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

ORDER
1370.111

Effective Date:
09/15/10

SUBJ: Removable Media Security Policy

1. Purpose of This Order. This Order establishes the security policy for removable media to protect the confidentiality, integrity and availability of the Federal Aviation Administration's (FAA) information and information systems. This Order establishes the principles and working practices to be adopted by all users in order for data to be securely stored, transported and transferred on removable media. This Order does not address the budget impact to the Lines of Businesses and Staff Offices (LOBs/SOs) to implement this policy.

2. Whom This Order Affects. This Order applies to all FAA employees and contractor personnel responsible for or has authorized access to the FAA information systems, including systems that store Sensitive Unclassified Information (SUI), Sensitive Security Information (SSI) and Personally Identifiable Information (PII). Responsibility for and authorized access to such information systems is granted by the System Owner to the FAA employees, contractor personnel, Authorizing Officials (AO), Information Systems Security Managers (ISSMs), and others. Others include grantees, consultants, licensees, and any person or entity, domestic or foreign, having a formal written agreement with the FAA. Each LOB/SO Chief Information Officer (CIO) must develop an implementation plan with budget requirements outlining the transition to utilize removable media that is Government Furnished Equipment (GFE) by September 30, 2010. Once the budget requirements to implement this Order are developed, the LOB/SO CIO must submit a request to their organizational budget office for funding. When funded, the LOB/SO is required to fully exercise their implementation plan. Migration to using only GFE must be completed within two years of signing this order.

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. Background. When removable media is used for storing, transporting and transferring data it provides a convenient entry point for the introduction of security exploitations. The widespread use of strong encryption technology is essential to ensure that the FAA's information systems and data are protected against unauthorized access, fraud and theft. There is a government-wide increase in the number of Information Technology (IT) security threats originating from removable media which infect systems with malicious code and/or inadvertent disclosure of SUI, SSI and PII. This policy addresses the additional security requirements to assist in preventing FAA data from being inadvertently moved outside the enterprise network and/or the physical premises where it can potentially be accessed by unauthorized resources. FAA employees must use approved encryption as required by Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules. The Personal Identity Verification (PIV) card encryption certificates can be used for encrypting and protecting FAA information. Using the PIV card along with digital credential enabled validation systems

provide stronger security measures, multifactor authentication, and reduces employee's password usage.

5. Scope. Removable media consists of portable devices that copy, save, store and/or move data from one system to another. All FAA employees and contractors who are connecting portable external memory devices (i.e., Universal Serial Bus (USB)) to the organizational network must ensure that all security processes normally used in the system and data management on conventional storage infrastructure are also applied here. This removable media security policy applies to, but is not limited to, all removable devices which would allow the transfer of FAA data either externally or internally such as:

a. Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, MiFi, irDA, Bluetooth, among others) or wired network access

b. Removable memory based media (e.g., USB memory devices/readers, removable hard drives, flash drives, thumb drives, jump drives, key drives, rewritable DVDs, CDs, and floppy disks)

c. Memory cards (e.g., SD, CompactFlash, miniSD, microSD, and xD cards) which can be used to support a data storage function on digital cameras, PDAs and smart phones, MP3 and MPEG devices

6. Removable Media Security Policy. Minimum security standards are defined for all users with business requirements to connect removable media to any infrastructure within FAA's internal network(s), related to technology resources or have access to FAA data. This policy provides security standards to protect the confidentiality, integrity and availability of the FAA's business data and systems. Below are the minimum security requirements that must be met:

a. Use removable media that is FAA Government Furnished Equipment (GFE) when storing, transporting or transferring FAA information on FAA-owned and controlled systems. FAA GFE is property acquired by the government and provided to Federal employees and contractor support personnel for work;

b. Configure all FAA-owned and controlled computer systems to detect and scan connected removable media for malicious software;

c. Do not connect personal or unknown removable media into any FAA GFE. Migration to using only GFE removable media must be completed within two years of signing this order. Employees using non-GFE removable media may access the FAA infrastructure with written approval from their LOB/SO;

d. Prevent unauthorized disclosure, modification, removal or destruction of FAA information assets;

e. System owners or LOBs/SOs must establish Standard Operating Procedures (SOPs) for the secure storage, transportation and transfer of data using removable media;

f. Use FIPS 140-2 compliant removable media hardware and/or software when storing,

transporting or transferring all SUI, SSI or PII data:

> The FIPS Publications 140-2 is a government computer security standard used to accredit cryptographic modules. Federal agencies and departments can validate hardware and/or software encryption certification they want to use by the FIPS 140-2 standard.

g. Protect all SUI and SSI in compliance with FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI); which covers the steps to minimize the risk of access by unauthorized persons;

h. Protect, store, transport and transfer PII on FAA-approved removable media and FAA owned equipment and systems only in accordance with FAA Order 1280.1B, Protecting Personally Identifiable Information (PII). The order states:

> "DOT policy only allows the downloading and storage of PII on FAA-owned equipment or systems and authorized support contractor systems. Storage of PII on unauthorized non-FAA-owned equipment and mobile devices is prohibited."

i. This policy does not include the use of removable media for classified information or classified systems. The Assistant Administrator for Security and Hazardous Materials (ASH) provides all security policy for classified information handling.

