

# **12 FAM 680 REMOTE ACCESS AND MOBILE COMPUTING TECHNOLOGY**

*(CT:DS-138; 08-04-2008)  
(Office of Origin: DS/SI/CS)*

## **12 FAM 681 PURPOSE**

*(CT:DS-138; 08-04-2008)*

This chapter establishes the minimum automated information system (AIS) security standards for remote access from, and processing of Department Unclassified / Sensitive But Unclassified (SBU) information on, non-Department systems; and for secure processing of Department information on mobile devices.

### **12 FAM 681.1 Applicability**

*(CT:DS-138; 08-04-2008)*

This chapter applies to all users remotely accessing and / or remotely processing Department Unclassified / SBU information.

## **12 FAM 682 REMOTE ACCESS FROM AND PROCESSING OF DEPARTMENT UNCLASSIFIED/SBU INFORMATION ON NON- DEPARTMENT SYSTEMS**

### **12 FAM 682.1 SCOPE**

*(CT:DS-138; 08-04-2008)*

- a. This policy establishes the minimum security requirements for remote access from, and processing of Department Unclassified / SBU information on, non-Department systems. Remote access to Department classified networks is not authorized.
- b. For purposes of this subchapter, "remote access" refers to accessing Department SBU and Unclassified networks, either domestically or abroad, from non-Department systems (e.g., personally-owned or public

access computers, PDAs, laptops, multi-function cell phones, etc.) via a Department-approved remote access program. Remote access includes but is not limited to the following activities:

- Department e-mail, contacts, and calendars
- Department major and minor applications
- Intranet, Extranet, and Internet browsing
- File access privileges (e.g., read, write, and execute)
- Remote storage and printing
- Sensitive data storage (e.g., hard drives, flash memory drives, etc.)

**NOTE:** Remote administration / maintenance is prohibited.

- c. "Remote processing" refers to processing Department information on non-Department systems at non-Department facilities.
- d. This [sub?]chapter does not apply to:
  - (1) Department-owned systems (e.g., Secure Dial-In (SDI) laptops, Information Technology Change Control Board (IT CCB)-approved Blackberry-type devices, etc.);
  - (2) Access to Department public Web sites via either personally-owned, public access, or other government agency computers;
  - (3) Dedicated connections, such as approved tail circuits to contractors or inter-agency connectivity; or
  - (4) Information Resource Center (IRC) and American Service Center (ASC) DINs that permit connectivity from non-Department-owned computers

## **12 FAM 682.2 Policy**

### **12 FAM 682.2-1 Remote Access Authorization**

*(CT:DS-138; 08-04-2008)*

- a. Remote access to Department networks from non-Department-owned systems (e.g., personally-owned or public access computers) is only authorized via Department-approved remote access programs (e.g., OpenNet Everywhere (ONE)). Users accessing the Department's networks under any authorized remote access program must meet the requirements stipulated in this policy as well those of the specific remote access program under which they are connecting (e.g., ONE). When the policy requirements and the program requirements differ, the more stringent requirements will apply.

- b. Remote access programs may be used in support of the Department's telecommuting program. In those instances where the telecommuter remotely accesses the Department via a non-Department-owned system, he or she must abide by these policy requirements as well as the 3 FAM 2360 and the 12 FAM 625.2-3, Telecommuting Policies.
- c. Remote access is restricted to personnel who possess a Department-issued identification card or are cleared U.S. citizens (as defined in 12 FAM 090) that have security clearances verified by the Office of Personnel Security and Suitability (DS/SI/PSS), and have a Department network account. This includes Department full-time employees (FTEs), contractors, locally employed staff (LES), and other-agency tenant personnel.
- d. In countries that have a post rated at the High or Critical Technical Threat or HUMINT Threat level by the Department's Security Environment Threat List (SETL), use of remote access is subject to additional restrictions. Specifically, use of remote access within such countries is authorized only:
  - (1) For U.S. citizens who hold security clearances at the SECRET level or higher; and
  - (2) From U.S. Government-owned or leased facilities.

