Department of Homeland Security
Management Directives System
MD Number: 11021
Issue Date: 06/29/2004

PORTABLE ELECTRONIC DEVICES IN SCI FACILITIES

I. Purpose

This Directive establishes policy and procedures for the use of Portable Electronic Devices (PEDs) and their introduction into Department of Homeland Security (DHS) Sensitive Compartmented Information (SCI) Facilities.

II. Scope

This Directive applies to all DHS personnel to include government (military and civilian) and contractors within all DHS and DHS affiliated SCI Facilities.

III. Authorities

A. National Security Act of 1947, as amended, 50 U.S.C., 401 et seq.

B. Central Intelligence Agency Act of 1949, as amended, 50 U.S.C. 403a-u

C. Executive Order 12333, “United States Intelligence Activities,” 4 December 1981

D. Executive Order 12958 as amended, “Classified National Security Information,” 3 March 2003

E. Executive Order 13011, “Federal Information Technology,” 16 July 1996

F. Federal Information Security Management Act of 2002

G. 40 U.S.C. Sections 1401-1503 (2000)

H. Director of Central Intelligence Directive (DCID) 6/3, “Protecting Sensitive Compartmented Information Within Information Systems,” 5 June 1999

I. DCID 6/3, “Protecting Sensitive Compartmented Information Within Information Systems - Industry Annex,” 1 August 2000

J. DCID 6/9, “Physical Security Standards for Sensitive Compartmented Information Facilities,” 18 November 2002

IV. Definitions

A. ***Bluetooth Technology***: A specification for low-cost, wireless communication and networking between PCs, mobile phones, PDAs, and other portable devices.

B. ***Cognizant Security Authority***: The single principal designated by a SOIC to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods, under SOIC responsibility.

C. ***Contractor Program Manager (CPM)***: Responsible for DHS activity on behalf of a contracting company in a contractor facility.

D. ***Designated Accrediting Authority (DAA)***: The official with the authority to assume formal responsibility for operating information systems at an acceptable level of risk.

E. ***Government-Furnished PED***: PEDs that are owned or leased by the U.S. Government.

F. ***Information System (IS)***: Any telecommunications and/or computer-related equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog), including software, firmware, and hardware.

G. ***Information System Security Manager (ISSM)***: The security official responsible for the IS security program for a specific Directorate, Office, or contractor facility.

H. ***Information System Security Officer (ISSO)***: The security official, either government or contractor, responsible for the security posture of a specific Information System.

I. ***Laptop***: A type of PED, usually a traditional notebook computer with a folding screen, with features similar to a standard desktop computer such as internal hard drive, standard communications and peripheral data ports, and larger in size than other PEDs.

J. ***Mission Essential PEDs***: PEDs that the DHS Program Manager approves as being required for a DHS employee or contractor.

K. ***Multi-Function PED***: A single device that has the capability to perform multiple functions such as voice and video/photo recording, Infrared (IR), and video/photo or text storage and wireless transmissions.

L. ***Personal Digital Assistant (PDA)***: A hand-held device that is a type of PED used for computing and information storage and retrieval capabilities such as calendars and address books. Some examples include Palm Pilots, Black Berries, and MP3 players.

M. ***Personally Owned Equipment***: Equipment not owned or leased by the U.S. Government.

N. ***Portable Electronic Device (PED)***: Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, processing, and/or transmitting data, video/photo images, and/or voice emanations. This definition generally includes, but is not limited to, laptops, PDAs, pocket PCs, palmtops, Media Players (MP3s), memory sticks (thumb drives), cellular telephones, PEDs with cellular phone capability, and pagers.

O. ***Program Manager (PM)***: Government manager responsible for the overall conduct of a DHS program or activity and responsible for determining if a PED is mission essential.

P. ***Receive-only Pager***: One-way text pagers that can receive messages, but are not capable of user input for transmission.

Q. ***Registration Label***: A label or bar code attached to a PED indicating that it has been approved for entry into DHS SCI Facilities because all known risks have been mitigated or accepted.

R. ***Senior Official of the Intelligence Community (SOIC)***: The heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations. DHS SOICs are the Secretary, the Deputy Secretary, The Under Secretary for Information Analysis and Infrastructure Protection, and the Assistant Secretary for Information Analysis.

S. ***Sensitive Compartmented Information (SCI)***: Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

T. ***Sensitive Compartmented Information (SCI) Facility***: An accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed.

U. ***Special Security Officer (SSO)***: Officer responsible for the overall security posture of a particular DHS program or facility on behalf of the government.

V. ***Systems Security Plan (SSP)***: The formal documentation of the security plan for a particular system.

W. ***User***: Any DHS employee, detailee, or contractor who wishes to introduce a PED into or use a PED within a SCI facility.

V. Responsibilities

A. The ***Program Manager (PM)*** will:

1. Establish the requirement for mission-essential PEDs.

2. Sign the DHS PED Registration Form for mission-essential PEDs within DHS SCI Facilities.

3. Ensure the SSO and ISSO have implemented a PED program that complies with all applicable DHS regulations and guidance and maintains up-to-date DHS mitigation procedures.