7. Roles and Responsibilities. All FAA organizations must comply with the roles and responsibilities in accordance with FAA Order 1370.82A, Information Systems Security Program, and carry out additional responsibilities listed below to mitigate risks associated with removable media.

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

(1) Provide agency-wide information systems security leadership, policy, guidance, and oversight of the FAA Removable Media Policy; and,

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

b. The Assistant Administrator for Security and Hazardous Materials (ASH) must: Provide agency wide policy and procedures for protecting SUI, SSI and classified information within the FAA.

c. The FAA 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), and Federal information system security policies, standards, requirements, and guidelines; and,

(2) Ensure compliance with all ISS requirements in this Order and required of the FAA under Federal laws, policies, standards, regulations, and guidelines.

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

(1) Ensure the security guidance and requirements established by this Order are appropriately implemented;

(2) Ensure compliance with Federal security mandates and guidelines concerning all removable media usage; and,

(3) Ensure the system security configuration is properly implemented and configured on the FAA information systems so that all removable media devices are identified when connected to FAA IT assets.

e. The Information Systems Owner (ISO) must:

(1) Ensure that all information systems under their purview comply with the security standards and methods established by this Order; including providing resources to properly implement and configure the information systems allowing the use of removable media;

(2) Ensure that FAA removable media complies with the requirements that SUI, SSI, and PII processed, stored, or transferred is encrypted using approved encryption methods in accordance with FAA Order 1370.103, Encryption Policy;

(3) Ensure compliance with the minimum security requirements for data handling requirements in accordance with FAA Order 1600.75, when using removable media; and,

(4) Ensure that users have the appropriate FAA GFE hardware and software to adhere to this policy.

f. The Network and System Administrators must:

(1) Ensure that SUI, SSI, and PII data can be encrypted when using removable storage media in compliance with the FAA Order 1370.103, Encryption Policy;

(2) Configure systems to scan removable media used on all FAA-owned and controlled computer systems to protect against any malicious attacks;

(3) Disable AutoRun or AutoPlay operating system features for removable media drives and ports on all GFE; and,

(4) Must report any incidence of disclosure or potential disclosure of sensitive data on removable media to their immediate supervisor.

g. Users must:

(1) Use strong passwords and PINs to protect removable media, where available, as defined in FAA Order 1370.92, Password and PIN Management;

(2) Encrypt SUI, SSI and PII stored on removable media utilizing encryption as stated in FAA Order 1370.103, Encryption Policy;

(3) Use removable media that is GFE when storing, transporting or transferring FAA information on FAA-owned and controlled systems;

(4) Use security measures and multifactor authentication when using removable media when available. (The PIV card encryption certificate can be used to provide encryption capability; and,

(5) Must report any incidence of disclosure or potential disclosure of sensitive data on removable media to their immediate supervisor.

8. Statutory Policy and Regulatory Mandates.

a. The E-Government Act Public Law (P.L.) 107-347, passed and signed into law by the President in December 2002, established the Federal Information Security Management Act (FISMA).

b. The Federal Information Security Management Act of 2002, (FISMA) requires that Federal agencies perform periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls with a frequency depending on risk, but no less than annually.

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 National Institute of Standards and Technology (NIST).

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

e. The OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006, requires the FAA to ensure that appropriate controls and mechanisms are in place to protect sensitive and privacy-related information.

f. The OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006, provides updated guidance on the reporting of security incidents involving PII for fiscal year 2008 budget submissions for information technology.

g. FAA Order 1370.82A, Information Systems Security Program addresses contractor compliance with agency-wide ISS policies, standards and requirements.

9. References. References are contained in Appendix A of this Order.

10. 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 B.

11. Notice of Exception or Noncompliance.

a. This Order establishes policy to comply with statutory and regulatory requirements, including NIST information systems security publications made mandatory by the FISMA. Compliance with the policy established by this Order is mandatory.

b. The head of a LOB/SO, ISO, or AO can request the FAA 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 Authorization Package must include the copy of the request and waiver decision.

12. 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.

13. 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 140-2, Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 2001.

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

c. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

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

e. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, July 2008.

f. NIST SP 800-64, Security Considerations in the System Development Life Cycle, October 2008.

g. NIST SP 800-95, Guide to Secure Web Services, August 2007.

h. NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007.

i. NIST SP 800-115, Technical Guide to Information Security Testing, October 2008.

j. FAA Order 1280.1B, Protecting Personally Identifiable Information (PII), December 17, 2008.

