U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
National Policy

ORDER 1370.92A

Effective Date:
08/06/10

SUBJ: Password and PIN Management Policy

1. Purpose of This Order. This Order establishes the Federal Aviation Administration's (FAA) Policy for passwords and Personal Identification Numbers (PIN) management as authentication tools used to access FAA information and information systems resources. This Order assigns the roles and responsibilities for managing access to and safeguarding FAA information and information systems.

2. Whom This Order Affects. This Order applies to anyone who is responsible for or has authorized access to the FAA information systems including Sensitive Unclassified Information (SUI), Sensitive Security Information (SSI), and Personally Identifiable Information (PII). This does not include systems that process or store classified information. This Order applies to all FAA employees, contractor personnel, FAA Lines of Business and Staff Offices (LOBs/SOs), Authorizing Officials (AO), Information System Security Manager (ISSM), and others. Others include grantees, consultants, licensees, and any person or entity, domestic or foreign, having a formal written agreement with the FAA.

3. Where Can I Find This Order? This Order can be found on the FAA's Intranet website at the following URL: https://employees.faa.gov/tools_resources/orders_notices/.

4. Cancellation. This order replaces FAA Order 1370.92, Password and PIN Management, dated June 28, 2004.

5. Background. A password or PIN is vulnerable to compromise whenever it is used improperly, transmitted from one location to another unencrypted, or stored unprotected. Weak passwords and PINs create opportunities for malicious users and programs to gain unauthorized access to a system or network. This Order provides the minimum security requirements to reduce password and PIN vulnerabilities and provides information to help users and organizations manage passwords and PINs.

6. Scope. This Order defines security requirements for passwords and PINs used to access FAA systems; (e.g., Government Furnished Equipment (GFE) such as: computers, BlackBerry devices, cellular devices) or other electronic devices used for FAA business.

7. Password and PIN Management Policy. This order provides security requirements and procedures for creating, changing, managing or storing passwords and PINs in accordance with statutory law Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev 3 "Recommended Security Controls for Federal Information Systems and Organizations" to comply with

identification, authentication, access controls and auditing security controls. FAA employees using a password or PIN as authentication tools to access FAA information and information systems resources must make a commitment to protect this information. Below are the minimum security requirements that must be met:

a. Passwords or PINs are required for all FAA GFE (e.g., computers, BlackBerry devices, cellular devices);

b. PINs must contain at least four (4) numbers and do not need to expire;

c. Passwords and PINs must not be shared. Some systems may require group passwords, such as legacy systems. In these cases, if the system is not capable of complying with these instructions then a waiver must be requested per the instructions in paragraph 11a of this order;

d. Immediately change a password or PIN when compromised. Follow your LOB/SO incident reporting procedures when a password or PIN is compromised;

e. All electronically stored passwords and PINs must be protected by using FAA-approved hardware or software tools that are FIPS 140-2 compliant, in accordance with FAA Order 1370.103, Encryption Policy:

FAA-approved hardware and software are resources that have been purchased through the FAA acquisition process (e.g., Blanket Purchase Agreement (BPA) the Strategic Sourcing for the Acquisition of Various Equipment and Supplies (SAVES) contract) or an FAA-approved product listed on the Federal GSA Schedule.

f. All stored operational and organizational passwords and PINs that are not electronically stored and protected must be physically protected in a secured location such as a locked file cabinet, safe, or office. Stored passwords and PINs must be marked “For Official Use Only” (FOUO), in accordance with FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI);

g. Accounts must be set to automatically lockout after three (3) failed attempts of entering an incorrect password or PIN with a lockout time set to 20 minutes minimum;

h. Passwords must be at least eight (8) characters in length, containing at least one upper case letter, one lower case letter, one number, and one special character (e.g. !, @, #, %, etc.);

i. Passwords less than 13 characters in length must be changed every 90 days;

j. Passwords 13 or more characters in length that are random, non-sequential characters do not need to expire. Passwords with 13 or more characters are equivalent to an 84-bit key. Current research estimates that cracking a password of this length and complexity would take over 1,100 years. Such passwords never need to be changed unless they have been compromised, or as directed by each LOB/SO CIO;

k. Passwords must not be reused within the first 10 password changes per LOB/SO organizational standards;

l. All factory-set passwords must be changed before the application or system is operational;

m. Machine-to-machine or service account passwords consisting of 13 or more characters do not need to expire and never need to be changed unless compromised;

n. All default operating system, user, developer generated and application passwords must be changed before the application or system is operational;

o. The Personal Identity Verification (PIV) card can be used instead of the user identification and password process. Using the PIV card along with digital credential enabled validation systems provide stronger security measures, multifactor authentication, and reduces employee's password usage; and,

p. PIV cards and security tokens must not be left unattended. Follow your LOB/SO incident reporting procedures when a PIV card or security token is lost or stolen.

