ORDER

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

1600.66

ASE-100 copies:1

LIBRARY

7/27/94

SUBJ: TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY POLICY

1. PURPOSE. This order establishes Federal Aviation Administration (FAA) policy and assigns responsibilities for ensuring the physical and technical security, information integrity and reliability, and the survivability of FAA owned and leased telecommunications and information systems, and for the protection of the assets comprising those systems/networks.

2. DISTRIBUTION. This order is distributed to the division level in Washington, regions, centers, and overseas area offices with a limited distribution to all field offices and facilities.

3. BACKGROUND. Under the Federal Aviation Act of 1958, the FAA's primary mission is to serve the Nation by providing a safe, secure, and efficient aviation system which contributes to the national security and the promotion of United States aviation. To accomplish its mission, the FAA provides support to the National Airspace System (NAS) through proprietary and leased information and telecommunications systems and networks that include air traffic control, surveillance, air navigation, communications, and other administrative facilities and services. Within these systems/networks the efficient transmission of essential FAA air traffic control information, data, and other agency communications depends upon a variety of different media including leased and public switched network telephone lines, radio frequency transceivers, twisted pair, fiber optic, coaxial cable transmission circuits, and microwave and satellite links. The FAA's national security mission includes providing command and control telecommunications systems and capabilities necessary to direct the operations and reconstruction of the NAS in support of the FAA/Department of Transportation/Department of Defense mission. Safeguards are required throughout the life cycle of FAA telecommunications and information systems to ensure their integrity, confidentiality, and survivability against a variety of threats. Depending on the type of system or services affected, specific threats or combinations of threats could result in interruption, corruption, or compromise of air traffic control and other agency telecommunications and information systems, and the disruption of FAA's capabilities to support the NAS as well as the national security.

4. DEFINITIONS. Explanations of the key terms used in this order are contained in Appendix 1, Glossary. An explanation of representative threat categories is contained in Appendix 2, Threats to Information.

5. SCOPE. Executive Orders, National Security Directives, National Security Decision Directives, Public Laws (P.L.), and Federal directives and regulations prescribe the National Security and Emergency Preparedness and communications security requirements to be implemented for safeguarding and control of telecommunications and information systems. The Computer Security Act of 1987, P.L. 100-235, specifically requires the institution of minimum acceptable security practices for computer systems/networks processing sensitive and Privacy Act information without limiting the scope of security measures already planned. Appendix 3, References, contains a listing of pertinent

curity directives. The requirements established in these national policies as implemented by this ler apply to:

a. All air traffic control and agency telecommunications and information systems equipment, ilities, and services within the FAA or contracted for by the FAA.

b. All FAA service organizations, program offices, employee, and contractor personnel who are olved with the design, planning, approval, life-cycle development, acquisition, operation, budgeting, management of FAA air traffic control and/or agency telecommunications and/or information stems.

POLICY. In accordance with applicable national policies, Federal laws, regulations, and DOT ectives, those FAA employees and contractor personnel who are responsible for the design, velopment, specification, and life-cycle planning for FAA telecommunications and information stems shall ensure that appropriate national policies, Public Laws, Federal regulations, and DOT d FAA telecommunications and information system security policies and procedures are applied ntinuously in the design, planning, development, acquisition, operation, and maintenance of these stems/networks throughout their life cycles. Specific threats to be addressed shall include but not limited to those listed in Appendix 2, Threats to Information.

RESPONSIBILITIES.

a. The Office of the Assistant Administrator for Civil Aviation Security, ACS-1, on behalf of the ministrator is responsible for:

(1) Providing overall assurance of compliance with the requirements of this order agencywide ough monitoring and oversight.

(2) Ensuring that telecommunications and information systems that handle national security ssified information or unclassified national security-related information are designed, acquired, erated, maintained, and safeguarded in accordance with national security policies and procedures ecified in this order.

(3) Coordinating with Systems Maintenance Service (ASM-1) and the Assistant Administrator Information Technology (AIT-1) in the development and implementation of procedures to provide ersight and monitoring of telecommunications and information systems processing sensitive, prietary, or Privacy Act information to ensure that the information and data are safeguarded in ordance with national policies and Public Laws.

b. The Office of the Assistant Administrator for Information Technology, AIT-1, is responsible for:

(1) Implementing the provisions of this order within its areas of responsibility to ensure that cycle security planning is incorporated into the planning, development, acquisition, operation, and ntenance of Federal information processing (FIP) resources to include telecommunications and rmation systems agencywide.