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

l. FAA Order 1370.89, Information Operations Conditions, August 25, 2003.

m. FAA Order 1370.91, Information Systems Security Patch Management, May 19, 2004.

n. FAA Order 1370.92, Password and PIN Management, June 28, 2004.

o. FAA Order 1370.100, Media Sanitizing and Destruction Policy, October 1, 2007.

p. FAA Order 1370.103, Encryption Policy, November 12, 2008.

q. FAA Order 1370.106, Information Systems Security Awareness and Training Policy, June 16, 2009.

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

s. FAA Order 1800.66, Configuration Management Policy, September 19, 2007.

Appendix B. Definitions

AutoPlay/ AutoRun: Components of the Microsoft Windows operating system that dictate what actions the system takes when a drive is mounted.

Encryption: A technique used to protect the plaintext by coding the data such that it is unreadable to the reader. Encryption hides its content from everyone except its intended audience.

Encryption Software or Hardware: A mathematical algorithm to scramble bits of data sent or stored on computer networks. The key to the cipher is a string of numbers or other characters. The stronger the algorithm and the longer the string, the harder it is to break.

FAA-approved: Provides a written list of services, 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.

Personally Identifiable Information (PII): Any information about a human being, living or deceased, regardless of nationality, that is maintained by an agency. This includes information that permits identification of that individual to be reasonably identified by either direct or indirect means (i.e., as in data mining). The following types of information are included, but not limited to: name, home address, social security number, driver's license identification number, date and place of birth, mother's maiden name, biometric records, education, financial

transactions, medical information, non-work telephone numbers, and criminal or employment history (including any other personal information that is linked or linkable to an individual).

Removable Media: Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer. This includes but is not limited to flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks.

Sensitive Personally Identifiable Information (SPII): The PII that, if released for unauthorized use, is likely to result in substantial harm to the individual to whom such information relates.

Sensitive Security Information (SSI): SSI is a designation *unique* to the DOT and DOT's operating administrations and to the Department of Homeland Security (DHS). It applies to information we obtain or develop while conducting *security activities*, including research and development activities.

Sensitive Unclassified Information (SUI): Any unclassified information in any form including: print, electronic, and visual and audio forms that must be protected from unauthorized disclosure outside of the FAA. The SUI is subject to limited, controlled distribution within the FAA as determined by the information steward. This includes personally identifiable information, aviation and homeland security, and protected critical infrastructure information, all of which may qualify for withholding from the public under the FOIA, 5 USC #552.

Appendix C. Baseline FIPS 140-2 Certified Products

Please Note: This appendix is a product baseline and is not all inclusive.

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules can be referenced from:

VENDOR	PRODUCT	LINK
USB Flash Drives		
IronKey	IronKey Personal S200 (1G-32G)IronKey Personal D200 (1G-32G)	https://www.ironkey.com/glossary/fips-140-2
Kanguru Solutions	Kanguru Defender Elite (1G-16G, 32G-128G)	https://www.kanguru.com/index.php/flash-drives/secure-storage/kanguru-defender-elite
Kingston Technology Company	DataTraveler 5000	http://www.kingston.com/flash/DataTravelers_gov.asp
Lexar Media, Inc.	JumpDrive SAFE S3000	http://store.lexar.com/?productid=LAD2GBCENA600 http://www.lexar.com/pdf/lit/Lexar_Ent_JD_SAFE_S3000_FIPS.pdf
MXI Security Co.	Stealth MXB Bio	http://www.mxisecurity.com/categories/display/9
SanDisk Corporation	Cruzer® Enterprise	http://www.sandisk.com/business-solutions/enterprise/cruzer-enterprise-fips-edition
Data Encryption Software		
Crypkey	Crypkey	www.crypkey.com
Data Encryption Systems Limited	DESlock+	www.des.co.uk
PKWARE, Inc.	SecureZip ®	http://www.pkware.com/software-data-security
Hard Drive Encryption Software		
Check Point Software Technologies LTD.	Full Disk Encryption	http://www.checkpoint.com/pricelist/US/Sections/main.jsp
Credant Technologies Corporation	Full Disk Encryption CMG for External Media	http://www.credant.com/products/client-services.html
Encryptx Corporation	Securflash Basic	www.encryptx.com http://www.encryptx.com/products/usb_flash_drive_encryption.php
Encryptx Corporation	Securflash Premium	www.encryptx.com http://www.encryptx.com/products/usb_flash_drive_encryption.php
GuardianEdge Technologies Corp.	Hard Disk Encryption Removable Storage Encryption	http://guardianedge.com/forms/sales-contact-form.php
McAfee®	SafeBoot	http://www.safeboot.com/secureUS/ http://www.safeboot.com/Press/Repeater_DataSource.aspx?NewsID=57

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm