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

ORDER
1370.110

Effective Date
09/15/10

SUBJ: Secure Telework Policy

1. Purpose of This Order. This Order establishes the Federal Aviation Administration's (FAA) enterprise-wide Secure Telework Policy. This Order outlines the roles and responsibilities associated with the implementation of a secure teleworking environment. This Order provides minimum security requirements for the FAA infrastructure and prepares eligible personnel for working remotely using Government Furnished Equipment (GFE). 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 who participate in the FAA Telework Program and access any FAA network. Each LOB/SO Chief Information Officer (CIO) must develop a secure telework implementation plan with budget requirements outlining the transition to the use of 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. The FAA Human Resources Policy Manual (HRPM) Volume 12: Work Life and Benefits provides policy and guidance to managers and employees on FAA's Telework Program and describes the rules and procedures that apply to teleworking. It is FAA policy to actively encourage the use of teleworking whenever possible. This policy addresses the additional security requirements to establish a secure teleworking environment. Teleworking at the FAA is consistent with and supports agency mission and performance goals, as well as improves the agency's capability to support homeland and national security requirements. Properly administered teleworking improves individual and organizational productivity, serves as a recruitment and retention tool and improves work life quality. It is an effective and efficient means for continuing critical functions when staff cannot travel to a central office due to geographical incidents, national disasters, or extended emergencies.

5. Scope. The Secure Telework Policy focuses on the security aspect of teleworking and not the eligibility to participate in the FAA Telework Program. It serves as a security enhancement to the FAA HRPM, FAA Telework Agreement and FAA Self-Certification Safety Checklist for all teleworkers. This Policy does not apply to the processing of classified information. The Assistant Administrator for Security and Hazardous Materials (ASH) provides all security policy for classified information handling.

6. Secure Telework Policy. The telework capability is designed to assist the FAA employees participating in the Telework Program to accomplish work effectively and securely from any location outside of the employee's office. Below are the minimum security requirements that must be met:

a. Employees must use GFE when connecting directly to the FAA infrastructure for purposes of teleworking using a Virtual Private Networking (VPN) capability;

> VPNs provide an additional layer of protection when transferring data to and from a FAA information system. The network uses a public telecommunication infrastructure while maintaining privacy through security procedures, to provide remote offices or individual users with secure access to their organization's network.

b. The use of non-GFE for access to FAA information outside the FAA infrastructure (e.g., FAA Webmail and Employee Express via the internet) is permitted except when it contains Sensitive Unclassified Information (SUI), Sensitive Security Information (SSI) and other individuals' Personally Identifiable Information (PII) (e.g., downloading attachments);

c. Migration to using only GFE must be completed within two years of signing this order. Teleworking employees using non-GFE are authorized to access the FAA infrastructure with written approval from their LOB/SO until GFE can be provided;

d. All SUI and SSI must be handled in accordance with FAA Order 1600.75, Protecting Sensitive Unclassified Information as stated:

> "Whether telecommuting from home or at a telecommuting center, you must provide the same level of protection for the information that you do from your normal site. Your manager must approve specific protective measures for handling paper records, and your information system security manager must certify the adequacy of security for off-site access to sensitive data."

e. Physically protect GFE (e.g., laptops or portable electronic devices) used for teleworking to prevent disclosure of FAA data or information to unauthorized persons;

f. Process, transmit and store privacy information on GFE in accordance with FAA Order 1280.1B, Protecting Personally Identifiable Information (PII) as stated:

> "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."

g. Dispose of SUI, SSI and PII in accordance with FAA Order 1370.100, Media Sanitizing and Destruction Policy as stated:

> "Disposal is discarding media with no technique employed, other than perhaps simple deletion, to remove stored information or render it unrecoverable. Disposal is suitable only for non-sensitive information such as information that is widely available (e.g., posted on an agency public-facing web site). Rewritable digital media must not be simply discarded if they could have been used to store sensitive information that may

still be recoverable. Placing hard copy media (or other media, if permitted) in a locked bin intended for unneeded sensitive information is not simply discarding, since the contents of the bin will pass through a trusted chain of custody that end in their destruction."