(2) Developing and planning in coordination with ACS-1 and ASM-1 telecommunications and rmation system security policies and procedures for the security and safeguarding of sensitive, prietary, and Privacy Act information. Ensuring the implementation of those procedures within its a of responsibility agencywide.

(3) Ensuring that information systems and resources processing sensitive, proprietary, and Privacy Act information are protected from end-to-end, consistent with requirements of national policy, Public Laws, applicable Federal regulations, and the magnitude of loss or potential harm which may occur from transmitted information loss, inaccuracy, alteration, unavailability, disclosure, or misuse.

(4) Developing and implementing appropriate telecommunications and information system security awareness education, training, and monitoring programs for sensitive, proprietary, and Privacy Act information and data.

(5) Developing, in coordination with ASM-1 and ACS-1, appropriate mechanisms for the conduct of reliable and continuing assessments of threats and vulnerabilities to FAA telecommunications and information systems processing sensitive, proprietary, and Privacy Act information, and for communicating the results of those assessments and the relevant actions required to the appropriate level of management.

c. The Director, Systems Maintenance Service, ASM-1, is responsible for:

(1) Implementing the provisions of this order.

(2) Providing management and operations policy guidance for all FAA air traffic control and agency telecommunications networks.

(3) Providing for the operational availability of services according to the criticality of those services, and ensuring that contingency and disaster recovery plans to maintain this level of service availability are provided.

(4) In coordination with ACS-1 and AIT-1, ensuring that telecommunications services and resources are protected from end-to-end consistent with the magnitude of the loss or potential harm which may occur from transmitted information loss, inaccuracy, alteration, unavailability, disclosure, or misuse.

d. Directors of FAA Offices and Services, are responsible for:

(1) Ensuring that the design, planning, and implementation of telecommunications and information systems within their respective office or service areas is accomplished in accordance with national and agency telecommunications and information system security policies and directives, and with the provisions of this order.

(2) Coordinating telecommunications and information system life-cycle security planning and operations within and between their office and service areas.

(3) Coordinating service telecommunications and information system security development, planning, and implementation with ACS-1, ASM-1, and AIT-1, beginning with the system life cycle and continuing throughout the operational life of the system.

(4) Ensuring that the provisions of this order are fully addressed in office and service lementing directives and guidelines which affect the design, security, development, acquisition, lementation, operation, and maintenance of telecommunications and information systems.

David Hinson

id R. Hinson
ninistrator

Appendix 1. Glossary

Agency telecommunications are all FAA telecommunications which are not air traffic control as defined herein. Examples include applications such as switched voice telephone services, voice and video conferencing systems/networks, and data transmission networks which support administrative computer-to-computer interfaces. Networks which provide primarily agency telecommunications include the FTS2000 telecommunications systems and the administrative data transmission network (ADTN).

Air traffic control telecommunications are associated with the processing of air traffic, including national security commitments. Included are: services and related equipment which provide air traffic control voice or data communications for en route, terminal, flight service, weather, and other air traffic control use to include all telecommunications used at air traffic control and air navigation facilities to perform the primary assigned facility functions, and all telecommunications services that require access into the air traffic control system. Air traffic control telecommunications also encompass those telecommunications services necessary to support national emergency operations.

COMSEC means communications security systems/networks, services, and concepts that constitute protective measures taken to deny unauthorized persons information derived from telecommunicaitons of the U.S. Government related to national security and to ensure the authenticity of such communications.

Federal information processing (FIP) resources means automatic data processing (ADPE) equipment as defined in Public Law 99-500(40 U.S.C. 759(a)(2)), and in the Federal Information Resource Management Regulation (FIRMR), Amendment 1, dated October 1990. (***Note: The acronym ADPE is used instead of the current term "AIS" to be consistent with the wording of the FIRMR.***)

Information systems security (INFOSEC) means a composite of factors necessary to protect FIP systems and the information they process to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats and to ensure authenticity. This protection results from the application of security measures; including cryptosecurity, transmission security, emission security, and computer security; to systems/networks that generate, store, process, transfer, or communicate information of use to an

adversary, and also includes the physical protection of sensitive material and systems.

National security and emergency preparedness (NSEP) means those physical, technical, and administrative characteristics of telecommunications and information processing systems that will ensure a prescribed level of survivability in times of national or other emergencies up to and including nuclear attack. Government common-use telecommunications systems/networks are designed, built, tested, and maintained to meet the defined emergency mission needs of the entities that use them.