Remote access by other personnel or from other locations—including public access terminals or public access wireless access points—is strictly prohibited unless an exception has been approved in writing by the Office of Computer Security (DS/SI/CS) and the Office of Information Assurance (IRM/IA). Such exceptions will be approved only for emergency situations and generally will not be granted in countries with a post that has a Technical or HUMINT Threat rating of Critical.

## **12 FAM 682.2-2 Remote Access Management Responsibilities**

*(CT:DS-138; 08-04-2008)*

- a. Management must exercise particular care and judgment with regard to records and information that are SBU, contain personally identifiable information (PII), and / or are subject to specific controls under the Privacy Act. Offices allowing employees to remotely access these records must ensure that the administrative, technical, and physical safeguards stipulated in this policy are implemented and maintained to ensure the protection of the confidentiality and integrity of records.
- b. A U.S. citizen direct-hire supervisor and either management officer or executive director must:
  - (1) Approve in writing all requests for remote access by individual

users;

- (2) Ensure that a sufficient business requirement exists; and
- (3) Notify the user's servicing ISSO.

Overseas, all requests for remote access must also be reviewed and cleared by the regional security officer (RSO) to ensure that adequate consideration is given to the local threat environment.

- c. The user's servicing ISSO must provide approved remote access users a security briefing on Unclassified / SBU remote access. The ISSO should use the briefing provided on the DS/IS/CS Awareness Web page. This briefing identifies the risks to the Department's networks and data, and clearly defines the user's responsibilities. The ISSO must include risks specific to the local environment in the briefing. The ISSO must have the user sign (hard copy or via an approved digital signature) an acknowledgment form indicating the user has received the Unclassified / SBU remote access security briefing. Copies of the acknowledgment form may be found on the DS/IS/CS Awareness Web page. This acknowledgment must be kept on file for two years. The ISSO must ensure that the user receives an annual refresher briefing and signs a new acknowledgment form each year.
- d. The ISSO must keep a list of all users with remote access. This list must be reviewed on an annual basis to ensure that the list is current and accurate. The ISSO must also keep a copy of the supervisor's written approval for each user authorized to access or process PII.
- e. Upon user departure from bureau / post, the ISSO must sign the user's check-out form indicating that all Department-owned remote access devices (e.g., ONE fobs, have been turned in and the user's remote access capabilities have been deactivated). The ISSO must also confirm whether the user had been authorized to access or process PII. For authorized users, the ISSO must instruct the users to remove all PII from their computer or removable media, using a file shredder application. This software will permanently delete the files without damaging the computer or media. The DS/IS/CS Home Use – File Destruction Web Page lists several available shredding products.

## **12 FAM 682.2-3 Configuring Remote Access Accounts**

*(CT:DS-138; 08-04-2008)*

- a. Remote Logon access must use two-factor authentication: something a user 'knows' (e.g., a password/passphrase) and something a user 'has' (e.g., the one-time password produced by ONE fob).
- b. Remote access program managers (e.g., the Messaging System Office (IRM/OPS/MSO) for the OpenNet Everywhere (ONE) remote access

program) must ensure that all remote access portals display the Department's pre-logon warning message on the initial logon page.

- c. Remote access transmission links to the Department's networks must be secured, at a minimum, with National Institute of Standards of Technology (NIST) Federal Information Processing Standard (FIPS) 140-2, level 2, certified encryption products. Encryption products must be configured in accordance with the associated product security policy listed with each product in the NIST approval list. The approval list may be found on the NIST Web site under the Cryptographic Module Validation Program.
- d. Remote access program managers must configure the remote OpenNet session to lock the OpenNet server after 20 minutes of inactivity. The remote access program must be configured to ensure that user re-authentication is required each time a user logs in.
- e. The user's servicing ISSO, in coordination with the user's U. S. citizen direct-hire supervisor, must ensure that user access privileges reflect the separation of key duties users perform with respect to specific applications (e.g., system administrator accounts must not be used as system user accounts, database management accounts must not be used as data entry accounts, etc.).
- f. Remote access is only authorized for user-level privileges; remote administration / maintenance is prohibited.
- g. Supervisory personnel may direct subordinates to not process especially sensitive information on a personally-owned or public access computer. (See 12 FAM 622.1-5.)

## **12 FAM 682.2-4 Remote Processing Authorization**

*(CT:DS-138; 08-04-2008)*

- a. Management and employees must exercise particular care and judgment with regard to records and information that are SBU, contain PII, and / or are subject to specific controls under the Privacy Act. Offices allowing employees to remotely process these records must ensure that appropriate administrative, technical, and physical safeguards are maintained to protect the confidentiality and integrity of records.
- b. Users must not store or process SBU or PII (other than basic personal information or contact information for colleagues and professional associates) on non-Department-owned computers unless it is necessary in the performance of their duties.
- c. U.S. citizen direct hire supervisors must:
  - (1) Approve, in writing, users processing PII on non-Department-owned

devices; and

- (2) Advise the user that all storage media (e.g., hard drives, flash memory, etc.) containing SBU or PII must be encrypted with products certified by NIST FIPS 140-2.

The encryption products must be configured in accordance with the NIST security policy provided with the certified product. A list of NIST products certified under the Cryptographic Module Validation Program may be found at NIST's Module Validation List Web page.

## **12 FAM 682.2-5 User Responsibilities for Remote Accessing and/or Processing of Department Unclassified/SBU Information**

*(CT:DS-138; 08-04-2008)*

- a. Users must adhere to the requirements set forth in 12 FAM 543, Access, Dissemination, and Release, when accessing and / or processing Department SBU or PII. In accordance with 12 FAM 543, users must ensure that:
  - (1) Discretion is exercised with respect to saving SBU or PII (e.g., save only when required). Users may save SBU or PII only to media under the user's continuing control (e.g., a personally owned computer hard drive or diskette, etc.). Users may not save SBU or PII on a hard drive that is accessible to the public (e.g., an Internet café, a public library, a document sharing site);
  - (2) All Department SBU or PII is encrypted as stated in 12 FAM 682.2-4c;
  - (3) Discretion is exercised with respect to printing SBU data (e.g., public printers will temporarily retain data images until overwritten). PII must not be printed in public locations (e.g., a kiosk, an Internet café);
  - (4) SBU or PII stored in hard copy format or on removable media must be secured as stated in 12 FAM 544.1, FAX Transmission, Mailing, Safeguarding/Storage, and Destruction of SBU.
- b. Users with individually assigned fobs must not share their remote access passwords and authentication tokens with other individuals. Users with group assigned fobs (e.g., duty officers) must have individually assigned UserIDs and Passwords for OpenNet. Group UserIDs and passwords on OpenNet are prohibited. Password controls must be in accordance with 12 FAM 622.1-3.
- c. While connected remotely, users must lock user-owned and managed computers (e.g., CTRL+ALT+DEL) or, if not possible, close the remote

access session when the user needs to temporarily leave the workstation. If the CTRL+ALT+DEL option is used then a twenty minute screen saver lockout feature must also be enabled as a backup security measure. To use these options the computer must be configured to use passwords. Information on implementing screen savers and passwords can be found on the DS/SI/CS Home Use Web page.

- d. Users must never leave a remote access session unattended at a public location. They must log out of the session and close the browser / remote access program before leaving the computer.
- e. Upon logout from a remote access session, users must verify that the logout confirmation screen is received before leaving the workstation.
- f. Users must exercise discretion when using remote access in public areas and take prudent measures (e.g., shield the screen from public view) to minimize unauthorized data viewing.
- g. Users must destroy SBU and PII files that have been saved on their personally-owned and managed computers and removable media when the files are no longer required. Destruction must be accomplished using a file shredder application to minimize file recovery. Information on file shredder applications can be found on the DS/SI/CS Home Use Web page.
- h. When using personally-owned computers for remote access or remote processing of Department data, users must implement basic home security controls, to include deploying a firewall, anti-spyware, antivirus, and file destruction applications. Upgrades / updates to these applications must be kept current. Further, security patches for operating systems and applications must be applied as soon as possible. Information on firewall, anti-spyware, antivirus, and file destruction software can be found on the DS/SI/CS Home Use Web page.
- i. In addition to the above security controls, when using wireless capabilities on a personally-owned computer, users must enable NIST certified encryption algorithms (e.g., AES, 3DES, etc.) across the wireless link as a secondary layer of security for data transmissions. Further information on configuring wireless access points can be found on the DS/SI/CS Home Use - Wireless Network Web page. At a minimum, personally-owned wireless access points must be configured as follows:
  - (1) Disable the Service Set Identifier (SSID) broadcast mode in the wireless network base station (e.g., router);
  - (2) Change the SSID so that only those configured with the same SSID can communicate with base stations having the same SSID;
  - (3) At a minimum, implement Wireless Protected Access 2 (WPA2) encryption. WPA2 uses AES encryption to secure the link; and

- (4) Change the default wireless network base station's administrator password to a password sufficiently complex as to not be easily guessed.
- j. When using personally-owned power-line networks (i.e., personally owned computers networked via home electrical outlets) users must change the default passwords on all power-line devices, and provide link encryption using NIST-certified encryption algorithms (e.g., AES, 3DES, etc.).
- k. When using a networked personally-owned computer (e.g., a home network) users must ensure that all computers on the network implement the security requirements identified above in paragraphs "h", "i" and "j" (e.g., firewall, anti-spyware software, file/hard drive encryption for SBU, hard drive encryption for PII, and NIST-certified encryption for a wireless or power-line network).

## **12 FAM 682.2-6 Cyber Security Incidents**

*(CT:DS-138; 08-04-2008)*

- a. Users must report the (actual or suspected) loss, theft, or compromise of the following:
  - (1) A Department-owned remote access device or associated Department-owned media;
  - (2) Non-Department-owned media (e.g. hard drive, CD) containing SBU information, or
  - (3) An access token (e.g., a smartcard) within 24 hours or the next duty day of the event, whichever comes first, to the information system security officer (ISSO) and system manager.

If the device or media (Department-owned or non-Department-owned) contained PII, the event must also be immediately reported to the computer incident response teams (DS/CS/CIRT). DS/CS/CIRT is available 24 hours a day, seven days a week and may be contacted via unclassified e-mail at CIRT@state.gov; classified e-mail at CIRT@state.sgov.gov; or by telephone at (301) 985-8347. DS/CS/CIRT must promptly notify the Office of Investigations (OIG/INV) when the loss, theft, or compromise of a device or media contains PII data. (DS/CS/CIRT is also required by Federal mandate to notify the U.S. Computer Emergency Readiness Team (US CERT) within one hour of receiving the report.) More information on reporting a PII breach can be found at the Bureau of Administration's PII Breach Response Policy Plan.

- b. In the event that an authentication "token" (e.g., the password fob or a Department Smart ID card) is reported missing, the user's servicing ISSO, bureau security officer (BSO), or primary unit security officer (PUSO), or RSO who oversees the user's account, must ensure that the

user's capability to logon remotely is immediately disabled. The user's remote access privileges may be reinstated upon re-issuance of a new token. Loss of Smart ID must be immediately reported to the user's PKI representative or the Department's Certification Authority.

- c. The ISSO must ensure that all cyber security incidents are reported as required in 12 FAM 590, Cyber Security Incident Program.

## **12 FAM 683 THROUGH 689 UNASSIGNED**