B. The ***Contractor Program Manager (CPM)*** will:

1. Establish the requirement for mission-essential PEDs within their respective contractor facility and submit a request for approval to their cognizant government official.

2. Sign the DHS PED Registration Form for mission-essential PEDs within their respective DHS SCI Facilities.

3. Ensure the SSO and ISSO have implemented a PED program that complies with all applicable DHS regulations and guidance and maintains up-to-date DHS mitigation procedures.

C. The ***Special Security Officer (SSO)*** will:

1. Provide guidance to the PM/CPM, in coordination with the ISSO/ISSM, regarding PED functionalities and associated risks for PEDs that are deemed mission essential.

2. Approve, in the absence of the ISSO/ISSM, the introduction of PEDs into DHS SCI Facilities, in accordance with this Management Directive and other applicable policies and procedures.

3. Ensure that the ISSO/ISSM has implemented procedures to validate that PED mitigation requirements are employed prior to the PEDs being used within a DHS SCI Facility.

4. Ensure that the ISSO/ISSM has implemented a process to register and track PEDs.

5. Assist the ISSO/ISSM in conducting PED audits, when required.

6. Assist the ISSO/ISSM with investigations and coordinate disciplinary actions resulting from PED security incidents.

D. The ***ISSO/ISSM*** will:

1. Manage the PED registration, briefing, and tracking process.

2. Approve the introduction of PEDs into DHS SCI Facilities, in accordance with this directive and other applicable policies and procedures.

3. Provide input to the SSO regarding acceptable mitigation and risk levels associated with the functionality of a particular device based on applicable DHS security guidance.

4. Document the process for handling PEDs, within their area of responsibility, in an applicable Systems Security Plan.

5. Maintain a listing of PEDs approved for use in their respective facilities and their functionalities.

6. Examine PEDs and ensure the user has implemented all DHS-approved risk mitigation requirements and that these are annotated on the PED Registration Form.

7. Administer, in coordination with the SSO, a random inspection program to verify conformity with mitigation standards and check for the presence of unauthorized classified information.

8. Brief users within their areas of responsibility and administer the PED User's Briefing Statement, ensuring users understand their responsibilities for using unclassified PEDs within secure areas, to include those PEDs approved for outside connectivity within secure areas.

9. Affix a barcode/registration label to approved PEDs that indicates all security requirements have been met and appropriate functionalities have been mitigated.

10. Maintain an inventory of PEDs within their area of responsibility.

11. Retrieve PEDs when the user is transferring to a new program or site, transferring to a non-DHS program, or when the PED is no longer needed and coordinate their return to the appropriate Property Officer or Program Manager.

12. Scan PEDs for unauthorized classified information and malicious code when the device is returned or prior to transferring custody to another user.

13. Take possession of PEDs that are suspected of being contaminated with classified data. Assist SSO with compiling incident reports, conducting inspections, and/or coordinating a forensics review with the DHS Office of Security, if warranted.

E. ***Office of Security, Special Security Programs Division (OS/SSPD)*** will:

1. Maintain an up-to-date familiarity with the latest PED technologies. Notify the DHS population of the consequent risks and mitigation procedures, in a timely manner, via the DHS web site and security notifications.

2. Upon request, research the capabilities and mitigation possibilities of particular PEDs. Coordinate with SSOs and notify the DHS population. This may include contact with the manufacturer and/or other Federal agencies.

3. When required, facilitate forensic reviews on PEDs, and provide reports to the responsible SSO, Personnel Security Division, and Office of General Counsel, and maintain copies of the report and supporting data within SSPD.

4. Provide guidance to all SSOs and ISSO/ISSMs regarding tools and best practices for conducting PED inspections.

5. Review this policy on an ongoing basis to ensure it reflects the appropriate guidance as it relates to the use of PEDs within DHS SCI Facilities.

6. Oversee the implementation of this policy and provide consistent guidance.

F. ***DHS Chief Security Officer (CSO)*** will:

1. Delegate approving authority for the introduction and use of PEDs within DHS SCI Facilities to the appropriate ISSO/ISSM.

2. Act as the Cognizant Security Authority (CSA) for requests to connect PEDs to other devices or systems, with approval by the appropriate DAA.

3. Consult with Chief Information Security Officer (CISO) to ensure this policy properly addresses vulnerabilities associated with state of-the-art PED technology and reflects the requirements outlined in DHS wireless policies.

4. Review this policy on an annual basis, or as required.

VI. Policy & Procedures

A. Government-Furnished Laptops and Notebook Computers:

1. Must be designated as mission essential by the Program Manager.

2. May be carried into accredited SCI Facilities.

3. May be connected to SCI Facility information systems with the approval of the site ISSM.

4. May be approved by the ISSM for classified processing purposes. If connected to a classified information system, the PED must be controlled and classified to the highest level that the information system is accredited to process.

5. Must follow appropriate accountability rules.

6. Must disable the built in microphone by inserting an adapter/erase plug into the laptop external microphone ports.

7. Must be certified and accredited for operation at a particular classification level.

8. Must follow the procedures set forth in section VI.F of this policy.

9. Laptops with wireless capabilities may be brought into accredited SCI Facilities, provided the following guidelines are followed:

a. Radio Frequency (RF): Laptops that have a wireless capability may be brought into and out of accredited SCI Facilities. However, the wireless functionality must be physically disabled. The RF capability may not be used at any time within the SCI Facility.

b. Infrared (IR): Laptops that have an infrared capability may be brought into and out of accredited SCI Facilities. However, the IR port must be covered by metal tape while in the SCI Facility area. The IR capability may not be used at any time within the SCI Facility.

B. Government-Furnished Personal Digital Assistants (PDAs) are prohibited within accredited SCI Facilities.

C. Government-furnished cellular phones are prohibited within accredited SCI Facilities

D. Government-furnished receive-only pagers are allowed within accredited SCI Facilities and do not require registration pursuant to section one of this policy. All other types of pagers and beepers are prohibited within accredited SCI Facilities.

E. Personally Owned PEDs

1. Personally owned laptops and notebook computers are prohibited within accredited SCI Facilities.

2. Personally owned PDAs are prohibited within accredited SCI Facilities.

3. Personally owned cellular phones are prohibited within accredited SCI facilities.

4. Personally owned receive-only pagers are allowed within accredited SCI Facilities, and do not require registration pursuant to section one of this policy. All other types of pagers are prohibited from within accredited SCI Facilities.

F. The following procedures are to be followed for government-furnished PEDs that are permitted in DHS SCI Facilities:

1. The Program Manager has established that the PED is mission essential. PEDs that are deemed to be mission essential by the Program Manager must be purchased and controlled by the U.S. Government.

2. Prior to entry, PEDs must be pre-approved by the ISSO/ISSM with special consideration given to the PED's functionalities and mitigation requirements. Mitigation procedures for multi-function PEDs must address all of the functions associated with the device. Examples are PEDs with cellular phone, Infrared (IR), Radio Frequency (RF), or image-capturing capabilities.

3. Immediately upon approval and prior to use, PEDs must be registered with the resident Information Systems Security Officer (ISSO), via the "PED Registration Form," which may be obtained from the ISSO.

4. Users must adhere to all mitigation measures prescribed by the ISSM/ISSO.

5. Approval/registrations will be valid until the user transfers, terminates, no longer has a need for the device; the PM determines it is no longer essential to the DHS mission; or the user intends to make modifications that could affect the PED's security profile.

6. The ISSO will affix a registration label/bar code that will be recognized by all DHS SCI Facilities as designating the PED acceptable for entry. PEDs must be appropriately labeled and controlled in accordance with applicable directives and regulations.

7. The ISSO/ISSM, in conjunction with the SSO, will establish and manage the PED process in accordance with this Management Directive and DHS SCI Administrative Security Manual for their areas of responsibility and validate mitigation requirements.

8. Any person seeking to bring a PED into a DHS SCIF expressly consents to a random inspection of the PED and to its retention if it is suspected of containing classified information, or if the device is believed to have been compromised.

9. Any person approved to bring a PED into a DHS SCI Facility will be trained on the security requirements associated with the PED being introduced into the facility.

10. Unclassified PEDs may not be connected, by any means, to any Information System that contains classified information.

11. All requests for connecting PEDs within SCI Facilities must be approved by the ISSO/ISSM, and coordinated through the SSO.

G. Devices that use Bluetooth wireless technology may not be brought into DHS SCI Facilities.

H. Devices that have audio, video, or recording capabilities may not be brought into DHS SCI Facilities.

I. PED policies may vary throughout the Intelligence and Department of Defense communities and are not always reciprocal. Prior coordination with other contractor and government sites is required prior to introducing PEDs into their SCI Facilities.

J. PEDs may be approved in certain DHS SCI Facilities, but not in others. Prior coordination is required before introducing PEDs into other DHS SCI Facilities.

K. All PEDs are subject to random inspections by security representatives. The site ISSO will develop and implement random inspections of all PEDs. In the event any PED is suspected of containing classified information without authorization, or if a PED is found to not be adhering to this directive, they are also subject to inspection by a forensics professional and/or retention by the U.S. Government. Any suspected illegal activities will be reported to the appropriate authorities for investigation.

L. Anyone found in violation of this policy will face disciplinary actions depending on the frequency of occurrence and severity of the violation, the intent of the individual, and whether or not compromise of classified information occurred. Disciplinary action may include oral and written reprimands, time off without pay, debriefing, and termination.

M. Any waivers or exceptions to this policy must be submitted in writing to the DHS Office of Security for consideration.

1. Submissions must contain a detailed description of the requested waiver or exception, a justification for the waiver, and any policies or devices that will be used to mitigate the risk of the waiver/exception.

2. Approvals of waivers and/or exceptions will be on a case-by-case basis, and will be made, in writing, by the Chief Security Officer, Department of Homeland Security.