

DATE July 6, 2001

SECURITY REQUIREMENTS FOR PERSONAL DIGITAL ASSISTANTS

1. **PURPOSE.** This policy establishes security requirements related to the introduction and use of personal digital assistants (PDAs) within the Bureau. It provides guidance on the risks involved in using PDAs; the types of information that may be processed and/or stored on them; the approval procedures for procuring them; and the specific, limited user support from the Bureau.

2. **SCOPE.** This section applies to all PDAs (government and personally owned) and the types of data that may be accessed or stored using these devices. This policy is an extension of several policies in Treasury Department Policy (TDP) 71-10, Chapter 6, Section 4.B., titled "Program for the Protection of Sensitive But Unclassified Information Processed in Automated Information Systems and Networks." Several specific restrictions, as they impact Bureau operations and information systems, are addressed. This policy shall apply to all Bureau employees, Bureau contractors, and other persons visiting or representing other Government agencies while on the Bureau premises. Additionally, it applies to all parties when they are connected to Bureau automated information systems and networks, on the premises or via remote access.

For the purposes of this policy, ALL information processed on Bureau automated information systems, networks and the peripheral devices connected to them, shall be categorized as Sensitive But Unclassified.

3. DEFINITIONS.

Portable Electronic Device: The generic title identifying a class of small electronic devices. Typically, the capabilities of these devices go beyond their originally designed purpose. An example is the cell phone. In addition to basic telephone services, it may have one or more of the following capabilities:

- Function as a PDA;
- Connect to the Internet to retrieve electronic mail;
- Used to access the Internet; and
- Function as a pager.

Personal Digital Assistant (PDA): An electronic device designed to function as an address and/or telephone book, calendar, and calculator. The capabilities of these devices have been expanded to include paging, Internet access, audio recording, and file exchanges with a variety of computer systems.

DATE July 6, 2001

Peripheral device: (Re: automated information systems and networks) An electronic device used to receive, process and/or transmit data. Examples include printers, facsimile machines, optical scanners, PDAs, and video conferencing equipment.

Unclassified information: Information that if lost, misused; or accessed, disclosed, or modified without authority would not adversely affect the national interest, or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, US Code (The Privacy Act).

Sensitive information: Information that if lost, misused; or accessed, disclosed, or modified without authority could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be classified in the interest of national defense or foreign policy. Information classifications found in this class are Sensitive But Unclassified (SBU), For Official Use Only, Limited Official Use, and Treasury Sensitive Information.

Classified National Security Information: Information that has been determined, pursuant to Executive Order 12958 or any successor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Information classifications found in this category are Top Secret, Secret, Confidential, and Special Compartmented Information and/or Facilities (SCI/SCIF).

Virtual Private Network (VPN): A secure electronic means of connecting to one's business or office network.

4. BACKGROUND. PDAs are small, portable personal electronic devices that are vulnerable to theft and the loss or disclosure of all data contained on them. The ports technology of the PDA provides useful functionality including:

- Easy storage and retrieval of personal data;
- Personal calendaring;
- Telephone number retrieval;
- Audio recording;
- Offline and remote e-mail capability;
- Connectivity via analog or wireless modems;
- Paging; and
- Internet browsing.

The current technology also permits the user to upload, download and synchronize information with the office workstation. This procedure can be accomplished using a cable connecting the PDA to the workstation. Many PDAs also contain sound recording devices. All of these technological advances also represent vulnerabilities that require careful consideration and elements of control.

5. POLICY. As it pertains to the usage of PDAs, the aforementioned classes of information will be handled as follows:

a. Unclassified information.

For the purposes of this policy, all unclassified BEP data will be elevated to SBU and treated accordingly. Unclassified Bureau business data may only be stored on government furnished PDAs.

b. Sensitive Information.

