index.html**.

8 ROLES AND RESPONSIBILITIES

If individuals choose to re-delegate or to assign responsibilities, that re-delegation or assignment must be documented.

8.1 EPA Administrator

The Administrator is responsible for:

1) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the Agency, and on information systems used or operated by the Agency or by a contractor of an agency or other organization on behalf of the Agency.
2) ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the Agency.
3) ensuring that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.
4) sending to OMB an annual report on the effectiveness of the Agency's information security program, including progress on remedial actions.

8.2 Chief Information Officer (CIO)

The CIO is responsible for:

1) ensuring the EPA network security infrastructure is developed and maintained in accordance with all applicable Federal laws, regulations and Executive Orders.
2) developing and maintaining an EPA-wide information security program.
3) ensuring the development and maintenance of Agency information security policies, procedures and control techniques to address Federal policies and standards.
4) appointing the Director of the Office of Technology Operations and Planning as the Chief Technology Officer.
5) appointing a Senior Agency Information Security Officer (SAISO).
6) coordinating with senior agency officials to evaluate the effectiveness of the Agency's information security program including progress on remedial actions and to report annually to the Agency Administrator.
7) ensuring that personnel with significant information security responsibilities are trained.
8) assisting Senior Agency Managers concerning their security responsibilities.
9) approving waivers from this policy.
10) maintaining a central record of all waivers to this policy.

8.3 OTOP Office Director (OTOP OD)

The OTOP OD is responsible for:

1) serving as the Chief Technology Officer (CTO). (This permanently replaces the DCIOT title.)

2) defining, identifying, developing, communicating, and issuing security procedures,

technical operations and standards, and related guidance for the EPA network.

3) ensuring that appropriate threat and risk information is exchanged with Senior Information Officials (SIOs) Information Management Officers (IMOs) Information Security Officers (ISOs) information system managers, and Information System Security Officers (ISSOs)
4) developing a program to manage the central IT infrastructure in a manner that ensures the continuing confidentiality, integrity, and availability of information and connected Agency IT resources.
5) developing the Agency's Security Architecture.
6) defining protection perimeters and ensuring implementation of these protections to safeguard the EPA network from external and internal threats.
7) ensuring the development of procedures and standards for network security and capacity monitoring.
8) ensuring that monitoring is conducted for potential and actual threats to the network and Agency IT resources.
9) ensuring the implementation of certification and accreditation processes to support risk and security management of general support systems and major applications.
10) ensuring only systems certified as compliant with this policy and authorized by management to operate are attached to the network.
11) providing on-going security awareness training for all personnel.
12) ensuring the operation of a CSIRC.
13) establishing procedures for Internet and other IT infrastructure-related emergency response advisories, warnings, and incident response procedures.
14) managing the IT security infrastructure to protect access points of EPA's network.
15) delegating to Regions and other entities as appropriate, co-management responsibilities for EPA's IT security infrastructure.

8.4 Senior Agency Information Security Officer (SAISO)

The SAISO [sometimes referred to as the Chief Information Security Officer (CISO)] is responsible for:

1) carrying out the Chief Information Officer's responsibilities for information security.
2) possessing professional qualifications, including training and experience, required to administer the information security program functions.
3) having information security duties as their primary duty.
4) heading an office with the mission and resources to assist in ensuring Agency compliance with this policy and with applicable Federal regulations.
5) supporting the Agency CIO in annual reporting to the Agency Administrator on the

effectiveness of the Agency information security program, including progress of remedial actions.

6) serving as the CIO's primary IT security liaison to the Agency's information security community including SIOs, IMOs, ISOs, information system managers, and ISSOs.

8.5 Agency Senior Managers [Deputy Administrator, Assistant Administrators (AAs), General Counsel, Inspector General (IG), Chief Financial Officer (CFO), Associate Administrators, and Regional Administrators (RAs)].