8. Roles and Responsibilities. All FAA organizations must comply with the roles and responsibilities in accordance with FAA Order 1370.82A, FAA Information Systems Security Program, and carry out additional responsibilities as follows:

a. The Federal Aviation Administration Chief Information Officer (CIO) must:

(1) Provide agency-wide information systems security leadership, ISS policy, guidance, and oversight of the FAA Passwords and PIN Management Policy; and

(2) Ensure that information owned or maintained by the FAA is protected against unauthorized access, use, modification or destruction, using Agency-administered security controls.

b. The Chief Information Security Officer (CISO) must:

(1) Oversee the implementation of this order and ensure compliance with the Federal Information Security Management Act (FISMA), all FAA, Department of Transportation (DOT) system security policies, standards, requirements and guidelines; and

(2) Conduct regular ISS compliance reviews to ensure the LOBs/SOs have implemented a FAA Password and PIN Management Process.

c. The Information Systems Owner (ISO) must:

(1) Require implementation of the security controls and requirements to protect stored passwords (e.g., encrypt files, restrict access to password files and store one-way cryptographic hashes) used by the LOB/SOs and identified in NIST 800-53 Rev 3;

(2) Set a timeframe for password expiration and session lockout in accordance with this policy for their systems and applications; and,

(3) Set passwords to at least eight (8) characters, containing at least one upper case letter, one lower case letter, one number, and one special character in accordance with this policy.

d. The Information Systems Security Manager (ISSM) must:

(1) Ensure the implementation of security controls and requirements to protect stored passwords (e.g., encrypt files, restrict access to password files, and store one-way cryptographic hashes);

(2) Ensure a timeframe for password expiration and session lockout in accordance with this policy for their systems and applications based on criticality and sensitivity;

(3) Coordinate security incidents with the Cyber Security Management Center (CSMC) regarding compromised passwords and PINs; and,

(4) Coordinate the use of multifactor authentication with the PIV card along with digital credential enabled validation systems with the LOB/SO CIO.

e. The System and Network Administrators must:

(1) Use identified security controls and requirements as prescribed in NIST SP 800-53 Rev 3, Recommended Security Controls for Federal Information Systems and Organizations to protect stored passwords including;

(2) Set controls to prevent users from creating a new password string similar to any of the last 10 passwords;

(3) Set the number of failed logon attempts;

(4) Monitor audit logs for excessive failed logon attempts;

(5) Use encryption to send reset passwords to users;

(6) When using PIV cards set systems to display unattended card alerts;

(7) Use password strength validation tools to ensure password compliance;

(8) Implement the timeframe for password expiration and session lockout for systems, operating systems, and applications based on criticality and sensitivity;

(9) Report all suspicious activity associated with passwords and PINs to the appropriate management personnel; and,

(10) Change all factory-set or default operating system, user, developer generated and application passwords must be changed before the application or system goes operational.

f. The FAA Users must:

(1) Create passwords that are at least eight (8) characters in length, containing at least one upper case letter, one lower case letter, one number, and one special character (e.g.,!, @, #, %, etc.);

(2) Protect passwords and PINs from inadvertent disclosure;

(3) Physically protect employee PIV cards and security tokens; and,

(4) Report all suspicious activity associated with passwords and PINs following their LOB/SO incident reporting procedures.

9. Statutory Policy and Regulatory Mandates.

a. The E-Government Act, Public Law 107-347, signed into law by the President in December 2002, established the Federal Information Security Management Act (FISMA). The FISMA states that each Federal department and agency must maintain an information security program that is consistent with policies, standards, requirements, and guidance issued by the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and other designated Federal agencies.

b. The Homeland Security Presidential Directive 12 (HSPD 12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 16, 2004, requires the FAA to implement a policy for establishing a common identification standard for Federal employees and contractors. The HSPD 12 requires the FAA to use a personal identification verification (PIV) card for logical access to the FAA information systems.

c. The OMB Circular A-130, Appendix III, Management of Federal Information Resources, states that Federal departments and agencies must implement policies, standards, requirements, and procedures that are consistent with standards and guidance issued by the NIST.

d. The OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005, provides the implementation instructions for HSPD 12.

e. The OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006, states that Federal departments and agencies must appropriately safeguard sensitive personally identifiable information and train employees of their responsibilities in this area.

f. FAA Order 1370.82A, Information Systems Security Program addresses contractor compliance with agency-wide ISS policies, standards and requirements when authorized by FAA contract.

g. FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI) addresses guidance for identifying and protecting sensitive unclassified information.

10. References. References are contained in Appendix A of this order.

11. Definitions. Definitions of specialized terms used in this subject area, with relevant abbreviations and acronyms, are contained in Appendix B of this Order. All information systems security definitions used in this Order are stated in the FAA Order 1370.82A, Information Systems Security Program, Appendix A.

