ORDER U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

1370.86

3/1/01

SUBJECT: AVR INFORMATION SYSTEMS SECURITY PROTECTION

1. **PURPOSE.** This order implements security policy defined in Order 1370.82, FAA Information Systems Security Program, and establishes minimum requirements for Information System Security (ISS) Protection to be implemented in the Regulation and Certification (AVR) line of business (LOB). The order defines acceptable practices and procedures for ensuring adequate protection of the AVR information systems.

2. **DISTRIBUTION**. This order is distributed to the division level in the Office of the Associate Administrator for Regulation and Certification, the Offices of Accident Investigation, Aviation Medicine, and Rulemaking, and to the Aircraft Certification and Flight Standards Services; to the Aircraft Certification, Flight Standards, and Aviation Medicine Divisions in the Regions; to the Medical Staff in the ARTCCs; and a limited distribution to all Aircraft Certification Field Offices and Flight Standards Field Offices.

3. **BACKGROUND.** AVR Information Systems provide mission support to the FAA National Airspace System. Federal guidance requires that these information system assets be protected against security threats. In the past, efforts to protect assets were primarily oriented towards physical security protection, user identification, and access control. While these protection measures are still required, AVR's use of new information technologies requires more sophisticated and secure methods for protecting the availability, integrity, and confidentiality of information.

Information assets in AVR consist of application systems which process regulatory, certification, aviation medical, and other data, as well as infrastructure hardware and software. To enable communication between applications and between AVR employees and contractors, AVR also maintains an automated network of telecommunications and information systems. The scope of this infrastructure ranges from desktop or laptop computers integrated into local area networks (LANs) to a wide area network (WAN) that has international connectivity to the public Internet and private FAA intranets.

4. **DEFINITIONS.** Appendix 1, Definitions and Acronyms, contains terms and acronyms used in this order.

5. **SCOPE.** This order applies to all AVR employees, contractors, subcontractors, and users of AVR information systems and assets that support the AVR mission. This order covers all information assets used or owned by AVR organizations; all AVR information stored, processed, disseminated, or transmitted using FAA information systems; all information systems funded or

Distribution: A-W(VR/AI/AM/RM/IR/FS)-2; A-X(CD/FS/AM)-2; A-YZ(AM)-2; A-FAC-0 (LTD); A-FFS-0(LTD)

Initiated by: AVR-10

managed by AVR, including prototypes, tests, experiments, or developmental systems; and all AVR or non-AVR facilities where these information systems are developed, housed, managed, or operated.

6. PRECEDENCE AND INTERPRETATION. This order is intended to complement and expand upon any FAA-wide orders dealing with addressed issues. This order has precedence over any other AVR order that may contain conflicting, incomplete, or obsolete ISS protection requirements.

7. STATUTORY, POLICY, AND REGULATORY MANDATES.

a. Computer Security Act. Public Law 100-235, The Computer Security Act of 1987, dated January 8, 1988, is the cornerstone of computer security within the Federal Government and is the basis for the development of the FAA ISS policy. Public Law 100-235 requires Federal agencies to identify sensitive systems, provide security training, and develop and implement an ISS plan for each sensitive system.

b. Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection (May 1998),* requires Federal agencies to develop and implement a comprehensive security program to protect their critical infrastructure. The FAA responded to this requirement with the publication of the FAA Critical Infrastructure Protection Plan (CIPP). The CIPP serves as the mission statement for the FAA, as it relates to ISS. PDD 63 addresses the cyber and physical infrastructure vulnerabilities of the Federal Government by requiring each department and agency to work to reduce its exposure to new and existing threats.

c. Appendix 2, Statutory and Regulatory Documents, contains additional Statutory, Policy, and Regulatory Mandate references.

8. RESPONSIBILITIES. The success of the ISS program depends on the involvement of all AVR offices that acquire, develop, operate, or replace information systems components. These offices shall comply with this Order and shall carry out responsibilities consistent with annual appropriations and as defined in Appendix 3, Roles and Responsibilities.

9. PROGRAM REQUIREMENTS. All activity in support of AVR information systems shall be performed in accordance with applicable national policies, Federal laws, DOT regulations and directives and FAA regulations and directives. This includes preparation of specifications, life cycle planning, design, development, test, operation, maintenance, and administration activities. AVR employees and contractor personnel shall adhere to all applicable information security policies and procedures during all activities associated with AVR information systems, and shall incorporate adequate security measures into information systems and into their operating and maintenance procedures. AVR information system security shall include provisions for protecting internal and external networks and interfaces from intrusion and other vulnerabilities. Establishing priorities for AVR Information System security activities shall be based on a risk assessment and risk mitigation analysis. AVR Information System Security

activities shall include personnel, equipment, data, operational and maintenance security, as well as access control, incident detection, and recovery actions.