Agency Senior Managers are responsible for:

1) serving as the delegated authority for information and information technology management within their organizations.
2) ensuring that the security of each network-connected general support system and major application under the responsibility of their organization is managed in accordance with Federal and Agency security standards and requirements.
3) ensuring that the organizational information security program under their management control includes infrastructure security components for the network in accordance with Federal and Agency security standards and requirements.
4) reporting annually to the CIO on the status of their organization's security program compliance.
5) ensuring implementation, follow-up, and coordination of activities in response to IT security alerts and incidents in a timely manner.
6) ensuring participation, coordination, and training of appropriate staff in the Agency's information security program.
7) ensuring that the Information Security Officers (ISOs) have access to the appropriate Senior Information Officials (SIO), Senior Resource Officials (SRO), and Information Management Officers (IMO) regarding security-related issues.
8) ensuring risk assessments, security control reviews, and other related reviews are performed for general support systems and major applications under their organization's responsibility.
9) ensuring that incident and risk assessment information is used to improve security and provide improved user awareness and training.
10) ensuring that personnel with significant security responsibilities are provided with sufficient training to comply with Federal and Agency security standards and requirements.

8.6 Inspector General (IG)

The IG is responsible for:

1) providing assistance to improve the efficiency and effectiveness of EPA's security program.
2) performing an annual independent evaluation of the Agency information security program and practices to determine the effectiveness of such program and practices.

3) conducting criminal investigations when warranted.

8.7 Computer Security Incident Response Center (CSIRC)

The CSIRC is responsible for:

1) developing and maintaining standard operating procedures to minimize, contain, and communicate computer incidents.
2) ensuring prompt response and documentation of all computer incidents.
3) ensuring threat and incident information is reported, communicated, and used to inform the Agency's IT security risk management, awareness and training, privacy, and physical security management programs.
4) cooperating with internal and external security and investigation authorities including the Inspector General when warranted.

8.8 Senior Information Official (SIO)

The SIO is responsible for:

1) Ensure establishment and implementation of effective processes and procedures within their organization for compliance with Agency information and information technology policies, procedures, operations and standards; statues; and Executive Branchy directives; including, but not limited to those relating to information assurance
2) Ensuring the information technology operated within their organization is managed effectively, including establishment of an internal monitoring program to evaluate policy effectiveness within their organization and consistent with Federal and Agency security standards and requirements.
3) establishing and implementing effective business processes and procedures within their organizations to ensure compliance with Federal and Agency security standards and requirements.
4) ensuring that personnel are provided with sufficient training to comply with Federal and Agency security standards and requirements.
5) accepting and forwarding IT waiver requests.

8.9 Information Management Officer (IMO)

The IMO is responsible for:

1) implementing and administering network security policy within their organization.
2) ensuring that network security policies, procedures, standards and related issues are fully documented and considered in the organization's information security program and in IT resources planning, budgeting, and system acquisitions.
3) participating in the planning and maintenance of network security infrastructure and associated operations for their organization.

4) conducting comprehensive assessments of management, operational, and technical security controls in an information system.

5) determining and certifying the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

6) making accreditation recommendations to the Authorizing Official (AO).

8.10 Information Security Officers (ISO)

The ISO is responsible for:

1) coordination and dissemination of CSIRC and risk management information and ensuring procedures are implemented and corrective actions are taken.
   a. serving as a primary point of contact and coordinator during any security incident involving a system or application under their purview.
   b. documenting and retaining the records concerning all security incidents involving a system or application under their purview.
   c. assisting in the investigation and resolution of any security incidents in conjunction with the CSIRC.
2) ensuring that periodic testing of security controls is conducted and those controls are operating effectively.
   a. ensuring that daily IT operations and security responsibilities are designed to effectively monitor and comply with Federal and Agency security standards and requirements.
   b. assisting in the development of risk assessments, security controls reviews, and other security reports as necessary.
   c. evaluating the technical and non-technical security features of the information system in support of the accreditation process.
   d. evaluating system controls and determining whether or not those controls provide the proper level of security.
   e. providing independent review as appropriate.
3) assisting general support system and major application managers in planning for and establishing adequate security for the general support system or major application as appropriate.
   a. providing advice and guidance on developing security plans.
   b. ensuring that security plans and related activities are completed in compliance with Federal and Agency security standards and requirements for systems under their organizational responsibility.
   c. ensuring security plans under their organization's responsibilities remain current.
   d. tracking and maintaining copies of security plans as submitted by general support system and major application managers.
4) providing ongoing user security awareness and training.
5) reporting as necessary, including unresolved security issues to Agency officials,

including the SIO and IMO on the status of compliance within their organization to this policy.

a. reporting the status of the IT security program within their organization annually to their Agency Senior Manager as appropriate.

b. ensuring general support systems or major applications developed in their organizations are reported to the Agency's central FISMA inventory.