(1) Government Owned PDAs;

- a) Government owned PDAs may be used for SBU information. Government owned PDAs may be connected to a Bureau computer or network that processes SBU information to perform file sharing and for other purposes such as updating of calendars. **Government PDAs will not be connected to any non-Bureau computer or network except as specified by this policy.**
- b) Bureau employees who are authorized to use a PDA must first attend an orientation briefing on the proper use of and the associated risks of the PDA. They will execute a statement of understanding **prior to** PDA issuance and use of a government owned PDA. An original signed statement of understanding will be executed with the CIO Directorate and a file copy will be provided to and maintained by the user's respective office.
- c) The PDA standards are established and maintained by the CIO Directorate. Only PDAs that conform to these standards may be procured.
- d) There will be two levels of PDA use within the Bureau. There will be no "in between" categories and no exceptions or variances granted. They are:
 - Level 1: Requires synchronizing via cable with user's office PC.
 - Level 2: Additionally provides remote access to BEP system resources via the Bureau Virtual Private Network (VPN). The Bureau VPN will be the only authorized means of remote access to the Bureau network. Training will be provided on the use of the VPN.
- e) User identification and level of use selection.

DATE July 6, 2001

- Each Office Chief will determine individuals who require a PDA.
- Level 1 users will be authorized by the Office Chief.
- Level 2 users must be authorized by the respective Associate Director.

- f) The PDA procurement process is as follows:
- The PDA standards are established by the CIO Directorate.
 - Each Office will procure the requisite PDAs against this standard.
 - Each Office will also be responsible for purchasing the Internet service provider (ISP) access services required for Level 2 PDAs to function.
 - Each Office is responsible for maintaining an accurate inventory of all PDAs procured, on hand, and to whom they are assigned.
 - Each Office will maintain a copy of each user's signed statement of understanding.
 - PDAs and monthly ISP contracts may be procured using credit cards assigned to Offices that are generally used to secure administrative support items.

(Note: The PDA standards will be available on the CIO page on the Bureau intranet site, In\$ite.)

- g) PDAs will be subject to random review by IT Security Division (ITSD), Office of IT Operations, Chief Information Officer Directorate (CIO) to determine adherence to policies. If the information is considered by the Bureau CIO to be highly sensitive, the information must be removed.

(Note: Contact ITSD for the current list of approved encryption software authorized for handling SBU information.)

- h) PDAs will be issued to and signed for by individual name only. No PDAs will be issued to a pool, organizational component name or activity.
- i) The PDA will be returned to the issuing Office when:
- The user no longer requires the PDA.
 - The user is transferring to another Bureau Office.
 - He/She is terminating Bureau employment.
- j) All files on Government owned PDAs are to be erased before the PDA is reissued to another individual. Bureau Office Chiefs will make appropriate arrangements with the CIO Directorate for the accomplishment of this procedure.

(2) Personally Owned PDAs.

a) **Personally owned PDAs shall not be connected to any Bureau computer or network for any purpose.**

b) Personally owned PDAs **shall be restricted from any Bureau area** where particularly sensitive data is stored or discussed.

c. National Security Information.

Treasury policy prohibits the processing or storage of National Security Information on personally owned PDAs. Under no circumstances will Classified or National Security Information be placed, processed, stored, or handled by means of a Bureau PDA.

d. Approved Models of PDAs for Government Purchase and Use.

Visit the CIO Intranet web site or contact the ITSD, for the current PDAs approved for Bureau use. Due to the rapid changes in technology, this list will be dynamic.

e. Proper Procedures on the Use of Government Owned PDAs with Government Information Systems.

(1) When powering on the PDA, all users are required to utilize the identification and password feature on their respective PDA. This feature must always be in the active mode and never disabled. Users, once logged on, shall not leave the PDA unattended when logged on.

(2) The only approved methods for accomplishing file sharing and updating calendars between workstations and PDAs are:

- Via connecting cable between the PDA to the user's workstation; and/or
- Use of a cradle, holder or other device connected to the user's workstation enabling the PDA to be synchronized.

(3) Users are not authorized to add, modify, or delete software applications contained on the PDA once issued. If the user requires changes to software configurations, a written request with justification will be required from the Office Chief to the CIO Directorate.

DATE July 6, 2001

- (4) Only Bureau approved ISPs will be used when connecting PDAs to the Internet. Visit the CIO Intranet web site or contact the ITSD for the current list of approved ISPs.
- (5) Bureau email shall be transmitted remotely only via VPN. Otherwise, all email transfers must be accomplished via the two previously described methods (in paragraph (2), above).
- (6) Government-owned PDAs are to be used for official purposes, and as authorized by ethics regulations, may be used for personal convenience.

