

CHAPTER 10

INFORMATION ASSURANCE (IA)

TABLE OF CONTENTS

10.001	Purpose
10.002	Scope
10.003	References
10.004	Definitions
10.005	Goal(s)
10.006	Policy
10.007	Responsibilities

The Information Assurance (IA) policy outlined in this chapter is supported by specific guidance, technical standards, and requirements documents. All of these documents combine to present a comprehensive body of IA direction for the U.S. Department of Transportation. The supporting body of IA documentation is listed in the References section of this chapter.

10.001 Purpose

This purpose of this chapter is to set forth the uniform policy, responsibilities, and authorities for the implementation and protection of the U.S. Department of Transportation's (DOT's) information technology (IT) systems that store, process or transmit unclassified information. Unclassified IT systems must be designated as Sensitive But Unclassified (SBU).

10.002 Scope

This policy applies to all DOT Operating Administrations (OAs), personnel, IT systems (to include hardware, software, media, and facilities), and to contractors acting on behalf of the Department. This policy also applies to any outside organizations, or their representatives, who are granted access to the Department's IT resources, such as other Federal agencies. This policy order provides the minimum requirements for the protection of Sensitive but Unclassified (SBU) IT systems used to collect, create process, transmit, store, and disseminate information by, or on behalf of, the Department. The requirements are based upon Federal statutes, regulations, Executive Orders, Office of Management and Budget (OMB) circulars, and other applicable direction.

The Department CIO will issue implementing technology policies and standards to support management, operational, and technical controls.

10.003 References

The following list of references is not intended to represent the entire body of guidance and direction applicable to the Department's IA policy. This list is not exhaustive. Other Federal laws, regulations, and guidance not listed here may apply. The following references represent significant supporting documents to the Department's IA policy:

1. Federal Laws and Regulations.

- a. Public Law 104-50, *Department of Transportation and Related Agencies Appropriation Act of 1996*, section 348, FAA Acquisition Management System.
- b. Public Law 107-347, *Federal Information Security Management Act of 2002*, December 17, 2002.
- c. Public Law 107-296, *Critical Information Infrastructure Act of 2002*.
- d. Public Law 104-106, *Clinger-Cohen Act of 1996*.
- e. Public Law 99-474, *The Computer Fraud and Abuse Act*.
- f. *United States Code of Federal Regulations (CFR)*, Department of Transportation (DOT), 49 CFR, Part 1520, "Protection of Sensitive Security Information."
- g. 5 United States Code (U.S.C.) Section 552, "The Privacy Act of 1974."
- h. 44 U.S.C. Chapter 35, "Coordination of Federal Information Policy."
- i. 49 CFR Parts 15 and 1520, "Protection of Sensitive Security Information."
- j. 49 U.S.C. Section 40119, "Sensitive Security Information."
- k. 29 U.S.C. 40119, Department of Transportation, Sensitive Security Information.
- l. *United States Code of Federal Regulations (CFR) 29*, Department of Homeland Security, "Procedures for Handling Critical Infrastructure Information."

2. Executive Orders.

- a. Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, April 3, 1984.
- b. Executive Order 13011, *Federal Information Technology*, July 16, 1996.
- c. Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.

3. Office of Management and Budget (OMB).

- a. OMB Circular Number A-130, *Management of Federal Information Resources*, February 8, 1996.
- b. OMB Circular Number A-123, *Management Accountability and Control*, revised June 21, 1999.
- c. OMB Circular A-11, *Preparation, Submission, Execution of Budgets*, July 16, 2004.
- d. OMB Memorandum M-00-10, *Procedures and Guidelines on Implementing the Government Paperwork Elimination Act*, April 25, 2002.
- e. OMB Memorandum M-99-18, *Privacy Policies on Federal Web Sites*.
- f. Presidential Decision Directive (PDD) 12, *Security Awareness and Reporting of Foreign Contacts*, August 5, 1993.

4. **Department of Homeland Security (DHS).**
 - a. Homeland Security Presidential Directive (HSPD-12), DHS Policy Directive 3, *Homeland Security Advisory System*, March 11, 2002
 - b. Homeland Security Presidential Directive (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
 - c. Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Operations* (October 21, 1998).