12. Notice of Exception or Noncompliance.

a. The head of a LOB/SO, ISO, or authorizing official can request the FAA Chief Information Officer (CIO) to grant a waiver of compliance based on a compelling business reason. The request must include: (1) justification, (2) what measures or compensating controls already exist, (3) risk acceptance, (4) risk mitigation measures, (5) waiver period, and (6) milestones to achieve compliance. The system's Authorization Package must include the copy of the request and waiver decision. Waivers to this policy are provided for users accessing operational air traffic control displays, equipment, monitoring and control devices (DSR, CARTS, STARS, etc.), and legacy information technology (IT) systems that cannot meet the requirements specified in this order.

b. Penalties for user noncompliance with this Order are subject to actions in accordance with existing policy and regulations, applicable union contracts and/or Human Resource Policy Management (HRPM) Employee Relations 4.1, Standards of Conduct, and the accompanying Human Resources Operating Instructions Table of Penalties or if applicable, Federal Aviation Personnel Manual (FAPM) 2635. These penalties include written reprimands, suspension of system privileges, temporary suspension from duty, and removal from current position or termination of employment. The FAA will enforce the use of penalties against any user who violates the FAA or Federal system security policy or order as appropriate.

13. Administrative Information.

a. The Assistant Administrator for Information Services and the Chief Information Officer (AIO-1) can issue changes to the FAA Information Systems Security Program. The AIO CIO's office approves changes that set policy, delegate authority, and assign responsibility.

b. Each LOB/SO may develop additional guidance and procedures to ensure compliance with this Order. To address individual business, operational, or security needs, FAA organizations are encouraged to implement more stringent security requirements than those stated in this Order, but the requirements of this Order must not be reduced.

14. Distribution. This Order is distributed to divisions in headquarters, regions, and centers with information systems or information systems security responsibility. Headquarters, regions, and centers must send this Order to all field offices and facilities within 30 days.

David M. Bowen
Assistant Administrator for Information Services
and Chief Information Officer

Appendix A. References

a. FIPS 181, Automated Password Generator, October 1993.

b. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

c. FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006.

d. NIST-SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001.

e. NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.

f. NIST SP 800-63, Electronic Authentication Guide, April 2006. Being updated

g. NIST SP 800-118, Guide to Enterprise Password Management, April 2009. Draft – keep watch

h. Department of Transportation Handbook DOT H 1350.260, Guide to Protecting Information Technology.

i. FAA Order 1370.82A, Information Systems Security Program, September 11, 2006.

j. FAA Order 1370.105, Logical Access Control Policy, December 10, 2008.

k. FAA Order 1370.107, Rules of Behavior/System Use Policy, June 04, 2009.

l. FAA Order 1370.110, Encryption Policy, December 14, 2008.

m. FAA 1600.75, Protecting Sensitive Unclassified Information (SUI), February 1, 2005.

Appendix B. Definitions

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Bit Size: A bit is the basic unit of information in computing and telecommunications; it is the amount of information that can be stored by a digital device or other physical system that can normally exist in only two distinct states. In cryptography, key size or key length is the size measured in bits of the key used in a cryptographic algorithm (such as a cipher).

FAA-approved: Provides a written list of products, devices, virtual private networks (VPNs), standards, software, or hardware that have been pre-approved by the FAA Administrator, an Assistant Administrator, a LOB/SO senior executive or a designated Authorizing Official, the IT Executive Board (ITEB), the CIO Council, and the Joint Resource Council (JRC). The FAA-approved lists are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. An FAA-approved list recommends quality products that satisfy the FAA or the LOB/SO needs with measurable improvements to its mission capability and operational support. FAA-approved hardware and software are resources that have been purchased through the FAA acquisition process, Dell Blanket Purchase Agreement, or an FAA-approved vendor and/or are listed on the Federal GSA Schedule.

FIPS 140-2, Security Requirements for Cryptographic Modules: This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

Government Furnished Equipment (GFE): Property acquired by the government and provided to Federal employees and contractor support personnel.

Multifactor Authentication: Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric.

Operating System: A set of services for the applications running on computers and provides the fundamental user interface for your computer.

Personal Identification Number (PIN): A password that is relatively short (usually 4 to 6 characters) and consists of only numbers.

Personal Identity Verification (PIV): Personal Identity Verification (PIV) is the term designated in FIPS 201-1 for the processes and technologies involved in (a) identification: verifying the identity of a Federal employee or contractor at the time of initial identification and enrollment into a Federal agency's identity management system, and (b) authentication: verifying the identity of the employee or contractor for purposes of physical and information systems access control.

PIV Card: A smart card that is designed, issued and managed according to the specifications in FIPS 201-1 and its related technical documents.

Password Aging: The concept that a user must periodically change their password in order to continue to authenticate to services. If the password is not changed within a specific amount if time, it expires and must be reset.

Service Accounts: Account used to run an application service or process or to provide access between application software and data.