National security systems/networks include telecommunications and information systems operated by the United States Government, contractors, or agents that contain national security-classified information or, as set forth in 10 United States Code (U.S.C.) Section 2315, that involve intelligence activities, cryptologic activities related to national security that involve command and control of military forces, or that involve equipment that is an integral part of a weapon or weapon system or involve equipment that is critical to the direct fulfillment of military or intelligence missions.

Sensitive information as defined in Section 3(d)(4), Public Law 100-235, The Computer Security Act of 1987, is: Any information which if subject to unauthorized access, modification, loss, or misuse could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (***Note: P.L. 100-235 does not address classified national security information and sensitive unclassified national security-related information.***)

Telecommunications facilities includes equipment used for such modes of transmission as telephone, telegraph, teletypewriter, and such corollary items as distribution systems/networks and communications security facilities.

Telecommunications services include, without limitation, the transmission, emission, or reception of signals, signs, writing, sounds, or intelligence of any nature by wire, fiber optic cable, radio, visual, or other electrical, electromagnetic, or acoustically coupled means.

Appendix 2. Threats to Information

Threats to the integrity, confidentiality, and survivability of FAA telecommunications and information systems may consist of one or multiple threat actions in succession. Examples of threats which must be considered include the following:

1. Common Threat Agents

a. People within the organization. This includes individuals who intentionally or unintentionally violate the integrity of the system.

b. People outside the organization. Hackers, hostile intelligence agents, industrial espionage agents, terrorists, and ex-employees.

c. Inanimate agents. This includes such things as routine water damage, power surges and failures, physical calamities, hardware failure within the information technology (IT) product, malfunctioning external devices and systems, and disabled external devices and systems.

2. INAPPROPRIATE DISCLOSURE THREATS (Confidentiality Violations)

a. Passive observation.

(1) Exposure.
(2) Scavenging.
(3) Eavesdropping.
(4) Wiretapping.
(5) Traffic analysis.
(6) Analysis of information technology (IT) product emanations. (Spurious emanations.)
(7) Other forms of signals intelligence.

b. Hardware attacks.

(1) Theft of physical media.
(2) Physical trespass and observation.
(3) Implanting eavesdropping devices.
(4) Disarming controls (e.g., via routine maintenance).

c. Masquerade.

(1) Individuals that impersonate (e.g., via password guessing).

(2) Processes that impersonate (e.g., Trojan horses).

d. Misuse of authority.

(1) Deliberate disclosure.
(2) Misuse of administrative privilege.

(a) Modification of access control attributes.
(b) Editing of password files.

(3) Exploiting inference and aggregation vulnerabilities. (e.g., reverse engineering).
(4) Exploiting product vulnerabilities.

(a) Exploiting covert channels.
(b) Inadequate authentication.
(c) Trap doors that bypass system checks.
(d) Improper initialization or recovery.
(e) Faulty reuse of objects or devices.
(f) Inadequate argument validation.
(g) Miscellaneous logic errors.
(h) Hardware flaws.

e. Browsing, searching for exploitable patterns.

f. Willful neglect and other errors of omission. An example would be failing to log out when leaving a workstation.

g. Preparation for misuse.

(1) Code-breaking efforts.
(2) Off-line password guessing.
(3) Autodialer scanning.
(4) Creating, planting, and arming malicious software.

3. FAULT-AND-ERROR THREATS (Integrity Violations)

a. Hardware attacks.

(1) Implanting malicious hardware.
(2) Disarming hardware controls.
(3) Malfunctioning hardware (via aging, routine maintenance).

b. Masquerade.

(1) Individuals that impersonate (e.g., via password guessing).
(2) Processes that impersonate (e.g., Trojan horses).
(3) Deception of users and operators.

c. Deception of users and operators.

d. Misuse of authority.

(1) Deliberate falsification via data entry or modification.
(2) Repudiation (falsely denying origin or receipt of information).
(3) Misuse of administrative privilege.
(4) Modification of access control attributes.
(5) Editing of password files.
(6) Exploiting inference and aggregation vulnerabilities (e.g., reverse engineering).
(7) Deliberate compounding of small errors.
(8) Exploiting product vulnerabilities.

(a) Exploiting covert channels.
(b) Inadequate authentication.
(c) Trap doors that bypass system checks.
(d) Improper initialization or recovery.
(e) Faulty reuse of objects or devices.
(f) Inadequate argument validation.
(g) Miscellaneous logic errors.
(h) Hardware flaws.