8.11 Information System Managers

Information system managers are responsible for:

1) reviewing and reporting on the level of compliance with Agency policies, procedures and standards as required.
2) ensuring that security controls implemented on their general support systems or major applications adequately support management, operational, and technical requirements as defined in this policy and CTO-issued procedures, standards, and operating practices.
3) documenting information system changes and assessing the potential impact on the security of the system throughout the information system life cycle.
4) ensuring that Agency and organizational policies and controls are implemented, performing as expected, and are documented in up-to-date security plans.
5) managing user authorization and access in accordance with this policy.
6) establishing the rules for the appropriate use and protection of the subject data/information (rules of behavior).
7) ensuring system users and support personnel receive the requisite security training.
8) participating in Agency and organizational security risk management programs.
9) categorizing information under their control in accordance with Federal and Agency security standards and requirements.
10) complying with all CSIRC procedures and incorporating them into system procedures, as appropriate.
11) ensuring that an ISSO is assigned in writing to be responsible for the security of each general support system or major application, as appropriate.

8.12 Information System Security Officer (ISSO)

The ISSO is responsible for:

1) ensuring the security and compliance with Federal and Agency security standards and requirements of the information system for which they are assigned responsibility, throughout its life cycle.
2) assisting in the development of risk assessments, security control reviews, and other security reports as necessary.
3) performing evaluations of the technical and non-technical security features of the

information system for which they are assigned responsibility, in support of the accreditation process.

4) evaluating system controls and determining whether or not those controls provide the proper level of security.
5) ensuring users and system support personnel have the required clearances, authorization, and need-to-know.
6) ensuring that users are instructed on the Rules of Behavior before they are granted access to the information system.
7) serving as a primary point of contact and coordinator during any security incident involving the information system for which they are assigned responsibility.
8) documenting and retaining the records concerning all security incidents involving the information system for which they are responsible.
9) reporting any unresolved security issues to the system manager and/or ISO.
10) developing and updating the system security plan.
11) coordinating changes to the system and assessing the security impact of those changes.

8.13 Managers and Supervisors

Managers and Supervisors are responsible for:

1) ensuring personnel with significant network security roles and responsibilities complete sufficient information system security training and continuing education to ensure compliance with this policy.
2) ensuring that the appropriate level of background checks are conducted for those who have access to sensitive information or manage/administer technical content of automated information systems.
3) ensuring information systems under their control are certified and accredited before they are implemented in a production environment.
4) ensuring appropriate resources are available to meet information security requirements.
5) serving as the Authorizing Official for systems under their control.

8.14 EPA Employees and Contractors

EPA employees and contractors are responsible for:

1) using EPA network resources for official government business or for other authorized use in accordance with Agency policies.
2) being aware of information security requirements associated with each system and application they use.
3) completing annual security awareness training.
4) managing and protecting their passwords.

5) implementing required security controls.
6) following the documented rules for the appropriate use and protection of the subject data/information (rules of behavior).
7) safeguarding sensitive information.

8.15 Chief Enterprise Architect

The Chief Enterprise Architect is responsible for:

1) developing and maintaining the Agency's Enterprise Architecture, including the Agency's Security Architecture.
2) facilitating the integration of information security into all layers of enterprise architecture to ensure Agency implementation of secure solutions.

8.16 Senior Resource Officials (SRO)

SROs are responsible for:

1) ensuring appropriate resources are available to meet information security requirements.
2) ensuring that significant security resource issues are resolved.

8.17 Director, Office of Administration in the Office of Administration and Resource Management (OARM)

The Director, OA, is responsible for:

1) developing, promulgating, implementing, and monitoring the organization's physical and personnel security programs.
2) establishing and implementing physical security standards, guidance, procedures, and controls in accordance with EPA information security and Federal physical security policies.