h. Encrypt all SUI, SSI and PII in accordance with FAA Order 1370.103, Encryption Policy;

i. Ensure the FAA enterprise hard drive encryption software is installed and running on GFE Portable Electronic Devices (PEDs);

j. Utilize a FAA or LOB/SO approved Virtual Private Network (VPN) using multifactor authentication in accordance with FAA Order 1370.90, Internet Access Point Configuration Management when accessing the FAA infrastructure. FAA-approved VPN's include the FAA Telecommunication Infrastructure (FTI) Remote Access Capability (FRAC), or other VPN's authorized by the FAA LOB/SOs.

7. 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 Secure Telework Policy; and,

(2) Ensure information owned or maintained by the FAA is protected against unauthorized access, use, modification, or destruction while teleworking.

b. The Assistant Administrator for Security and Hazardous Materials (ASH) must:

(1) Provide agency wide policy and procedures for protecting SUI and SSI within the FAA.

(2) Provide agency wide policies and procedures for protection of classified information within the FAA.

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

(1) Oversee the implementation of this order; all FAA and DOT orders dealing with information system security policies, standards, requirements and guidelines; and, the best business practices adopted by the FAA contained in the Federal Information Security Management Act (FISMA); and,

(2) Conduct annual compliance reviews to ensure the LOBs/SOs have implemented a FAA secure telework process.

d. The FAA Privacy Officer must:

(1) Ensure appropriate privacy protections exist for PII that are collected, stored, disseminated, transmitted, or disposed of by information systems owned or operated by or for the FAA;

(2) Ensure compliance with all privacy requirements imposed on the FAA under Federal laws, policies, standards, regulations and guidelines; and,

(3) Serve as the principle advocate for FAA personnel when PII has been compromised, disclosed or released to unauthorized persons.

e. Line of Business/Staff Office (LOB/SO) Chief Information Officer (CIO)

(1) Must develop a secure telework implementation plan with budget requirements outlining the transition to the use of GFE; and,

(2) Must exercise their implementation plan when funded.

f. The Information Systems Owner (ISO) must:

(1) Define general and system-specific Rules of Behavior (ROB) that contain minimum requirements in accordance with FAA Order 1370.107, Rules of Behavior/ System Use Policy.

g. The Information Systems Security Managers (ISSMs) must:

(1) Ensure that the appropriate operational security posture is implemented and maintained for the information systems or programs within their LOB/SO;

(2) Ensure that Supervisors are aware of the Secure Telework Checklist and the requirements for its use.

h. Supervisors must:

(1) Ensure all FAA employees approved to telework either physically or electronically acknowledge and sign the Secure Telework Checklist identified in Appendix C of this Order; and,

(2) Maintain copies of signed employee Secure Telework Checklist and forward copies to the LOB/SO telework coordinator.

i. LOB/SO Facility Information Technology (IT) Local Area Network (LAN) Team:

(1) Ensure that employees approved to telework have the appropriate FAA hardware and security software (firewall, antivirus, VPN and hard drive encryption software) installed on their GFE; and,

(2) Grant access to specific FAA systems and applications at the discretion of the LOB/SO, system owner and management.

j. Teleworking employees must:

(1) Sign and adhere to the Secure Telework Checklist, Appendix C, regarding the use of FAA information and information systems; and,

(2) Use security protections and follow FAA security policies as they pertain to the protection of information and information system resources. These policies require that:

(a) All electronic devices that carry agency SUI data must be encrypted in accordance with FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI) when storing or transmitting data outside the FAA network;

(b) All electronic devices that carry agency PII data must be encrypted in accordance with FAA Order 1280.1b, Protecting Personally Identifiable Information (PII) when storing or transmitting data outside the FAA network;

(c) Maintain the minimum security measures and procedures identified in this policy and the LOB/SO; and,

(d) Report any suspected cyber security incident involving the theft, loss, or unauthorized disclosure of information or an information system device immediately to the employee's supervisor.