5. **Department of Commerce (DOC). National Institute of Science and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (SP).**
 - a. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
 - b. FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, February 25, 2005.
 - c. FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001.
 - d. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995.
 - e. NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.
 - f. NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems, Revision 1*, February 2006.
 - g. NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, November 1999.
 - h. NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.
 - i. NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.
 - j. NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.
 - k. NIST SP 800-31, *Intrusion Detection Systems (IDS)*, November 2001.
 - l. NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
 - m. NIST SP 800-36, *Guide to Selecting Information Security Products*, October 2003.
 - n. NIST SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*, May 2004.
 - o. NIST SP 800-40, *Procedures for Handling Security Patches*, September 2002.
 - p. NIST SP 800-44, *Guidelines on Security Public Web Servers*, September 2002.
 - q. NIST SP 800-45, *Guidelines on Electronic Mail Security*, September 2002.
 - r. NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002.
 - s. NIST SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, November 2002.

- t. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.
- u. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.
- v. NIST SP 800-53a, *Guide for Assessing the Security Controls in Federal Information Systems*, July 2005.
- w. NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.
- x. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, August 2003.
- y. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security System*, August 2003.
- z. NIST SP 800-61, *Computer Security Incident Handling Guide*, January 2004.
- aa. NIST SP 800-63, Version 1.0.1, *Electronic Authentication Guideline*, September 2004.
- bb. NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003.
- cc. NIST SP 800-73, *Interfaces for Personal Identity Verification*, April 2005.

6. Department of Transportation (DOT).

The Department of Transportation inherently subscribes to the standards, guidelines and implementation polices of the NIST organization. In situations for which the DOT has not developed a policy, standard or guideline relative to any Information or Information System Security subject, DOT implementation will revert to the published NIST document pertaining to that subject.

In the area of system design, C&A and security configuration, all DOT systems will subscribe and be compliant with the standards and benchmarks developed by the Information Assurance Program Office, or in absence of such a published standard the DOT will revert to CIS for that IT systems security configuration standard.

- a. DOT Handbook 1350.2, *Departmental Information Resources Management Manual, Information Systems Security Program*, May 1, 2001.
- b. DOT Handbook 10-202, *Departmental Guide to Network Security*, April 24, 2002.
- c. DOT Personal Data Assistant (PDA) and Wireless Technologies Security Implementation Guidelines, January 2004.
- d. DOT memorandum, Federal Information Security Management Act, DOT Guidelines, August 2003.
- e. DOT H 1350.250 Series: “Departmental Information Protection Planning”
- f. DOT H 1350.260: “Departmental Guide to Protecting Information Technology”
- g. DOT H 1350.270 Series: “Departmental Guide for Information Protection Awareness/Training”
- h. DOT Order 1630.2, Personnel Security Management.

7. Other Sources.

10.04 Definitions

The following list of definitions are provided for clarity and consistency in interpreting the policy set forth in this document. This list is not intended to be comprehensive or all inclusive.

Acceptable Level of Risk. An authorizing official conducts an assessment that an information system meets the minimum requirements of applicable security directives and the risks associated with the system's operation are reduced to an acceptable level. The assessment should consider the sensitivity and criticality of information, threats and vulnerabilities, countermeasures, and the effectiveness in compensating for vulnerabilities, and operational requirements.

Access Control. The process of limiting access to the resources of an information system only to authorized users, programs, processes, or other information systems.

Accountability. The quality or state that enables violations or attempted violations of ISS to be traced to individuals who may then be held responsible.

Accreditation (adapted from NIST SP 800-37). 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, agency assets, or individuals based on the implementation of a set of agreed-upon security controls and countermeasures.

Audit Trail. An audit trail is a chronological record of information system activities that enables the reconstruction, reviewing, and examination of a sequence of events.

Authorization. See Accreditation.

Authorizing Official (AO) (adapted NIST SP 800-37). The authorizing official (previously, designated approving authority) is a senior executive, appointed in writing by the head of LOB or SO, who determines whether to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

Availability. The requirement to provide timely, reliable access to data and information services for authorized users.

Certification. A comprehensive assessment of the management, operational, and technical 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.

Certification and Accreditation Package. A document presented to the authorizing official for final accreditation of the information system. The C&A package includes the ISS plan, vulnerability assessment report, risk assessment, security test plan and security test results, disaster recovery and contingency measures, and ISS C&A statements.

Certification Team. A group of individuals who are responsible for performing the certification and accreditation work and is accountable for the content and quality of all documentation. Typically, the ISS Certifier or information system owner appoints the Certification Team.

DOT Chief Information Officer (CIO). The Chief Information Officer (CIO) is the DOT official responsible for: designating a senior DOT Chief Information Security Officer; developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements; training and overseeing personnel with significant responsibilities for information security; assisting senior DOT officials concerning their security responsibilities; and in coordination with other senior DOT officials, reporting annually to the Secretary of Transportation on the effectiveness of the DOT information security program, including progress of remedial actions. The CIO, with the support of the senior DOT Chief Information Security Officer, works closely with AOs to ensure that an agency-wide security program is effectively implemented and that there is centralized reporting of all security-related activities.

Chief Information Security Officer (CISO). The Chief Information Security Officer (CISO) is the senior management official responsible for developing and maintaining the resources to ensure IA compliance. The CISO reports directly to the CIO.

Deputy Chief Information Security Officer (DCISO). The Deputy Chief Information Security Officer (DCISO) is the senior management official, subordinate to the CISO, for the technical implementation and compliance with FISMA, and implementation of the IA program. The Deputy CISO is also responsible for cyber protection, detection, identification, and authentication, and response to all cyber incidents.

Confidentiality. A requirement to protect an information system from intentional or accidental attempts to disclose sensitive data and information to, or by, unauthorized individuals.

Configuration Management. The management of security features and assurances through control of changes made to hardware, software, firmware, test plans and procedures, test fixtures, and documentation throughout the life cycle of an information system.

Contingency Plan (NIST SP 800-34, adapted). Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Contingency Measures (NIST SP 800-34, adapted). Measures maintained for emergency response, backup operations, and post-disaster recovery for an information system, ensuring the availability of critical resources and facilitating the continuity of operations in an emergency situation.

Continuity of Operations Plan (COOP) (NIST SP 800-34). A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for 30 days as a result of an emergency or disaster event before returning to normal business operations.

Countermeasures (CNSS Instruction 4009). Actions, devices, procedures, techniques, or other measures, which can reduce the vulnerability of an information system. This term is synonymous with security controls and safeguards.

Critical Infrastructure Protection (CIP). The national critical infrastructure is defined as the assets, systems, and functions vital to our national security, economic need, or national public health and safety. Homeland Security Presidential Directive-7 (HSPD-7), December 17, 2003, formerly designated the National Airspace System (NAS) as part of the national critical infrastructure.

Critical System. A system whose information, if modified or denied, could significantly increase the risk of placing someone in jeopardy of injury or death, or could significantly increase the risk of violating public trust.

Cyber-incident Handling. A practice, technique, or method used in response to a suspected, observed, reported, or otherwise detected cyber incident.

Cyber-incident Handling Program. A set of plans, policies, guidelines, and procedures that ensure resources are available to respond to a suspected or known violation of an explicit or implied security policy.

Data. A collection of programs, files, or other information stored in, or processed by, a computer system and has a specific physical representation.

Denial of Service. Unauthorized access to information resources or systems that degrades or prevents performance at specified levels.

Designated Approving Authority (DAA). See Authorizing Official (AO).

Disaster Recovery Plan (DRP). A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

Event. Any observable occurrence in a network or system. Events include a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail (e-mail), and a firewall blocking a connection attempt.

Facility. Any facility that is owned, leased, or loaned to the FAA, where agency information systems, or any portion of those systems will be developed, housed, or operated; or where FAA information is collected, stored, processed, disseminated, or transmitted using agency owned or leased equipment.

Firewall. A set of related infrastructure that protects the resources of a private network from other networks. A firewall, working closely with a router, filters all network packets to determine whether to send them toward their destination. A firewall is often installed away from the rest of the network so no incoming request can get directly at private network resources.

Incident. A violation or imminent threat of violation of agency computer security policies, acceptable use policies, or standard security practices.

Incident Handling. The process of mitigating a violation of security policies, acceptable use policies, and standard computer security practices.

Information (FIPS 199). An occurrence of an information type.

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Steward (FAA Order 1375.1X). For information originating within the FAA, the information steward is the manager responsible for establishing the rules for the use and protection of the subject information. For information originating elsewhere, the information owner is the originating entity, represented by a designated individual.

Information System (OMB Circular A-130, Appendix III, adapted). A discrete set of information resources, either in stand-alone or networked configurations, that is organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Information systems are of two types:

1) General Support Systems (OMB A-130, Appendix III). Interconnected information resources that are under the same direct management control and share common functionality, e.g., telecommunications and networks.

2) Major Application Systems (FISMA). Systems that require special management attention because of their importance to an agency's mission; their high-maintenance, development, and operating costs; or their significant role in dealing with the agency's programs, finances, property, or other resources.

Information System Owner (ISO). The manager responsible for the organization that sets plans, direction, and manages funds for an operational information system. Systems under development are owned by the developing organization until accepted and authorized by the operating organization.

Information Systems Security (ISS). The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction and the assurance of confidential, integrity, and availability.