10. IMPLEMENTATION. The critical rules for protecting AVR information systems are contained in Appendix 4 of this order, Requirements, Practices and Procedures. The AVR rules for implementation address the six fundamental areas of security: Integrity; Identification/Authentication; Confidentiality; Availability; Access Control; and Security Management/Administration.

Thomas E. McSweeny
Associate Administrator for Regulation and Certification

APPENDIX 1. DEFINITIONS AND ACRONYMS

Acceptable level of risk. A judicious and carefully considered assessment by the appropriate DAA that an information system(s) meets the minimum requirements of applicable security directives. The assessment should take into account the sensitivity and criticality of information, threats and vulnerabilities, safeguards and their effectiveness in compensating for vulnerabilities, and operational requirements.

Access Control. Limits what the user can read, write, modify, and/or delete.

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

Adequate protection. Protection that is commensurate with the risk and magnitude of the potential harm resulting from the loss, misuse, or unauthorized access to or modification of information resources. This protection includes ensuring that systems and applications used by the FAA operate effectively and provide appropriate confidentiality, integrity, availability, and accountability by using cost-effective management, personnel, operational, physical, and technical controls commensurate with an information system's sensitivity level. (OMB Circular A-130)

Assurance. Policies and procedures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This assurance includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Authentication. A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or user.

Authorization. A formal declaration by the DAA who has fiscal and operational responsibility that an information system is approved to operate in a particular security mode using a prescribed set of safeguards. This is the official management authorization for operation and is based on information provided in the Security Certification and Authorization Package (SCAP) as well as other management considerations. The authorization statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Availability. The accessibility to information or an information system on a timely basis to support mission requirements and deadlines.

AVR facility. Any facility that is owned, leased, or lent to AVR, where AVR Information Systems, or any portion of AVR Information Systems, will be developed, housed, or operated, or where AVR information is collected, stored, processed, disseminated, or transmitted using AVR or non-AVR equipment.

AVR Information System. Any Information System utilized by any service or office within the AVR line of business (See **Information System).**

Classified information system. An information system designed in accordance with Department of Defense standards to handle Confidential, Secret, or Top Secret information.

Common Criteria. A multi-part standard (ISO/IEC 15408) that defines criteria that are to be used as the basis for evaluating security properties of information technology products and systems. By establishing such a common criteria base, the results of an information technology security evaluation are meaningful to a wider audience.

Confidentiality. A requirement that private or confidential information not be disclosed to unauthorized individuals.

Contingency measures. Measures maintained for emergency response, backup operations, and post-disaster recovery for an information system, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Countermeasures. See **Safeguards.**

Critical Infrastructure Protection Plan (CIPP). The FAA's plan that defines the ISS program in accordance with the requirements of Presidential Decision Directive 63.

Critical Infrastructure Protection Remediation Plan. The annually updated plan that details how the CIPP will be executed.

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.

Designated approving authority (DAA). A senior FAA management official, appointed in writing by a member of the Management Board, who determines whether or not to authorize a system for operation or to remove that authorization.

Developer or developing organization. The organization that has primary responsibility for developing or acquiring an information system. If a contractor develops a system, the FAA organization responsible for that contract is the developing organization.

General support system. An interconnected set of information resources that share a common functionality under the same direct management control. These systems, which include software, host computers (mainframes, minis, workstations), and networks (LANs and WANs), provide support for a variety of users and applications.

Government information. Information that is created, collected, processed, disseminated, or disposed of by or for the federal government.

Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. FAA information is categorized as follows:

a. Classified information. Information that, in the interest of national security, requires protection against unauthorized disclosure as determined under Executive Order 12356, Classification of National Security Information. Such information is classified as top secret, secret, or confidential.

b. Sensitive security information. Information whose unauthorized disclosure, modification, or unavailability would harm the agency. Sensitive security information includes:

(1) Essential or critical air traffic control information and any other information that must be protected in performance of an FAA mission to ensure confidentiality, integrity, or availability of information.

(2) Information identified in Executive Order 12958, requiring protection under the provisions of the Privacy Act of 1974.

(3) Information designated "For Official Use Only" (FOUO).

(4) Information whose disclosure or modification might impact on the contractual or resource management function.

(5) Proprietary information.

(6) Information identified in the Information Technology Management Reform Act of 1996.

(7) Information falling under the auspices of the Computer Security Act of 1987.

(8) Information protected under the Sensitive Security Information rule, 14 CFR Part 191.

(9) Financial management information.

(10) Information exempt from disclosure under the Freedom of Information Act.

Information owner. For information originating within the FAA, the information owner is the manager responsible for establishing the requirements 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. The information owner retains responsibility for its security even when the information is shared with other organizations.