(9) Willful neglect and other errors of omission. For example, failing to log out when leaving a workstation.
(10) Preparation for misuse.

(a) Code-breaking efforts.
(b) Off-line password guessing.
(c) Autodialer scanning.
(d) Creating, planting, and arming malicious software.

e. Lack of adequate competence.

(1) Accidental falsification via data entry or modification.
(2) Installing flawed application software.

(3) Misapplication of software.

(a) Application to wrong data.
(b) Miscommunication of inputs.
(c) Improper runtime environment.

4. LOSS OF SERVICE THREATS.

a. Inherent system inadequacies.

(1) Inadequate deadlock avoidance.
(2) Inadequate response to transient errors.

b. Hardware threats.

(1) Deliberate hardware modification.
(2) Disabling critical components.
(3) Shutting off system or power supply.
(4) Implanting self-destruct devices.

c. Inadvertent hardware modification.

(1) Normal aging.
(2) Routine maintenance.
(3) Accidental damage (e.g., water damage).

d. Interference (e.g., electronic jamming).

e. Usage threats.

(1) Deliberate denial of service.
(2) Misuse of administrative privilege.

(a) Modification of access control attributes.
(b) Editing of password files.

(3) Exploiting product vulnerabilities.

(a) Exploiting covert channels.
(b) Inadequate authentication.
(c) Trap doors that bypass system checks.
(d) Improper initialization or recovery.

(e) Faulty reuse of objects or devices.
(f) Inadequate argument validation.
(g) Miscellaneous logic errors.
(h) Hardware flaws.

(4) Excessive usage via masquerading. This includes individuals that impersonate (e.g., password guessing), as well as processes that impersonate (e.g., Trojan horses).

(5) Creating, planting, and arming malicious software.
(6) Willful neglect and other errors of omission.
(7) Failure to order necessary supplies.
(8) Failure to perform routine maintenance.
(9) Administrative actions.

(a) System shutdown.
(b) Disabling user accounts.

(10) Incorrect setting of security attributes.
(11) Accidental deletion of critical data.
(12) Overload.

(a) Normal excess usage.
(b) Runaway programs.
(c) Personal use of organization computers.

Appendix 3. References

1. Executive Order (E.O.) 12333, United States Intelligence Activities.

2. E.O. 12472, Assignment of National Security Emergency Preparedness Telecommunications Functions.

3. E.O. 12656, Assignment of Emergency Preparedness Responsibilities.

4. National Security Directive (NSD-42), National Policy for the Security of National Security Telecommunications and Information Systems, dated July 1990.

5. NSD-97, National Security Telecommunications Policy, dated June 1983.

6. National Security Decision Directive (NSDD-145), National Policy on Telecommunications and Automated Information Systems Security, dated September 17, 1984.

7. Director of Counterintelligence Directive (DCID) 1/16, Security Policy for Uniform Protection of Intelligence Processed in AIS's and Networks.

8. National Telecommunications and Information Systems Security Policy (NTISSP) 200, National Policy on Controlled Access Protection.

9. Office of Management and Budget (OMB) Bulletin 88-16, Agency Security Plans.

10. OMB Bulletin Number 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information, dated July 9, 1990.

11. OMB Circular A-123, Internal Control Systems, dated August 4, 1986.

12. OMB Circular A-127, Financial Management System.

13. Federal Information Resource Management Regulation (FIRMR), to include 41 CFR Subpart 201-21-3.

14. Public Law (P.L.) 93-579, The Privacy Act of 1974.

15. P.L. 97-255, The Federal Manager's Financial Integrity Act (FMFIA).

16. P.L. 98-473, Comprehensive Crime Control Act of 1984--Computer Security.

17. P.L. 99-474, Computer Fraud and Abuse Act.

18. P.L. 99-508, Interception or Disclosure of Wire, Oral, or Electronic Communications.

19. P.L. 100-618, Voice Privacy Protection Act of 1988.

20. FAA Order 1600.2, National Security Information. (Latest version)

21. FAA Order 1600.6C, Physical Security Management Program.

22. FAA Order 1600.8, Communications Security (COMSEC). (Latest version)

23. FAA Order 1600.54, FAA Automated Information Systems Security Handbook. (Latest version)

24. FAA Order 6000.32, Security Requirements for Remote Access of NAS Facilities, dated February 3, 1986.