Table of contents

11 System security

Note: In 2000, the FAA came out with FAA Order 1370.82. This order cancelled FAA Order 1600.54B, Automated Information Systems Security Handbook. FAA Order 1600.54B is cited frequently throughout this chapter. The information in this chapter will be revised at a future time to reflect the cancellation of FAA Order 1600.54B.

This chapter pertains to the human factors aspects of security safeguard features for new (or modified) facilities, systems, and equipment that are to be acquired and maintained by the FAA. Human factors considerations can enhance the security effectiveness and suitability of new or upgraded systems.

> **Definition. Security safeguards** are the protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to: operational procedures, physical security, or hardware and software features.

The FAA Order 1600.54, FAA Automated Information Systems Security Handbook, and associated directives explain security safeguards associated with communication security, necessary provisions for classified information, and security safeguards such as Tempest requirements.

> **Discussion.** From a system analysis viewpoint, "security safeguards" need to be thought of as a subsystem of any new operational system. The human component of any operational system or subsystem, as well as the security component need to be considered and technically integrated from the concept phase throughout the procurement and implementation phase.

The FAA modernization program increasingly relies on automated processing systems. New computer technologies make it possible for remote users to access large databases through communication networks. Telecommunications systems and Automated Information Systems (AIS) boundaries are becoming vague and are highly susceptible to interception, unauthorized access, exploitation, and hostile threats.

11.1 General design practice

This section defines the **security architecture** of the NAS and provides human factors rules for risk analysis, interface considerations, certification and accreditation activities, and security test and evaluation. Other general rules for system security are also addressed.

- 11.1.1 **Accreditation and certification.** The accreditation and certification of FAA AIS shall conform to FAA Order 1600.54. Human factors rules of this section are to be complied with before accreditation and certification are given. [Source: Department of Transportation (FAA Order 1600.54B), 1989]

  Definitions. Accreditation is the authorization and approval granted to an AIS or network to process sensitive data in an operational environment. **Certification** is the technical evaluation that supports the accreditation process and establishes the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements. [Source: FAA Order 1600.54B, 1989]

- 11.1.2 **Security test and evaluation.** Test and evaluation activities shall be conducted by the contractor to verify that equipment, software, and facility designs meet the security and associated human factors requirements. [Source: Department of Defense (MIL-STD-46855B), 1979]

11.2 Physical security and access control

Physical security addresses the application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources (for example, automated assets, facilities, telephone lines, or information). Good physical access control takes into account threats to a protected area due to vandalism, theft, modification, or destruction. This section gives rules for regulating the physical access to FAA AIS, the facilities that house those systems, and other FAA assets.

The physical security provided to a facility and AIS is based upon the alternative protection measures derived from security risk and requirements analyses. Provisions for protection are to be built into systems, subsystems, facilities, and equipment work areas in accordance with the selected protection features and the security policies applicable to the NAS environment.

Physical security and access control requirements can be found in FAA Orders 1600.54B and 1600.6C.

□ 11.2.1 **Automatic access control.** When appropriate, automated safeguards should be used to control and monitor access to facilities and automated systems. These safeguards may include access control systems such as smart cards or other authentication technologies described in Section 11.3. [Source: National Research Council (NRC), 1990]

■ 11.2.2 **Access control log.** Automatic control systems shall be capable of providing, in hard copy and machine-readable format (for later analysis), the date, time, location, and user identity of each valid and invalid entry attempt, and the reason for denial of access for each invalid entry attempt. [Source: NRC, 1990]

11.3 Identification and authentication

The *FAA Automated Information Systems Security Handbook,* FAA Order 1600.54, requires that all FAA automated systems have and use a software user identification and authentication capability.

Definitions. Identification is the process that enables the security safeguards to recognize a user name (usually through a machine-readable name) as an identical match to a name previously listed in an authorized user file. **Authentication** is the act of identifying and confirming the eligibility of a station, originator, or user to access specific categories of information. Authentication is a measure designed to provide protection against fraudulent entry or transmissions by establishing the validity of a transmission, message, station, or originator. **Authorization** is granting, to a user or user group, the right of access to a program, a process, or information.

11.3.1 General

■ 11.3.1.1 **Task simplicity.** System designers and integrators shall ensure that the identification and authentication tasks for authorized users are straightforward, simple, and consistent with the protection levels of the information to be processed in the system. [Source: Smith & Mosier (ESD-TR-86-278), 1986]

■ 11.3.1.2 **Log on process.** The log on process associated with the security subsystem shall be completed before a user is able to select any operational options. [Source: ESD-TR-86-278, 1986]

■ 11.3.1.3 **Log on prompts.** A log on process shall provide prompts for all user entries, passwords, and other data required to confirm user identity. A log on prompt shall be provided automatically upon terminal or system initialization without other user actions. [Source: ESD-TR-86-278, 1986]

□ **11.3.1.4 Log on delay.** If a user tries to log on to a system and the log on attempt is denied because of system unavailability, an advisory message should be displayed to tell the user what the system status is and when the system will become available.
[Source: ESD-TR-86-278, 1986]

□ **11.3.1.5 Unsuccessful log on attempts.** The security safeguards should not allow more than three log on attempts. This implementation provides a margin for user error while continuing to protect the system from persistent attempts at illegitimate access. Unsuccessful attempts beyond the third should initiate an alarm for the system administrator or at the terminal or both.
[Source: ESD-TR-86-278, 1986]

■ **11.3.1.6 Access protection.** The following security measures shall be taken to ensure that security and safety will not be compromised by unauthorized access to an unattended workstation or console.
[Source: ESD-TR-86-278, 1986]

a. An individual's single log-on password shall permit all access and data entry capabilities, from any workstation, that the individual has been authorized. The authorized individual is then responsible to protect his or her password and workstation in accordance with appropriate system and work area security policy.

b. If an individual has authorization for access to sensitive information or for entry of critical data, then that individual's use of his or her password on any authorized workstation shall enable appropriate access.

> **Discussion.** As an option, a pre-programmed protection of the sensitive information (such as a screen saver or "read only" mode) could automatically engage after an appropriate period of workstation disuse. The period would be established by policy and administered by the system and network administrators. After the established period, the system shall default to the pre-programmed protection that excludes all sensitive information and disables data entry capabilities until an authorized individual re-enters his or her password to again validate his or her authentication. The re-entry of a password will be prompted. Upon password authentication the system would continue the previous operation.

The attempted user shall be notified that the terminal is in a locked-out mode for security reasons, if the authentication is not successful (see Paragraph 11.3.1.7).

Discussion. If the system security policy permits an authorized user to continue after the delay, then a correct identification and authentication would be permissible upon prompting. If the new authentication is successful, the system would then prompt the new user with an option to continue at the previous operation or to select another applicable operational mode.

c. The user shall be able to engage this protected "read only" or screen save mode by an input command without waiting for the delay period. Thus, the authorized individual user is always responsible to ensure that his or her workstation is in a protected mode at any time, however brief, when he or she vacates a workstation where sensitive or critical information is accessible.

d. These same security measures and processes shall apply to any remote or network capabilities that can allow access to sensitive or critical information.

e. If the protection required by a., b., c., and d. is not provided for a workstation where critical or sensitive information is processed, then that workstation area shall be physically secured or guarded so that sensitive or critical information cannot be accessed by unauthorized personnel. Information classification levels and their respective physical requirements are detailed in FAA Order 1600.2 and 1600.54, Chapter 5). [Source: ESD-TR-86-278, 1986]

- 11.3.1.7 **Continuous recognition of user identity.** If a user has been identified and authenticated, data access and change privileges that are authorized for that user shall continue throughout a work session. [Source: ESD-TR-86-278, 1986]

11.3.2 Passwords

The composition, length, source, storage, and ownership of passwords used in FAA AIS are governed by FIPS PUB 112, *Standard for Password Usage*. Password protection mechanisms and management responsibility are to conform to FAA Order 1600.54. [Source: FAA Order 1600.54B, 1989; Department of Defense (CSC-STD-002-85), 1985]

Discussion. Security safeguard designers need to realize that random alphanumeric strings are equivalent to nonsense syllables which are very difficult for humans to memorize or retain, especially if they have five or more characters. Though mnemonic techniques can assist learning, computer-generated passwords will contribute to human memory and input errors. [Source: FAA Order 1600.54B, 1989; CSC-STD-002-85, 1985]

□ 11.3.2.1 **Changing passwords.** Users should be permitted to change their passwords consistent with the sensitivity or security level of the information being accessed. [Source: ESD-TR-86-278, 1986; CSC-STD-002-85, 1985]

> **Discussion.** This capability allows users to adapt unique passwords that will minimize erroneous entries. Such a self-chosen capability allows users to make a change when compromise is suspected. [Source: ESD-TR-86-278, 1986; CSC-STD-002-85, 1985]

□ 11.3.2.2 **Password protection.** Training should be given to users to ensure that common passwords (such as "me", "password", and "ABC") or commonly known user data (such as addresses, names spelled backwards ("ydnA"), and user birth dates) are not used. Self-chosen passwords should be protected by security safeguards. [Source: Department of Defense (MIL-HDBK-761A), 1989]

■ 11.3.2.3 **Recording of date and time of log on.** After a user logs on, the system shall automatically record the date and time of the log on. [Source: CSC-STD-002-85, 1985]

11.4 Auditing

■ 11.4.1 **Auditing users or security levels.** Security safeguards shall enable the system administrator to selectively audit the actions of any specific user or users based on individual identity or security level. [Source: Department of Defense (DOD 5200.28-STD), 1983]

11.5 Information and data protection

11.5.1 General

This section gives rules for the protection of classified data, automated transaction logs, and the transmission of messages.

■ 11.5.1.1 **Automated security measures.** Automated security safeguards shall be provided to protect data security and system integrity to the extent possible. [Source: ESD-TR-86-278, 1986]

> **Discussion.** The goal of data protection is to minimize data loss resulting from potentially destructive failures, user errors, and unauthorized access. Even careful, conscientious users will sometimes make mistakes, and the user interface needs to mitigate the consequences of those mistakes. [Source: ESD-TR-86-278, 1986]

■ **11.5.1.2 Integrity of data.** Security safeguards shall minimize the risk of unauthorized modifications of data files or system control data. [Source: System Specification for Communication System Segment, 1986]

■ **11.5.1.3 Warning of threats to security.** Messages or alarm signals shall be provided to warn users and system administrators of potential threats to data security. The number of false alarms shall not negate the effectiveness of the alarms. [Source: ESD-TR-86-278, 1986]

■ **11.5.1.4 "Read-only" status.** A "read-only" status indication shall be provided to users not authorized to change displayed data. Authorization for "read-only" data may require logging onto the system when the information warrants such protection (such as classified data). [Source: MIL-HDBK-761A, 1989;ESD-TR-86-278, 1986]

■ **11.5.1.5 Degraded system warning.** The system shall generate an alarm when performance of components has degraded beyond established thresholds. [Source: System Specification for Communication System Segment, 1986]

11.5.2 Classified data protection

Classified data must to be processed only in approved, secure areas as defined in FAA Order 1600.54. A computer room that has approval to process classified information is to be designed as a "closed area," in accordance with FAA Order 1600.2C.[Source: FAA Order 1600.54B, 1989]

■ **11.5.2.1 Encrypting messages.** If it is necessary to transmit classified or sensitive data over insecure communication channels, automatic encryption shall be provided. This encryption shall be transparent to the user. All requirements for communication security (COMSEC) and the use of cryptographic systems with the FAA are defined in FAA Order 1600.8C. [Source: ESD-TR-86-278, 1986; MIL-HDBK-761A, 1989]

11.5.3 Automated transaction logs

□ **11.5.3.1 Automatic recording of data access.** If logs of data access are needed, security safeguards should keep those records automatically. Users should not be responsible for critical record keeping actions. [Source: ESD-TR-86-278, 1986; MIL-HDBK-761A, 1989]

□ **11.5.3.2 Informing users of automated record keeping.** Users should be informed concerning the nature and purpose of automated recording of individual actions. [Source: MIL-HDBK-761A, 1989]

Discussion. This may be accomplished by various methods such as a security briefing or a message at the time of log on. [Source: MIL-HDBK-761A, 1989]

11.5.4 Transmission of messages

■ **11.5.4.1 Automatic protection of transmitted data.** Automated measures shall be provided to protect data during transmission (for example, encryption) until the data have been received. [Source: ESD-TR-86-278, 1986]

■ **11.5.4.2 Reviewing messages.** Users shall be provided a means of reviewing outgoing messages and their security provisions (for example, its security classification) before transmission. [Source: MIL-HDBK-761A, 1989]

□ **11.5.4.3 Confirmation codes.** If a user must confirm the identity of a message source, computer aids such as computer-generated confirmation codes should be provided. [Source: MIL-HDBK-761A, 1989]

11.6 Documentation of security safeguards

This section gives rules for documentation of the security safeguards, their interactions with other systems, the AIS facilities, and the protection of these documents.

■ **11.6.1 User documentation.** The user documentation shall provide rules for security safeguard use, a description of how security safeguards interact with each other, and a description of the protective mechanisms they employ in order to facilitate maintenance of the security system. [Source: FAA Order 1600.54B, 1989]

■ **11.6.2 Design documentation.** Documentation providing a description of the manufacturer's human-security safeguards interface shall be available for non-developmental items and commercial-off-the-shelf equipment. If the security safeguards are composed of distinct modules, the interfaces between these modules shall also be described. [Source: FAA Order 1600.54B, 1989]

Glossary

Accreditation - The authorization and approval granted to an AIS or network to process sensitive data in an operational environment.

Authentication - The act of identifying and confirming the eligibility of a station, originator, or user to access specific categories of information. Authentication is a measure designed to provide protection against fraudulent entry or transmissions by establishing the validity of a transmission, message, station, or originator.

Authorization - Granting to a user or user group, the right of access to a program, a process, or information.

Certification - The technical evaluation that supports the accreditation process and establishes the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements.

Identification - The process that enables the security safeguards to recognize a user name (usually through a machine-readable name) as an identical match to a name previously listed in an authorized user file.

Security architecture - A subset of the overall system architecture that protects the automated system, telecommunication, physical, and informational assets through denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction.

Security safeguards - The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to: operational procedures, physical security, or hardware and software features.

References

Department of Defense. (1979). *Human engineering requirements for military systems, equipment, and facilities* (MIL-STD-46855B). Philadelphia, PA: Navy Publishing and Printing Office.

Department of Defense. (1983). *Trusted computer system evaluation criteria* (DOD-5200.28-STD). Philadelphia, PA: Navy Publishing and Printing Office.

Department of Defense. (1985). *Department of Defense password management guideline* (CSC-STD-002-85). Philadelphia, PA: Navy Publishing and Printing Office.

Department of Defense. (1989). *Human engineering guidelines for management information systems* (MIL-HDBK-761A). Philadelphia, PA: Navy Publishing and Printing Office.

Department of Transportation. (1989). *FAA automated information systems security handbook* (FAA Order 1600.54B). Springfield, VA: National Technical Information Service.

National Research Council, System Security Study Committee. (1990). *Computers at risk: Safe computing in the information age*. Washington, DC: National Academy Press.

Smith, S.L., & Mosier, J.N. (1986). *Guidelines for designing user interface software* (ESD-TR-86-278). Hanscom AFB, MA: Electronic Systems Division.

System Specification for Communication System Segment. (1986). Springfield, VA: National Technical Information Service.

Index