Information system. 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:

a. General support systems. Interconnected information resources that are under the same direct management control and share common functionality, e.g. telecommunications and networks.

b. Major application systems. Systems that require special management attention because of their importance to the agency's mission; their high-maintenance, development, or operating costs; or their significant role in dealing with the agency's programs, finances, property, or other resources.

Information system owner. See **System owner.**

Information systems security (ISS). The collected attributes that describe the security measures taken to protect information systems and the information of FAA information resources, either individually or collectively.

Information technology (IT). The hardware, software, and networks that process information, regardless of the technology involved, whether computers, telecommunications, or other.

ISS Certification. Comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the authorization process. The evaluation establishes the extent to which a particular design and implementation meets a set of specified security requirements and that risk has been mitigated commensurate with magnitude of harm.

ISS Certification agent. A senior level manager responsible for ensuring an impartial, quality control review of the SCAP, who makes recommendations to the ISS certifier and the DAA as appropriate. The certification agent signs the final ISS certification document before forwarding to the ISSM for review prior to the DAA deciding whether or not to authorize the system.

ISS Certifier (ISSC). An FAA employee in the organization that owns the information system who is responsible for certifying that system security technical controls are present and functional, management and physical controls are described and in place, and risk has been mitigated commensurate with magnitude of harm.

ISS plan (ISSP). A document that identifies the information system components; operational environment; sensitivity and risks; and detailed, cost-effective measures to protect a system or group of systems. The ISS plan must be maintained throughout the system life cycle and is complete when selected controls are tested and the responsible FAA official signs the SCAP.

Life cycle. There are two categories of life cycle:

a. **Information.** The stages through which information passes typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

b. **Information system.** The phases through which an information system passes typically characterized as initiation, development, operation, termination, and decommissioning.

Major application. An application that requires special attention to security because of the risk and magnitude of the harm that could result from the loss, misuse, or unauthorized access to, or modification of, the information in the application. Such a system might actually comprise many individual application programs and hardware, software, and telecommunications components.

Management Board. The Management Board is chaired by the FAA Administrator. The Management Board's membership is the Deputy Administrator, Assistant and Associate Administrators, and the Chief Counsel.

Mission support system. Systems that are regulatory support.

Mutual recognition arrangement (MRA). An agreement between two or more entities to accept Common Criteria certifications and validations completed by the other members of the arrangement

Network. Communications hardware and software that allow one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area networks (LANs), or wide area networks (WANs), and public networks such as the Internet.

Non-critical system. Any information system that is not a critical system.

Non-FAA facility. Any facility that is not owned or leased by the FAA where FAA information systems, or any portion of FAA information systems, will be developed, housed, or operated or where FAA information is collected, stored, processed, or transmitted. It is not necessary that the equipment used is owned by the FAA, only operated on behalf of or connected to FAA information systems.

Operational controls or operations. The day-to-day administrative, physical, technical, and procedural mechanisms used to protect operational systems and applications.

Penetration testing. The portions of security testing in which the evaluators attempt to circumvent the security features of a system.

Personnel security program. This program provides a basis for security determinations for sensitive positions, clearances for access to classified material, and suitability for Federal employment. The authority for this program is the same as that for the investigations program. Order 1600.1, Personnel Security Program, provides internal guidance.

Physical security. The combination of 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. Order 1600.69, FAA Facility Security Management Program, defines the physical security program.

Protection profile. A combination of security requirements, including assurance and functional requirements, with the associated rationale and target environment to meet identified security needs. A protection profile is included in the SCAP.

Protection profile certification. Certification issued by an accredited Common Criteria evaluation facility that the protection profile contains requirements that are justifiably included to counter stated threats and meet realistic security objectives, internally consistent and coherent, and technically sound.

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.

Risk. The combination of a threat, its likelihood of successfully attacking a system, and the resulting effects and harm from that successful attack.

Risk acceptance. Process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the sensitivity and criticality of the information protected.

Safeguards. The protective measures for an information system, whether technical, physical, or personnel.

Security Certification and Authorization Package (SCAP). The package that is presented to the DAA for final authorization of the system. The SCAP includes the ISS plan, vulnerability assessment report, risk assessment, security test plan and security test results, disaster recovery and contingency measures, and ISS certification and authorization statements.

Security compliance review. Assessments at FAA facilities, which are coordinated with a DAA, facility management, and, if applicable, the Contracting Officer, that examine operational assurance as to whether a system is meeting stated or implied security requirements, including system and organizational policies.

Security Target. A set of security functional and assurance requirements and specifications to be used as the basis for evaluation of an identified product or system in response to a chosen protection profile.

Sensitive security information. See **Information**.

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, or 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. An assembly of computer hardware, software, or firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, or controlling information with a minimum of human interventions.