Information Systems Security Certification Agent (ISSCA). A senior level manager responsible for ensuring an impartial, quality assurance review of the C&A package. He or she makes recommendations to the ISS Certifier and the authorizing official, as appropriate.

Information Systems Security Certifier (ISSC). A senior manager in the developmental or operational organization that owns the information system and is responsible for certifying that information system security technical controls are present and functional, management and physical controls are described and in place, and risk has been mitigated commensurate with the magnitude of harm.

Information Systems Security Manager (ISSM). An ISSM is a full-time Federal employee responsible for ensuring the appropriate operational security posture is maintained for an information system or program within a single line of business (LOB) and staff office (SO).

Information Systems Security Officer (ISSO). An ISSO is the Federal employee who is responsible to the system owner, information system security manager, or other

manager for ensuring the fitting operational security posture is maintained for an information system, program or appointed IT / IA assets.

Information Type (FIPS 199, adapted). A specific category of information (for example privacy, medical proprietary, financial, investigative, classified, or sensitive security information), defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.

Integrity. The degree of assurance obtained that information has not been altered in an unauthorized manner or destroyed since its origination.

Interim Authority to Operate (IATO). Temporary authorization granted by the AO for an IT system to process, store and/or transmit information based on preliminary results of a security certification of the system. It is the DOT CIO's position that IATOs will only be granted under conditions of critical need and mission requirement.

Internet. A network of many networks that interconnect worldwide and use the Transmission Control Protocol/Internet Protocol (TCP/IP) for transmission and recovery of data and information.

Key ISS Personnel. A group of personnel who have ISS responsibilities that account for 51 percent or more of their job-related duties.

Logical Access Controls. Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.

Malware. Malware is an abbreviated term for malicious software. This generic term is used to describe any form of malicious software that is specifically designed to destroy or harm other software or networks, such as including viruses, Trojan Horses, and malicious active content.

Management Controls. The security controls (safeguards and countermeasures) applied to an information system that focuses on managing risk and ISS management. Management controls refer to those actions that are performed primarily to support management decisions about ISS.

Mission Critical. A system that processes information in which the loss, misuse, disclosure or unauthorized access would have a negative impact on the mission of the agency.

NAS Mission Critical (NAS-SR-1000, adapted). IT / IA includes those functions or services that, if lost, would prevent the NAS from exercising safe separation and control over aircraft.

National Security System (44 U.S.C., section 3542). Any information system (including any telecommunication system) used or operated by an agency, a contractor, or other organization on behalf of an agency – (i) the function, operations, or use of which: involves intelligence activities; involves cytological activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons systems; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is used for routing administrative and business applications, for example, payroll, finance logistics, and

personnel management applications); or, (ii) is protected by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Network. A network is comprised of communications hardware and software that allows one information system to connect to another information system.

Operational Controls. The security controls (safeguards and countermeasures) applied to an information system that is primarily carried out by people (as opposed to the information system).

Operational Prototype. Functional representative rendition of a system that is created late in the development cycle and is used to determine readiness of a system for full-scale deployment. The operational prototype contains real or a representative set of operational information. The operational prototype serves as the basis for demonstration, testing, and evaluation before an authorizing official granting full authority to operate.

Personal Identity Verification (PIV). Use of a common physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Physical Security. A discipline that combines security controls that bar, detect, monitor, restrict, or otherwise control access to sensitive areas. Physical security also refers to the measures for protecting a facility that houses ISS assets and its contents from damage by accident, malicious intent, fire, loss of utilities, environmental hazards, and unauthorized access. FAA Order 1600.69, FAA Facility Security Management Program, defines the physical security program.

Public Trust Position. A position that has the potential for action or inaction by an incumbent to affect the integrity, efficiency, or effectiveness of assigned government activities.

Remote Access (Adapted from NIST SP 800-53). Access by a user (or an information system) from a source that is external to an information system security perimeter.

Risk (NIST SP 800-30, adapted). The combination of a threat, its likelihood of successfully attacking a information system, and the resulting effects and harm from that successful attack.

Risk Assessment (NIST SP 800-30, adapted). The process of identifying the risks to an information system, this includes determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Risk Assessment is a segment of risk management and synonymous with the term, risk analysis.

Risk Management (NIST SP 800-30, adapted). The total process of identifying, controlling, and mitigating information system-related risk. IT / IA includes risk analysis; cost and benefit analysis; and the selection, implementation, and security evaluation of safeguards. This overall system security review considers both

effectiveness and efficiency, including impact on the business and constraints due to policies, regulations, and laws.