8.18 Agency Privacy Act Officer

1) developing, promulgating, implementing, and monitoring the organization's privacy program.
2) developing and implementing response procedures in the event of a breach of sensitive PII, commensurate with risk of harm to the individual.
3) ensuring coordination with agency managers, including, but not limited to, CIO, CTO, SAISO, CSIRC, OIG, and OGC

9 DEFINITIONS

Reference: National Institute of Standards and Technology, *Glossary of Key Information Security Terms*, April 25, 2006.	
Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals based on the implementation of an agreed-upon set of security controls.
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Contingency Planning	IT contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. Contingency planning generally includes one or more of the approaches to restore disrupted IT services: • Restoring IT operations at an alternate location • Recovering IT operations using alternate equipment • Performing some or all of the affected business processes using non-IT (manual) means (typically acceptable for only short-term disruptions).
Enterprise Architecture	The Enterprise Architecture provides a model of the Agency's strategic direction, organizational programs and projects, lines of business, information technology portfolio (i.e., data, applications, and technologies), security measures, and the inter-relationships among them. It is maintained to provide support for the Agency's strategic planning, budget formulation and execution, information technology capital planning, information technology acquisition, human capital, and security planning processes.
Firewall	A gateway that limits access between networks in accordance with local security policy.
General Support System	An interconnected set of information resources under the same direct management control which shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Information Security Officer (ISO)	The official responsible for ensuring that information security programs in their organizations are implemented in accordance with Federal and Agency security standards and requirements.
Information Systems Security Officer (ISSO)	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that: 1) requires the use of such equipment. 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
IT infrastructure	Underlying basic facilities, equipment, installation and support structure that supports information processing. The infrastructure is defined by its location and management control, e.g., Headquarters infrastructure or the infrastructure in one of the regional offices.
Internet	Worldwide collection of networks and gateways that use the TCP/IP suite of protocols to communicate with one another. It offers a range of services to users including FTP, E-mail, the World Wide Web, IRC, telnet and others.
Intranet	Private EPA network based on Internet protocols such as TCP/IP but designed for information management within the Agency. The intranet is logically separate and physically protected from the Internet by enhanced security controls such as firewalls.
IT Resources	Information technology hardware, software, or data that is part of a larger system.

Major Application	An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
National Data Communications Network (EPA network)	Information system resources and general support systems and applications under EPA's direct management and control including on-site contractor IT resources.
Network	A system that transmits any combination of voice, video and/or data between users.
Network Access	The establishment of connectivity between one device and another via telecommunications technology such that the two may exchange data.
Network Access Point	A device or set of technologies that provide an interface to establish connectivity to a network, or between two separate networks. A network access point provides the physical and logical capability for a device to exchange data with network-attached resources.
Network-Attached Resources	Any resource with an Internet Protocol (IP) address or IT-related object on the EPA network.
Network Security	The authorization of access to files and directories in a network.
Perimeter Security	Protection of information resources based upon real-time decisions about whether requested information flows should occur, based on the location, form, or content of the flow in context.
Personally Identifiable Information	Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
Sensitive Personally Identifiable Information	Social security numbers or comparable identification numbers; financial information associated with individuals; and medical information associated with individuals.

Remote Access	Access by users (or information systems) communicating external to an information system security perimeter.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Security Architecture	A description of security principles and an overall approach for complying with the principles that drive the system design: i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies
Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Standard Operating Procedure (SOP)	Established procedure to be followed in carrying out a given operation or in a given situation.
System Security Plan (SSP)	See *Security Plan.*
TSSMS Account	Time Sharing Services Management System account (TSSMS) which registers the customers who can access the National Computer Center's computers and other resources.
Wide Area Network	Private long distance network that uses leased lines to connect computers or Local Area Networks. Abbreviated as WAN.

10. WAIVERS

10.1 Offices may request exception to this policy 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

10.2 The CIO may grant a waiver to this policy for sufficient reasons exercising judgment in the best interests of Agency security and ensuring that oversight procedures are in place so that overall network security is not compromised.

10.3 A central repository of all waiver(s)shall be maintained.

11. RELATED PROCEDURES AND GUIDELINES

Reference	Description/URL
Federal Information Processing Standards (FIPS)	**FIPS** documents are mandatory federal standards that federal agencies must follow. **FIPS 140-2,** *Security Requirements for Cryptographic Modules*, May 2001, provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. **FIPS 199**, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, documents standards for categorizing information and information systems. **FIPS 200**: *Minimum Security Requirements for Federal Information and Information Systems, March 2006,* specifies minimum security requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, as amended. **http://csrc.nist.gov/publications/fips/index.html**
National Institute of Standards and Technology Special Publications (NIST SP) 800 series	**NIST SP 800 series** documents are federal guidelines for use by federal agencies. The following are some of the more important guideline documents available on the NIST website: **NIST SP 800-100,** *Information Security Handbook: A Guide for Managers*, October 2006 **SP 800-88,** *Guidelines for Media Sanitization*, September 2006 **SP 800-64,** *Security Considerations in the Information System Development Life Cycle*, *(revision 1 released June 2004)* **SP 800-61,** *Computer Security Incident Handling Guide*, January 2004

	SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* June 2004 **Draft SP 800-53A,** *Draft Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems* **SP 800-53 Rev. 1,** *Recommended Security Controls for Federal Information Systems*, December 2006 **SP 800-50***, Building an Information Technology Security Awareness and Training Program*, October 2003 **SP 800-37,** *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004 **SP 800-34,** *Contingency Planning Guide for Information Technology Systems*, June 2002 **SP 800-30,** *Risk Management Guide for Information Technology Systems*, July 2002 **Draft SP 800-26, Rev. 1,** *NIST DRAFT Special Publication 800-26, Revision 1: Guide for Information Security Program Assessments and System Reporting Form,* August 2005 **SP 800-18 Rev. 1,** *Guide for Developing Security Plans for Federal Information Systems*, February 2006 **SP 800-16,** *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* April 1998 **http://csrc.nist.gov/publications/nistpubs/index.html**
EPA Orders and OEI Policies	**EPA Orders** are EPA's internal administrative polices. **2030.1A,** *Continuity of Operations Policy,* 4/27/05[1] **2040.1a1**, *National Security Emergency Preparedness Policy*, 2/6/01[1] **2060.1A**, *Disaster Assistance Coordination*, 12/2/77[1] **2100.1**, *Accessible Electronic and Information Technology,* 4/5/061 **2100.3A1**, *Policy on Limited Personal Use of Government Office Equipment,* 4/2/04[1] **2100.5**, *System Life Cycle Management Policy*, 4/7/06[1] **2151.0**, *Privacy Policy*, 9/27/07[2] **2165.1**, *Software Management and Piracy Policy,* 5/15/03[1] [1]**http://intranet.epa.gov/rmpolicy/ads/transorders.htm** [2]**http://intranet.epa.gov/oei/imitpolicy/policies.htm**

EPA Manuals	**EPA Manuals** are information technology/information management and related policies. **2190**, *Privacy Act Manual,* 12/2005 **2100B8,** *Information Resources Management (IRM) Policy Manual*, 6/15/01 **2195A1**, *Information Security Manual*, 12/20/99 **http://intranet.epa.gov/rmpolicy/ads/transmanuals.htm**
Security Procedures (IT SECURITY Website)	This website contains EPA security policies, such as the ANSP; procedures, such as the Personnel Security Handbook; technical operations and standards that describe the technical standards required to meet Agency security policies; and security-related guidance that provides details on technical implementation of security requirements. **http://intranet.epa.gov/itsecurity/polprocedures.html**
Operational Directives	Technical information that describes how to implement procedures that pertain to other assets. **http://basin.rtpnc.epa.gov/ntsd/directives.nsf/BySub?OpenView**
LAN Operational Procedures and Standards Manual (LOPS)	Technical information that describes how to implement procedures that pertain to LANS. **https://intranet.epa.gov/nis/lops.html**
NCC Systems Engineering Procedures	Technical, miscellaneous, and deployment papers **http://cfint.rtpnc.epa.gov/otop/network/index.cfm** **http://lansys.epa.gov/** **http://ion.rtpnc.epa.gov/unix/policies/index.html**
Standard Configuration Documents (SCD)	Technical configuration documents **http://cfint.rtpnc.epa.gov/otop/dss/index.cfm**
Lotus Notes Databases	The Lotus Notes databases are another storage location for agency standards. Need to know person that has access to the desired Lotus Notes database to get into the site.

12. MATERIAL SUPERSEDED / RESCINDED

12.1 Supersedes the previous ANSP 2195.1 A4, dated 3/30/01.

12.2 Rescinds EPA Manual 2196, *Information Security Manual for Personal Computers*, dated 4/30/93.

12.3 Rescinds *Information Resource Management (IRM) Policy Manual*, 2100B8, Chapter 8, “Information Security.”

13. ADDITIONAL INFORMATION

For additional information, contact:

Myra Galbreath, Chief Technology Officer, (202) 566-0300, **galbreath.myra@epa.gov**.

Marian Cody, Chief Information Security Officer, (202) 566-0302, **cody.marian@epa.gov**.

Molly A O'Neill

Molly A. O'Neill Assistant Administrator
and Chief Information Officer
Office of Environmental Information