System owner. The manager responsible for the organization that sets policy, direction, and controls funding for an information system. Systems under development are owned by the developing organization until accepted and authorized by the operating organization.

Threat. An activity, whether deliberate or unintentional, with the potential for causing harm to an information system or processing activity.

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

Vulnerability. A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to an information system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow an information system or activity to be harmed by an attack.

ACRONYMS

AVR	Associate Administrator for Regulation and Certification
CFR	Code of Federal Regulations
CM	Configuration Management
CSIRC	Computer Security Incident Response Capability
COTS	Commercial Off-the-Shelf
DAA	Designated Approval Authority
DOD	Department of Defense
DOT	Department of Transportation
FAA	Federal Aviation Administration
GOTS	Government Off-the-Shelf
I&A	Identification and Authorization
IPT	Integrated Product Team
IS	Information System
ISS	Information Systems Security
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
LAN	Local Area Network
MAN	Metropolitan Area Network
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PC	Personal Computer
PDD	Presidential Decision Directive
SCAP	Security Certification and Authorization Package
ST&E	Security Test and Evaluation
WAN	Wide Area Network

APPENDIX 2. STATUTORY AND REGULATORY DOCUMENTS

14 CFR 191.1 (Protection of Sensitive Security Information – Applicability and Definitions), March 21, 1997

DITSCAP 5100.40 (DoD Information Technology Security Certification and Accreditation Process)

DOT H 1350.251, Appendix G (DOT Network Security Guide)

NIST Special Publication 800-12, An Introduction to Computer Security, NIST Handbook

NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems

NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems

OMB Circular A-130, Management of Federal Information Resources

Order 1370.82, Information System Security Program

Order 1600.1D, Personnel Security Program

Order 1600.2D, Safeguarding Control and Procedures for Classified National Security Information and Sensitive Unclassified Information, Appendix 10

Order 1600.6D, Facility Security Policy

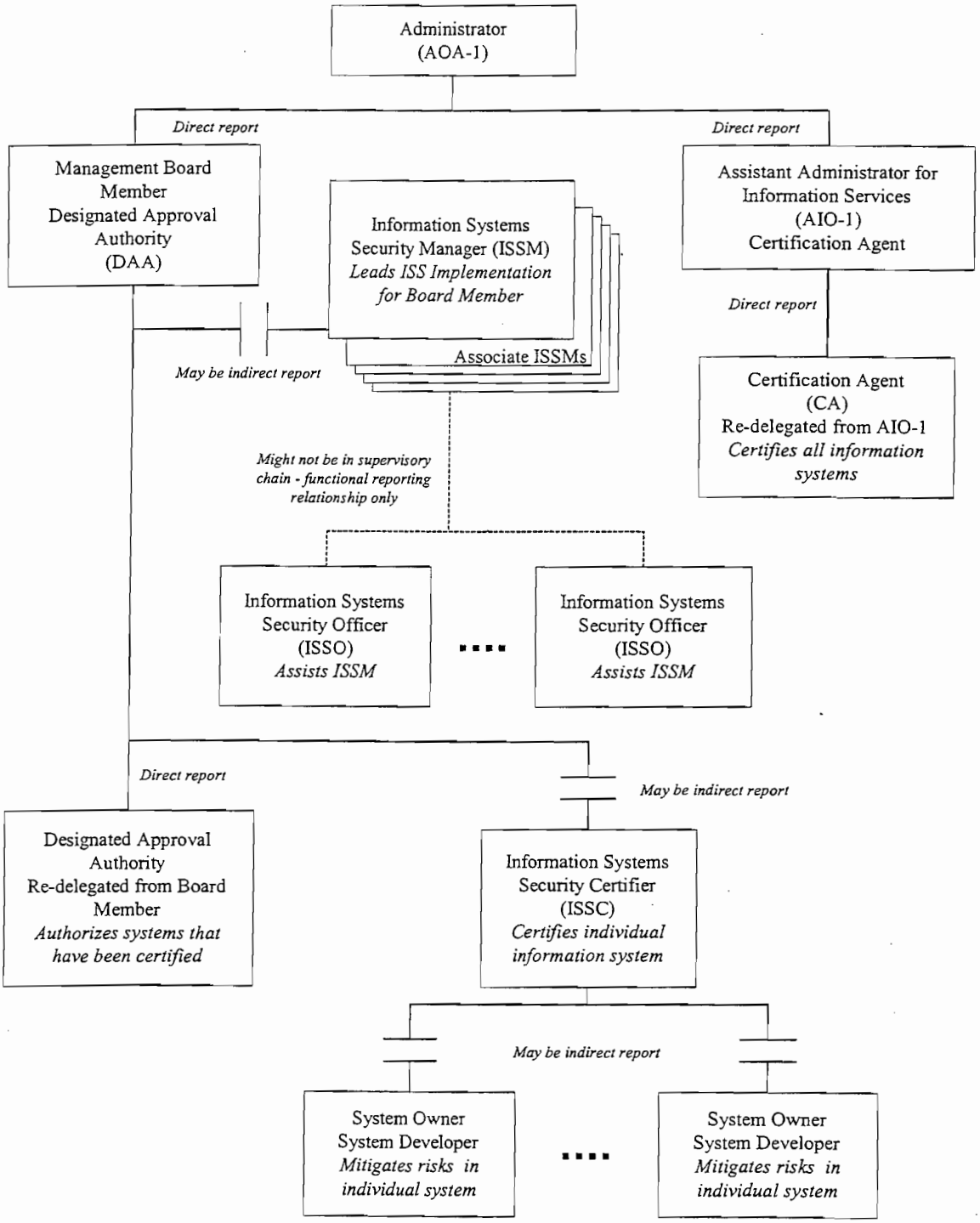
Order 1600.66, Telecommunications and Information Systems Security Policy

PDD 63, Critical Infrastructure Protection

Note: This list is not exhaustive. Various statues, regulations, and directives not listed here (e.g., Administrative Procedures Act, Trade Secrets Act, Privacy Act and Executive orders) may be applicable.

APPENDIX 3. ROLES AND RESPONSIBILITIES

This chart depicts the operational reporting relationship between key FAA ISS functions.



The section below further specifies the described roles with respect to AVR.

The roles and responsibilities are in an evolutionary state and may be modified as conditions and requirements change. Two of the roles below do not describe a specific existing position, but define the ISS duties for personnel who have assigned field and application program ISS responsibilities. The two roles are labeled as the Facility Information Systems Security Officer (ISSO) Role and the Application Program ISSO Role.

1. The AVR DAA shall:

a. Be the Associate Administrator for Regulation and Certification (AVR-1) or shall be designated in writing by AVR-1.

b. Determine whether or not to authorize for operation or continue operation for any information system owned by the line of business or staff office. Such authorization will be based on information provided in the SCAP and shall mean that the DAA has determined that the risks associated with the operation of the system have been reduced to an acceptable level. The DAA makes a formal declaration that an information system is approved to operate in a particular security mode using a prescribed set of safeguards. The authorization statement affixes security responsibility with the DAA and shows that due care has been taken for security.

c. Perform all other duties of the line of business DAA as defined in Order 1370.82.

2. The AVR ISSM shall:

a. Implement the AVR LOB ISS program within the AVR line of business. This position shall be empowered to represent and make decisions relating to ISS for the LOB organization at all management levels, both external and internal to AVR.

b. Implement ISS mitigation safeguards identified through ISS alerts or bulletins, as applicable.

c. Ensure that ISS safeguards and procedures specified in the information system authorization are implemented and sustained.

d. Lead the Associate ISSMs and ISSOs in their performance of ISS activities.

e. Ensure that adequate operational, contingency, emergency, and incident response plans are in place and being executed.

f. Review the SCAP for each certified information system and advise the AVR DAA whether or not to authorize the system.

g. Participate in ISS compliance reviews and threat assessments and advise the DAA on changes in risk and recommend appropriate action, including withdrawing system authorization.

h. Perform all other duties of the line of business ISSM as defined in 1370.82.

3. AVR Associate ISSMs will:

a. Be assigned to represent a part of the AVR Line of Business. AVR Associate ISSMs will implement the AVR ISS program within their part of AVR. This individual shall be empowered to represent and make decisions relating to ISS for the part of the AVR organization that they represent.

b. Implement ISS mitigation safeguards identified through ISS alerts or bulletins, as applicable.

c. Ensure that ISS safeguards and procedures specified in the information system authorization are implemented and sustained.

d. Lead the ISSOs in their performance of ISS activities.

e. Ensure that adequate operational, contingency, emergency, and incident response plans are in place and being executed.

f. Perform all other duties of the Associate ISSM as defined in 1370.82.

4. AVR Information System Security Certifiers (ISSCs) shall:

a. Appoint the team responsible for development of the SCAP and shall be accountable for the development, content, and quality of that SCAP.

b. Certify 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.

c. Sign the final ISS certification together with the Certification Agent and forward it to the AVR ISSM for review prior to the AVR DAA deciding whether or not to authorize the system.

d. The AVR ISS Certifier or Certifiers shall be designated in writing by AVR-1.

e. Perform all other duties of the Information System Security Certifiers as defined in Order 1370.82.

5. AVR ISSOs.

a. Facility/Local ISSO Roles and Responsibilities

(1) Coordinate installation, modification or replacement of any AVR System hardware or software component and any configuration change that affects AVR System security.