Rules Of Behavior or System Use. These are the rules that have been established and implemented about use of, security in, and acceptable level of risk for the information system. Rules will clearly describe responsibilities and expected behavior of all individuals with access to the information system.

Safeguards (CNSS Instruction 4009, adapted). Protective measures prescribed to meet the security requirements (for example, confidentiality, integrity, and availability) specified for an information system. This term is synonymous with security controls and countermeasures.

Security. See Information Assurance.

Security Compliance Review. Assessments at FAA facilities, which are coordinated with a authorizing official, facility management, and, if applicable, the Contracting Officer, that examine operational assurance determining whether an information system is meeting stated or implied security requirements, including information system and organizational policies.

Security Controls (FIPS 199). The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system, which taken together, adequately protect the confidentiality, integrity, and availability of the information system, its data, and information.

Security Plan (NIST SP 800-18). A formal document that gives an overview of the security requirements of the information system. IT / IA also describes the security controls in place and planning for meeting those requirements.

Security Requirement. Requirement levied on an information system based on laws, Executive orders, directives, policies, instructions, regulations, or organizational needs to ensure the confidentiality, integrity, and availability of the data and information process, stored, or transmitted.

Service Level Agreement. A written agreement between two or more entities detailing agreed on levels of service.

Site Surveys. A visit to a non-FAA facility to assess the level of implementation of the FAA ISS Program and compliance to FAA orders, policies and procedures as stated in a contract, MOU, MOA, agreement, or any internal security plans requested by the FAA. These surveys are led by AIO and coordinated with the developer, facility management, and contracting officer.

System Administrator. An individual who is responsible for: ensuring that operating systems for each information system are configured properly and the security features appropriate to the intended level of system operation are properly set; ensuring audit software is properly configured; and ensuring audit trail reports are periodically reviewed.

Technical Controls (NIST SP 800-18, adapted). The security controls (safeguards or measures) for an information system that are implemented and executed by the

information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat. Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. The result is the loss of confidentiality, integrity, or availability.

Trusted Interface (CNSS 4009). An interface that is established between two information systems under the complete control of the FAA employees.

Untrusted Interface. An interface between two information systems, one of which is not under the complete control of the Department of Transportation or the FAA.

User. An employee, contractor, subcontractor; Federal, state, and local government agencies; authorized domestic and international aviation industry partners; and authorized foreign governments having access to and use of FAA information or FAA information systems, nationally or internationally.

Vulnerability (CNNS Instruction 4009). Weakness in an information system, security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Additional definitions specific to the various areas of Information Assurance (IA) policy, standards, and guidance will be found in the supporting documents addressing those areas.

10.005 Goal(s)

The goal of the U.S. Department of Transportation (DOT) IA policy is to ensure that the Department's IT systems and infrastructure maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance between the mission criticality and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to an IT system; and, cost effectiveness.

All information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, the Department on IT systems requires some level of protection. The loss or compromise of information entrusted to Department employees or its contractors may affect the nation's economic competitive position, the environment, the national security, Department missions, or the personal privacy of United States citizens.

In addition to the aforementioned goal, it is also the intent of this policy chapter to ensure that the Department's IA policy remains in line with, and supportive of, all national policy and direction with regards to IT security.

10.006 Policy

Information resources within the Department of Transportation will be protected using appropriate controls and in accordance with existing federal laws, regulations, and guidelines. The controls applied to the protection of departmental information systems and assets fall into one of three categories:

Management/Administrative Controls: Management and administrative controls define the human factors of security. These controls involve all levels of personnel within an organization and determine which users have access to which resources and information by such means as:

- Configuration Management
- Asset Management
- Personnel Hiring and Separation of Duties
- Certification and Accreditation
- Risk Management
- Training and Awareness

Operational Controls: Operational controls are those controls that are implemented on an ongoing basis and applied to the day-to-day operation of information systems. Examples of operational controls are:

- Personnel Security
- Incident Response and Reporting
- Security Awareness Training
- Security Documentation
- Data Integrity
- System Maintenance
- Contingency Planning
- Production, Input/Output Controls
- Physical and Environmental Security

Technical Controls: Technical controls use technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network. Technical controls are far-reaching in scope and encompass such technologies as:

- Encryption
- Smart Cards
- Network Authentication
- Access Control Lists (ACLs)
- Host Integrity and Auditing
- Firewalls
- Intrusion Detection

Specific policies, standards, guidelines and procedures applicable to each of the above control categories are, or will be, detailed in the supporting documents listed in the References section of this chapter.

10.007 Responsibilities

This section describes the roles and responsibilities of the individuals involved in the decision-making activities related to the Department's IA Program. IT / IA security personnel described below must have the authority to enforce security policies and safeguards for IT systems within their purview. An individual at the OA level may hold two or more positions of responsibility, unless prohibited by Federal law, regulations or guidelines. The individual must also possess professional qualifications, including training and experience, required to carry out the functions described in this section. The OA level may establish additional roles, as needed to meet DOT's overall IA Program.

The DOT Chief Information Officer (CIO) is the senior management official responsible for the Department's overall IA program. The Department's CIO is responsible for the creation and promulgation of all applicable IA policy, guidance, compliance, implementation and oversight requirements.

The DOT Chief Information Security Officer (CISO) is the senior management official responsible for developing and maintaining the resources to ensure FISMA compliance, and verification of the Department's IA program.

The DOT Deputy Chief Information Security Officer (DCISO) is the senior management official, subordinate to the CISO, for compliance with FISMA, technical implementation and control, and the day-to-day management of the Department's IA program. The Deputy CISO will also have visibility into the Department's IA budget and resources. The Deputy CISO is responsible for cyber protection, detection, identification, and authentication, and response to all cyber incidents within the Department.

The Operating Administration (OA) CIO. The OA CIO is the agency focal point with overall responsibility to protect agency information and information systems. The OA CIO is authorized to interpret the terms of this order, resolve any conflicts with other orders, revise this order to be consistent with significant changes in Federal, Departmental, and FAA mandates, and issue detailed IA implementation orders, standards, requirements, and guidance for carrying out this order. The OA CIO must:

1. Occupy a full-time Federal Senior Executive position that must be designated as a high-risk, public trust position, at a minimum, and maintain a national security SECRET clearance;
2. Report annually on the effectiveness of the OA information security program, including progress of remedial actions;
3. Appoint, in writing to the DOT DCISO, an OA ISSO and an alternate OA ISSO;

4. Ensure that Federal information which is collected, stored, disseminated, transmitted, or disposed of by information systems owned or operated by or for the DOT, is properly protected against unauthorized access, use, modification, destruction, or denial of service through implementation and integration of management, operational, and technical controls;
5. Develop strategies to link IA performance measures to a return-on-investment and the OA's capital planning and investment strategy;
6. Develop, issue, and maintain agencywide IA policies, standards, requirements, guidelines, and procedures in support of this policy;
7. Serve as the IA liaison to DOT Inspector General, Congress, and other external organizations. The OA CIO must consolidate and develop responses to IA inquiries received from Congress, OMB, GAO, and other organizations;
8. Authorize mapping, vulnerability scanning, and penetration testing on OA information systems with advanced coordination with the system owners, information owner (if not the same as the system owner), and OA ISSMs;
9. Ensure that the agency inventory of information systems is up to date and accurate, as required by OMB Circular A-130 and DOT Order 1350.2, Chapter 10, Information Assurance;
10. Ensure compliance with all IA requirements in this order and imposed on the DOT under Federal laws, polices, standards, regulations, and guidelines;
 - Establish and manage a process for conducting IA compliance reviews in collaboration with Departmental Authorizing Officials (AO) and ISSMs;
 - Advise senior agency officials regarding appropriate procedural, contractual, technical, or programmatic actions to correct deficiencies; and
11. Ensure regular and systematic assessment of the OA IA Program through a combination of self-assessments, independent assessment and audits, formal testing and certification, network or host vulnerability or penetration testing, and OA IA program reviews.
12. Ensure all OA IA key personnel have and maintain all required OMB and NIST management, operational and technical education, training and awareness, as well as all appropriate and required certifications.

The OA Information System Security Officer (ISSO). The OA ISSO is an official responsible for ensuring the appropriate operational security posture is maintained for the

information system(s) or program(s) within a single OA, as assigned. The OA ISSO reports directly to the OA CIO. The OA ISSO is the OA's IA program lead. The OA ISSO is empowered to represent and make IA decisions at all management levels, except for accepting residual risk, that responsibility rests with the AO. The AO and OA ISSO may not be the same person. The OA CIO must designate the OA ISSO, and an alternate OA ISSO, in writing. For their respective OA or LOB, the OA ISSO or associate OA ISSO must:

1. Be a Federal employee and occupy a position that must be designated as a high-risk, public trust position, at a minimum, and maintain a minimum national security SECRET clearance;
2. Serve as the principal adviser to the OA AO, OA CIO and OA information system owners on all matters involving the security of the OA information systems, including ensuring IA policies are published, where applicable, and provide technical and security guidance for C&A process;
3. Ensure that departmental policy and guidance is adhered to, and perform oversight of OA ISSMs/system owners in the performance of their IA activities;
4. Coordinate with the management and other key IA personnel, as appropriate, on a variety of security related matters, including security engineering, security management, and security architecture;
5. Ensure that security controls specified in information system accreditations/authorizations are implemented and sustained;
6. Participate in IA compliance reviews, vulnerability, and threat assessments; advise the OA AO on changes in risk; and recommend appropriate action, including withdrawing system accreditation;
7. Ensure, in collaboration with the system owner, that the security risk of systems under his or her purview are identified and prioritized, risk assessments are completed, and risk mitigation plans developed and maintained;
8. Ensure the information system COOP, disaster recovery and contingency plans are developed, tested, and maintained for all systems and their components within the overall OA business continuity plan;
9. Coordinate, in advance, with other ISSOs when a configuration change or change in ownership impacts information systems security in one or more OAs;

10. Assist the DOT TCIRC in conducting inquiries into IA incidents. Inquiries may include contacting external groups and other organizations to better understand the threat posed by incidents, to share information about incidents, and to develop recommendations on the best course of action in dealing with incidents;
11. Serve as the OA representative to the TCIRC during the investigations of IA incidents as specified in policies and procedures;
12. Oversee implementation of the DOT IA Awareness, Education and Training Program within the OA;
13. Oversee the development, implementation, and reporting of ISS mitigation measures in response to IA alerts or bulletins or security assessment and audits;
14. Be the authoritative source with delegation authority for the management and validation of the OA IT system inventory, certification, and NIST requirements compliance; and
15. Represent their OA in the following areas:
 - a) All DOT IA committees and working groups
 - b) Development of their OA IA budget and strategic plan
 - c) Authoritative source of OA information contained in the DOT Enterprise Security Portal (ESP) and for authorizing OA personnel access to their OA information within the ESP
 - d) Identify and maintain current listing of all OA IA key personnel
 - e) Development, implementation and verification of all IA guidance, techniques, tactics and procedures for all DOT issued IA policy
 - f) Authoritative source for all OA FISMA reporting requirements.

The OA Information System Security Manager (ISSM). The OA ISSM is the OA line of business (LOB) official responsible for the overall level of oversight of procurement, development, integration, modification, operation, and maintenance of the information and information based systems for the LOB. The OA ISSM collaboratively supports the definition, design, and implementation of the overall OA IA program in conjunction with the OA ISSO. The ISSM is empowered, with coordination with the OA ISSO, to represent and make IA decisions at all management levels, except for accepting residual risk, that responsibility rests with the AO. [OAs are under no mandate to establish an OA ISSM position. If an OA ISSM is established, they will assume all the roles of the OA ISSM]. However if ISSMs are appointed the OA LOB ISSM(s) must:

1. Ensure, in collaboration with the system owner, that the security risk of systems under his or her purview are identified and prioritized, risk assessments are completed, and risk mitigation plans developed and maintained;

2. Ensure the information system COOP, disaster recovery and contingency plans are developed, tested, and maintained for all systems and their components within the overall OA business continuity plan; and
3. Assist the DOT TCIRC or their organic CIRC organization in conducting inquiries into IA incidents. Inquiries may include contacting external groups and other organizations to better understand the threat posed by incidents, to share information about incidents, and to develop recommendations on the best course of action in dealing with incidents.

The Authorizing Official (AO) (formerly known as Designated Approval Authority) assumes the responsibility for operating a system at an acceptable level of risk to agency operations, agency assets, or individuals; and is accountable for the risk associated with operating a system. In determining acceptable risk, the AO ensures the newly authorized system(s) do not compromise the security of interconnecting systems. The AO will have the authority to commit OA funding and resources to correct deficiencies and weaknesses identified for their OA systems. The AO must:

1. Occupy a full-time Federal Senior Executive position that is designated as a high-risk, public trust position, at a minimum, and maintain a national security SECRET clearance;
2. Make a formal written declaration that a system is approved to operate and connect to other systems as described in the system C&A package. The written declaration must state whether a system meets security requirements and has an acceptable level of residual risk. If the interconnection is with a system for which another AO is responsible, then both AOs must authorize the interconnection in writing. The AO may designate one of the following:
 - (a) Authorization to operate (ATO) a system;
 - (b) Interim authority to operate (IATO) a system, if unacceptable security risk(s) exist;
Temporary authorization granted by the AO for an IT system to process, store and/or transmit information based on preliminary results of a security certification of the system. It is the DOT CIO's position that IATOs will only be granted under conditions of critical need and mission requirement. All DOT IATOs must be submitted to the DOT OCIO Associate Chief Information Office for Information Technology Investment Management for submission to the DOT CIO for approval/disapproval. The goal is to achieve full authority to operate (ATO) accreditations for all DOT systems.
 - (c) Denial of authority to operate a system, including disconnection of a system;

3. Ensure all applicable Federal and DOT ISS policies, standards, regulations, and guidelines are met;
4. Conduct ISS compliance reviews for systems under the AO's control, including remediation plan and compliance follow-up reviews, based on applicable Federal laws, ISS policies, regulations, standards, and guidelines;
5. Identify and prioritize critical information systems and their components for information systems under their purview;
6. Ensure that an information system contingency plan is developed, validated, and maintained for each critical information system and their components as part of the overall OA business continuity of operation plan (COOP);
7. Ensure that independent security risk assessments, testing and evaluation of the effectiveness of security plans and requirements, and security tests and evaluations are conducted for information systems based on system criticality; and
8. Ensure compliance with applicable Federal and DOT ISS policies, standards, and activities to mitigate vulnerabilities for information systems under AO purview.

Information System Owners/Application Owners The Information Systems Owner (ISO) is a Federal manager who is responsible for planning, directing, and managing resources for an operational information system. Systems under development are owned by the developing organization until accepted and authorized by the operating organization. The ISO may function as the information steward with the statutory or operational authority to establish the necessary controls for the generation, collection, processing, dissemination, and disposal of information. Specifically, the ISO must:

1. Ensure that information, which is collected, stored, disseminated, or transmitted by information systems owned or operated for the DOT, is properly protected against unauthorized access, use, modification, destruction, or denial of service through implementation and integration of management, operational, and technical controls;
2. Ensure the requirements of this policy are applied throughout a program's life cycle for all information systems under their purview;
3. Serves as the official who is responsible for the overall procurement, development, modification, integration, operation, and maintenance of an information system. The ISO must ensure adequate resources are available to maintain the operational system or domain security posture, conduct C&A activities, and carry out risk management activities;
4. For each system the ISO owns, at least annually, or whenever there is a significant change to the system, evaluate the security controls to ensure an

acceptable level of protection of the data and documents these control, in the individual system security plan; and

5. Ensure a system administrator is designated, in writing, for each information system, program, or designated information and information system asset.

System Administrators: An individual responsible for ensuring that information systems are configured, administered, and monitored properly and security features are appropriately set to the intended level of operation. At a minimum, system administrators must perform the following duties for each information system under his or her purview:

1. Ensure audit software is properly configured and operating as intended and that audit reports are periodically reviewed;
2. Promptly respond to management requests to alter access to an account if the user is identified as having left the Department, changed assignments, changed contracts, or completed work on a grant or other agreement, or no longer requires system access;
3. In response to an ISS incident, the system administrator must take action to promptly contact the responsible OA ISSM and ISO and coordinate actions to mitigate further disruption or destruction to the system; and
4. Complete annual security awareness training and other training commensurate with their role and responsibilities.

Managers and Supervisors: Managers and supervisors must:

1. Ensure employees under their supervision attend annual security awareness training. The manager or supervisor must also ensure that annual security awareness training is monitored and documented based on Federal and DOT policies;
2. Report cyber-security incidents, including virus and malware attacks;
3. Cooperate with computer security incident response team members under procedures established by TCIRC and their respective OA;
4. Cooperate with DOT CIO representatives or other designated DOT personnel during ISS compliance reviews;
5. Ensure that all users have read, understood, and agreed to follow the rules of behavior, before authorizing access to an information system. The supervisor or manager must periodically review these documents to ensure that the privileges assigned to system users are accurate; and

6. Carry out management, operational, and technical security controls identified through ISS alerts or bulletins, as applicable, according to procedures established by their OA.

Users: A user is defined as an employee, contractor, subcontractor; Federal, state, and local government agencies; authorized domestic and international aviation industry partners; and authorized foreign governments having access to DOT information or DOT information systems. Users must:

1. Report cyber-security incidents, including virus and malware attacks, according to procedures established by DOT TCIRC and their OA;
2. Be familiar with policies, guidance, and procedures for using the data, systems, and software applications to which they have been granted access;
3. Comply with DOT and OA ISS policies, standards, and requirements;
4. Ensure that all information, regardless of sensitivity, is treated in an appropriate and secure manner; and
5. Complete annual security awareness training.