6. WAIVERS. All sections of this policy are mandatory. No waivers will be granted.

7. RESPONSIBILITIES.

a. The Bureau users:

- (1) Will undergo a brief orientation acquainting them with the proper use of the PDA and the proper handling and storage of data, read the Bureau policy on PDAs, and execute a statement of understanding with the CIO Directorate prior to issuance and use of a government owned PDA.
- (2) Will not effect any connections of a government owned PDA to any non-government computer or network; nor connect to any classified government computer or network.
- (3) Will use proper logon and password procedures to activate each session of the PDA; and will not leave it unattended while logged on or while the PDA is active.
- (4) Will report immediately to his/her respective Office Chief any missing, misplaced, or lost equipment associated with the PDA (i.e., modem, cradle, synchronization cable) and/or missing, misplaced, or lost components (i.e., PDA, memory cards, lost or corrupted data, unintentional or unauthorized disclosure of SBU information).
- (5) Perform all file transfers and synchronizations via the Bureau approved methods.
- (6) Upon transfer or termination of employment, return the PDA to the issuing Office.

b. Office Chiefs.

- (1) If the user is **leaving the Office** that issued the PDA, secure its return.
- (2) Coordinate with the ITSD for the erasure of all data and reconfiguration of applications **before** PDA is issued to next prospective user. Prior to PDA re-issuance, ensure the prospective user has attended the security briefing on the appropriate use and risks associated with PDA use.

(Note: Simply 'deleting' the data is not adequate for this procedure.)

- (3) Determine those persons within your respective Office requiring a PDA. The respective Office Chief may approve the issuance of PDAs to those persons not requiring access to Bureau networks via remote means. Names of those persons requiring Internet access/VPN remote access function to Bureau networks shall be forwarded to the respective Associate Director for approval/disapproval. PDAs will be issued to a named individual (the actual user) only.
- (4) Perform an annual internal review of all PDAs issued by the Office. The review, which includes an inventory of PDAs and peripheral equipment, will assess and certify compliance with PDA policy. Furnish copies of these audits to the CIO Directorate. These documents will be used to maintain accountability of the PDAs.
- (5) Ensure that the theft or loss of any PDA containing sensitive information is reported to the Bureau CIO immediately.

c. Associate Directors/Deputy Director/Director.

- (1) Review requests for issuance of PDAs with remote access to Bureau networks capability. Approve/disapprove.
- (2) Prior to PDA issuance, ensure the prospective user has attended the security briefing on the appropriate use and risks associated with PDA use.
- (3) Recover PDA from user if he/she is leaving the Directorate that issued the PDA.
- (4) Coordinate with the ITSD for the erasure of all data and reconfiguration of applications before issuance to next prospective user.

DATE July 6, 2001

(Note: Simply 'deleting' the data is not adequate for this procedure.)

- (5) Determine those persons within your respective Directorate that require or need a PDA. Where access to Bureau networks via remote means is not required by the user, the respective Office Chief may approve the request. The respective Associate Director, Deputy Director or Director will review and approve/disapprove the names of persons requiring remote access to Bureau networks. PDAs will be issued only to a named individual (the actual user).
- (6) Ensure that the theft or loss of any PDA containing sensitive information is reported to the Bureau CIO.

d. Bureau Chief Information Officer (CIO).

- (1) Develop and publish protective measures as Bureau policies for the safeguarding and dissemination of SBU information processed or stored on PDAs.
- (2) Review cases where highly sensitive SBU information may exist. Make a determination and prescribe the appropriate encryption standards for the specific Bureau PDAs handling/storing the highly sensitive information.
- (3) Add the operation and security of PDAs to current security awareness programs.
- (4) Accredite PDAs in accordance with TDP 71-10 Chapter VI, Section 7.
- (5) Compile source documentation of annual internal reviews for all government owned PDAs. The annual review results shall be maintained for three years.

In the event of missing, loss, or theft of any government owned PDA, it will be immediately reported to the Departmental Office of Information Systems Security.

8. OFFICE OF PRIMARY RESPONSIBILITY. Associate Director (Chief Information Officer).

<SIGNED>

Ronald W. Falter
Associate Director (CIO)

Distribution: E