(2) Coordinate changes to functions or parameters on AVR System firewalls, routers and remote interfaces, in coordination with the site support facility.

(3) Monitor AVR System information security configuration and user access process to ensure secure operation of the system.

(4) Coordinate site-specific, security-related issues between AVR System sites and established interfaces to non-AVR systems and sites.

(5) Communicate the site's information security policy and procedures to its AVR System users.

(6) Verify that user accounts are deleted when notified of withdrawal of AVR System users.

(7) Manage local security incident assessment and response.

(8) Coordinate incidents and security changes with the facility manager, computer specialist, and the ISSC.

(9) Assume coordination responsibility for information security with physical site security accreditation (including site-specific risk assessment) with coordination of the facility manager and the ISSC.

(10) Provide oversight and facilitate the enforcement of information system security directives, orders, standards, plans, and procedures.

(11) Provide appropriate labeling guidance to AVR System personnel for documents or files that identify or describe AVR System critical security functions or parameters.

(12) Coordinate within the guidelines of Order 1600.2D the release of confidential or sensitive security AVR System documents and files to specific AVR System users or to non-AVR System personnel.

(13) Coordinate with appropriate investigation authorities and provide requested media, printouts or written records of security incidents.

b. Application Program ISSO Roles and Responsibilities

(1) Monitor AVR System information security configuration and user access process to ensure secure operation of the system.

(2) Communicate the system's information security policy and procedures to its AVR System users.

(3) Coordinate within the guidelines of Order 1600.2D the release of confidential or sensitive security AVR System documents and files to specific AVR System users or to non-AVR System personnel.

(4) Coordinate with those required to ensure that access to information system resources is terminated when an AVR employee or contractor no longer needs such access.

(5) Coordinate incidents and security changes with the appropriate Associate ISSM/ISSO and the ISSC.

(6) Provide oversight and facilitate enforcement of security directives, orders, standards, plans, and procedures for affected application systems.

(7) Provide appropriate labeling guidance to AVR System personnel for documents or files that identify or describe AVR System critical security functions or parameters.

(8) Coordinate with appropriate investigation authorities and provide requested media, printouts, or written records of security incidents.

6. AVR Managers, Supervisors, Employees, and Contractors shall:

a. Comply with this order and apply its principles to daily work activities.

b. Be accountable for protection of confidential or sensitive security information under their control in accordance with this order.

c. Annually review ISS awareness information.

d. Report ISS incidents, including virus and malicious code attacks, according to procedures established by the AVR line of business. This should include reporting to AIS, ENET, CSIRC and other parties outside AVR that need this information.

e. Cooperate with computer security incident response team members.

f. Implement ISS mitigation safeguards identified through ISS alerts or bulletins, as applicable.

g. Cooperate with AIO and AVR ISS representatives during conduct of security compliance reviews at AVR facilities and site surveys at non-FAA facilities.

APPENDIX 4. REQUIREMENTS, PRACTICES AND PROCEDURES

1. AVR Information System security requirements that have been developed to ensure the safe and secure operation of AVR Information Systems can be grouped into six fundamental areas:

a. Integrity

b. Identification and Authentication

c. Confidentiality

d. Availability

e. Access Control

f. Security Management and Administration

Requirements specific to each of these areas are detailed below.

2. Integrity

a. Integrity verification shall be used to ensure that unauthorized modification of AVR Information System software/data is detected.

b. Integrity checking of the following types of software and data shall be accomplished for:

(1) new or modified software or data

(2) transmitted or shipped software or data

(3) stored software or data (i.e. backups)

c. AVR Information System operational sites shall perform integrity checking of software and data on a periodic basis using the AVR Information System approved integrity checking procedures.

d. Failure of integrity checks may be handled as a computer security incident.

3. Identification and Authentication

a. A separate and unique-user identifier and password will be assigned to each AVR Information System user.

b. Accounts named "Administrator" by the software vendor should effectively be renamed by taking privileges away from the built in "Administrator" accounts, and creating administrative accounts of a different name with full administrative privileges for use.

c. Use of identifiers/passwords such as "default" or "guest" are prohibited.

d. Each AVR information system user identifier shall have an associated password.

e. Electronic recording or transmission of passwords "in the clear" is prohibited. Writing down of passwords is strongly discouraged. Passwords that are written down must be secure. Passwords shall not be accessible to anyone except their owner.

f. When maintenance requires disclosure of a user's password, the owner of the disclosed password shall change the password as soon as the maintenance is completed.

g. Passwords shall be a minimum of eight characters in length, shall not be a word in the standard Webster English language dictionary, shall not be a name, place, or calendar date and must contain three of the following four types of characters: lower-case alpha, upper-case alpha, numeric or symbols created by <SHIFT> numeric key within the password string. For example, the phrase "My Birthday is right after July 4!" could become "MbiraJ4!" This method conforms to Microsoft "complex password" constraints and permits implementing passfilt.dll by enabling "Passwords must meet complexity requirements" setting in the Local Security Policy software.