8. Statutory Policy and Regulatory Mandates.

a. The Electronic Communications Protection Act (ECPA) of 1986, 18 United States Code (U.S.C.) §§ 2510-22 and §§ 2701-12 states that ECPA prohibits the unauthorized interception, disclosure, or use of electronic communications that imposes both civil and criminal liability. Title I – Amendment to Wiretap Act limits electronic interceptions to those taking place during transmission, and Title II – Stored Communications Act addresses intentional unauthorized access to an electronic communication service facility to obtain, modify, or prevent authorized access to electronic communications.

b. The Privacy Act of 1974, 5 U.S.C. § 552a, is concerned with the protection of Personally Identifiable Information (PII) and privacy records. Federal agencies must establish controls that safeguard PII and privacy records through the deployment of physical, technical, and administrative controls.

c. Public Law (P.L) 106-346, passed by and signed into law by the President in October 2000, established the Department of Transportation Related Agencies Appropriations, 2001, under which eligible employees may participate in teleworking to the maximum extent possible without diminished employee performance.

d. Public Law 106-346, § 359, dated October 23, 2000, as interpreted by the Office of Personnel Management (OPM) in a memorandum dated February 9, 2001, instructs Federal agencies (1) to review existing teleworking policies to reduce and eliminate barriers that inhibit

the use of teleworking and to increase program participation; (2) to establish eligibility criteria; and (3) that, subject to any applicable agency policies or bargaining obligations and without diminished employee performance, employees who meet the criteria and want to participate must be allowed that opportunity if they are satisfactory performers. The law provides that its requirements must be applied, by 2004, to 100% of the eligible Federal workforce.

e. Public Law 104-52, Treasury, Postal Service and General Government Appropriations Act of 1996, enables agencies to use appropriated funds to install and fund telephone lines and/or other equipment in the homes of employees authorized to work at home.

f. Public Law 108.199, division B, section 627 established directives to certain agencies to increase telework participation in the workforce by specified amounts.

g. The Department of Transportation (DOT) Order 1501.1A, Telework Policy, addresses managing telework and promoting appropriate controls for performance accountability, safety, and information security.

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

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. Penalties for user noncompliance with this Order are subject to actions in accordance with existing policy and regulations, applicable union contracts and/or 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.

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. OPM Report to Congress, Status of Telework in the Federal Government, dated December 2008.

b. OPM Memorandum to Heads of Executive Departments and Agencies, Subject: Washington, DC Area Dismissal or Closure Procedures dated October 2008.

c. OPM Guide to Telework in the Federal Government dated August 2006.

d. OPM Guide to Processing Personnel Actions, Chapter 23, dated September 21, 2000.

e. GAO-09-783T Influenza Pandemic_ Greater Agency Accountability Needed to Protect Federal Workers in the Event of a Pandemic, dated June 2009.

f. DOT Order 1501.1A, Department of Transportation Telework Policy.

g. General Services Administration (GSA) Federal Management Regulation; Guidelines for Alternative Workplace Arrangements dated March 17, 2006.

h. NIST SP 800-114, Users Guide to Securing External Devices for Telework and Remote Access, dated November 2007.

i. NIST SP 800-46 Rev. 1, Guide to Enterprise Telework and Remote Access Security, dated June 2009.

j. FAA Human Resource Policy Manual (HRPM) Volume 12: WLB-12.3 FAA Telework Program.

k. FAA Self-certification Safety Checklist for Home-Based Teleworkers.

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

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

n. FAA Order 1370.90, Internet Access Point Configuration Management, August 01, 2003.

o. FAA Order 1370.100, Media Sanitizing and Destruction Policy, October 01, 2007.

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

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

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

Appendix B. Definitions

Alternate Worksite: A place away from the traditional worksite that has been approved for the performance of officially assigned duties. It may be an employee's home, a telework center, or other approved worksites including a facility established by state, local, county governments, or private sector organizations for use by teleworkers.

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. A 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 a 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: A system wherein two (or more) different factors are used in conjunction to authenticate. Using two or more factors as opposed to one factor generally delivers a higher level of authentication assurance. An example of multifactor authentication is a verification of "something you have" (PIV card) and "something you know" (PIV PIN).

Portable Electronic Devices (PEDs): A piece of electronic equipment such as a laptop computer or mobile phone that is small and easy to carry.

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).

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.

Telework: Refers to any arrangement in which an employee performs officially assigned duties at an alternative worksite on either a regular or recurring, or on an ad hoc, basis (not including while on official travel). The terms teleworking and telework for government employees refer to two scenarios enabled by remote access networking technology; working from home (also called teleworking) and working mobile, such as in a field-based role or working temporarily at a remote location.

Telework Agreement: A written agreement completed and signed by an employee and appropriate official(s) in his or her component, that outlines the terms and conditions of the telework arrangement.

Virtual Private Network (VPN): A connection between a remote computer and server on a private network that uses the Internet as its network medium or a remote network and another network that uses the Internet as its network medium. The remote computer and the network server then establish a secured connection that protects the data exchanged between them as it travels over the Internet. This technique is called tunneling, because the connection runs across the Internet inside a secure conduit, protecting the data in the way that a tunnel under a river protects cars from the water above it.

Appendix C. Secure Telework Checklist

FEDERAL AVIATION ADMINISTRATION
Secure Telework Checklist

Name: _____ Organization: _____
Location: _____ Phone: _____
Alternate Worksite Location: _____

The following checklist ensures that the employee is protected at the alternate worksite. Each participating employee and his/her manager must read, sign and date this Secure Telework Checklist.

	Yes	No
I telework using Government Furnished Equipment (GFE)	☐	☐
LOB/SO IT LAN Team has verified that GFE is properly up to date with the following:		
• **Anti-virus software installed and running with up-to-date virus definitions**	☐	☐
• **Firewall software installed and running with current firewall rule sets**	☐	☐
• **Software and OS patch updates are applied**	☐	☐
• **FAA enterprise hard drive encryption software is installed and running**	☐	☐
I use remote access via a FAA Virtual Private Network account using multifactor authentication.	☐	☐
I accept and allow the installation of all software updates when prompted.	☐	☐

1. Follow security practices that are the same as or equivalent to those required at my primary workplace. Adhere to all security provisions or agreements related to off-site work.
2. Physically protect GFE used for official teleworking.
3. Employees must not allow any non-government personnel to use any government-furnished equipment.
4. Comply with:
   - FAA Order 1280.1B, Protecting Personally Identifiable Information
   - FAA Order 1370.79A, Internet Use Policy
   - FAA Order 1370.81A, Electronic Mail
   - FAA Order 1370.82A, Information Systems Security Program
   - FAA Order 1370.92, Password and PIN Management
   - FAA Order 1370.94, Wireless Technologies Security
   - FAA Order 1370.100, Media Sanitizing and Destruction Policy
   - FAA Order 1370.103, Encryption Policy, Peer-to-Peer (P2P) Software Policy Memo
   - FAA Order 1370.107 Rules of behavior/System Use Policy
   - FAA Order 1600.75, Protecting Sensitive Unclassified Information
   - FAA Order 1370.xx, Secure Telework Policy, as amended
5. Report any suspected cyber security incident involving theft, loss, or unauthorized disclosure of information or an information system device immediately to your supervisor.

Employee Signature: _____ Date _____

Manager Signature: _____ Date _____

Attach a copy of this checklist to your FAA telework agreement, forward to your telework coordinator and retain a copy for your records.