h. All AVR Information System passwords shall be configured to expire after a specified period of time. The maximum expiration period shall be 90 days. Shorter periods may be specified on a site basis depending on sensitivity, criticality, threat, and operational issues. The minimum password age should be set to two (2) days and the Password Uniqueness option should be set to at least four (4) in order to create a sufficiently long password history list.

i. Whenever accessing the WAN/LAN/MAN, system identification and authentication (I&A) functions shall be enabled on all workstations.

j. Programmable function keys and automatic logins shall not be used for user account access. All users shall manually enter individual login name identifiers and associated passwords. When automated processes require resource account access, these automated login scenarios must be reviewed and approved by the ISSM. Such approval shall be for a fixed period not to exceed twelve (12) months.

k. When required by applications, or changes in policy, additional authentication technologies will be applied as authorized by the AVR ISSM.

4. Confidentiality

a. Confidential or sensitive security AVR Information System data, programs, configuration files and integrity check sums shall be protected from unauthorized or inadvertent disclosure at all times, including during transmission or while stored on mobile systems.

b. Encryption keys (if employed) shall be protected from deliberate or inadvertent disclosure. Clear text transmission of symmetric or private encryption keys is prohibited.

c. Network scanning, monitoring or capturing data or messages not intended specifically for the receiver from any component of the AVR Information System network shall be prohibited except as authorized in writing to specific individuals in the performance of official duties.

d. User tokens, names, passwords, and access control items shall not be shared among users.

5. **Availability**

a. All AVR facilities/systems shall have backup procedures in place to guarantee the availability of the system data. Program owners shall determine currency of backup data, but in every case, systems shall make new backups at least every 30 days.

b. Full system backups shall be stored in a manner that provides sufficient protection based upon the sensitivity of the system data with access restricted to authorized personnel.

c. AVR Information System sites shall verify their ability to fully restore their site capabilities from both incremental and full backups.

d. External systems shall not be connected to AVR Information System without successful completion of a security assessment of the interface, mitigation of the identified risks to an acceptable level and completion of an interface control document as authorized by the DAA.

e. Virus protection shall be used on all PC-based and other systems supporting AVR Information Systems.

f. AVR employees and contractors shall exercise caution and due diligence in their actions with respect to received floppies, email attachments, web downloads and other possible avenues for the introduction of malicious code into AVR information systems.

g. AVR Information Systems shall employ mechanisms or procedures to identify suspected intrusion attempts.

h. The source, version, characteristics, authenticity and authorization to install new or replacement software, data files or parameters for any AVR Information System shall be verified through reliable security procedures and communications mechanisms prior to installation.

i. All components of the AVR Information System shall be maintained at the current security patch revision unless such a patch would adversely affect the proper operation of the AVR Information System.

6. **Access Control**

a. Users shall be granted the minimum privilege and physical access necessary to accomplish their assigned responsibilities.

b. A remote workstation shall be automatically, logically disconnected after a pre-determined number (not to exceed 3) of failed attempts to identify and authenticate.

c. A remote workstation shall be automatically logged off after any 20-minute period of non-activity.

d. Access to AVR Information System equipment and information shall be audited for unauthorized or inappropriate use on a regular basis and when special circumstances dictate.

e. AVR Information System network routers, servers, modems, firewalls and other vital equipment shall be in a secured area with limited accessibility.

f. AVR Information System equipment used outside of any AVR Information System site (e.g., laptop computers) shall be in the possession of an authorized individual or, when not in use, be secured.

g. Making a connection of any AVR Information System communications line or system component with a non-AVR Information System communications line or component (including authorized diagnosis and maintenance equipment) without prior DAA approval is prohibited. Such action may constitute a major change in the risk profile for AVR networks.

h. Interfaces with non-AVR Information System equipment must conform to the connection configuration and constraints approved by AVR access control constraints.

i. Identification of unauthorized connections to any AVR Information System shall be handled as a computer security incident.

j. The source of external data shall be validated upon entry into the AVR Information System.

k. All AVR Information System interfaces shall be implemented on a "default deny" basis in which all protocols, ports, services, etc. shall be disabled unless specifically authorized.

l. Remote or dial-in operators shall be identified and authenticated prior to performing any function. Additional identification and authentication (I&A) controls for external dial-in authentication will require a challenge-response or electronic token-based system in addition to password constraints in section 5.0. Access shall require something you have in combination with something you know.

m. Access to system and component audit logs shall be controlled and generally restricted to security personnel or system administrators.

n. Filtering rules or other technical mechanisms shall be in place on dial-up ports to ensure against dial-in being used to gain unauthorized access from the Internet or other external network. Mechanism should not allow packets from

a source address other than the address assigned to the specific system dialing in and engaged in the computer session.

o. Dial in access configurations shall not allow dial-in to dial-out and dial-in to insecure and uncertified FAA-provided Internet Access Points.

p. All AVR Information Systems will show warning Banners upon initial access that correspond to Order 1370.79 or alternatives acceptable to the ISSM.

q. All AVR firewalls shall conform to minimum FAA firewall functional requirements as defined by the FAA Configuration Control Committee established in FAA Order 1370.83 and/or by the "FAA-wide firewall team" sponsored by the AIS organization. Guidelines defined by those groups shall followed for filtering rules, network address translation, auditing requirement and other technical or procedural requirements. This will include the denial of packet services that allow external entities to gather topology, naming, addressing or configuration information.

7. Security Management and Administration

a. Where required by regulation, AVR Information System users shall receive background checks to determine suitability for access commensurate with their potential impact to operations per instructions in O.M.B. Standard Form 85 and 86 and according to the requirements in Order 1600.72, Order 1600.73, Order 1600.1D or the latest versions thereof.

b. All AVR Information System users shall receive security awareness information or training at least once per year. At that time users will be required to review "Rules of Behavior" which describe the security responsibilities and expectations of all AVR users, and to sign forms accepting responsibility for and holding individuals accountable for their actions.

c. Users shall be trained as defined in the FAA ISS Training Program such that people will know what actions to take with respect to AVR Information System operations and information whenever an incident is declared.

d. AVR Information System sites shall be staffed with sufficient knowledgeable personnel that have the necessary authorization and capability to perform the defined security requirements to ensure the continued operation of the site.

e. Account administrators shall remove, within 24 hours after notification, specific user account access for all affected systems after being notified of the reassignment, departure, retirement or dismissal of the specific system user. Notification to account managers should be given at least 24 hours prior to user departure in order to allow adequate time to administer the user account. Account administrators must deny account access no later than departure, earlier if appropriate. All accounts shall be reviewed on an annual basis and re-certification of users performed as appropriate. Access shall always be approved based on the user's need-to-know.

f. Users authorized for highly privileged functions shall utilize a specific account created for that purpose, rather than assuming broader system capabilities than needed for the function such as becoming an 'administrator', 'supervisor', 'admin', 'super-user' ('su') or assuming 'root' identity.

g. Assignment of 'administrator', 'supervisor', 'admin', 'root' or 'su' privileges to any AVR Information System user must be approved in writing by the appropriate authorized ISSO for the site, or AISSM/ISSM as appropriate.

h. Software must be properly licensed or officially approved by configuration management or ISSO functions of AVR before software can be loaded and/or stored on AVR Information System equipment. All employees using AVR Information System equipment shall comply with software licensing agreements and/or contracts.

i. Only data relating to AVR Information System operations or support shall reside on AVR Information System equipment.

j. System logging that is enabled or activated during system installation or upgrade shall not be disabled without coordinating with the appropriate Information Security (ISSO/ISSM) authorization authority.

k. All AVR Information System sites shall create, maintain and practice security event and disaster response and follow recovery plans (contingency plans) which address the operation's continuation, shutdown and/or service resumption of AVR Information System as appropriate for the event.

l. In the event of a suspected AVR Information System security breach, the affected user shall create and maintain a written record and notify the local system administrator/security specialist of the suspected breach and subsequent response, including the time/date/location where the breach and response actions occurred. The local system administrator/security officer shall determine if the "event" is a false alarm or if it is a reportable incident. A reportable incident must be documented and reported to the servicing Associate ISSM for follow-up actions. Actions may include investigating, monitoring, closing or recovering from a security breach.

m. Documents or files that identify or describe AVR Information System critical security functions or parameters (sensitive security information) shall be labeled as such with language provided by the ISSC.

n. Only an AVR Information System ISS Coordinator or ISS Officer may, in conjunction of the Privacy Officer, authorize the release of confidential or sensitive security AVR Information System documents and files to specific AVR Information System users or to non-AVR Information System personnel.

o. Recipients of AVR Information System data shall protect confidential or sensitive security documents or files against unauthorized disclosure or distribution.

p. Any electronic media containing confidential and sensitive security data, including AVR Information System recorded data, must be completely erased or destroyed before disposal. This data must be overwritten or degaussed so that it cannot easily be retrieved from this media.

q. Personnel who are required to operate and maintain AVR Information System operational software shall be trained to provide service in the event of system failures.

r. The computer system shall audit security-related events. Specific AVR Information System technical audit policy shall be documented including minimum audit configuration and frequency that audit logs are checked.