ANNEX D

Part I - Portable Electronic Devices in Sensitive Compartmented Information Facilities

A. PURPOSE

This annex establishes Director National Intelligence (DNI) guidelines to control the introduction and use of portable electronic devices (PEDs) in sensitive compartmented information facilities (SCIFs).

The DNI recognizes that:

- PEDs may pose a risk to classified intelligence information.
- PEDs often include information processors with capabilities to interact electrically or optically with other information systems (ISs) in the accredited SCIF.

B. GUIDELINES

In conformance with DNI policy:

- The Cognizant Security Authority (CSA) and, when appropriate, the Designated Accrediting Authority (DAA) coordinate and approve the introduction/use of PEDs into a SCIF. (See section D.)
- Senior Officials of the Intelligence Community (SOICs) institute and ensure a program of appropriate mitigations (countermeasures) is in place to allow PEDs into SCIFs within the United States.

Within the United States, if the CSA determines that the risk to classified intelligence information from PEDs under their cognizance is acceptable, taking a PED into the SCIF may be allowed. A complete risk assessment addressing each component of risk as defined in section E must be completed. Only PEDs with low risk may be allowed entry to a SCIF; therefore, mitigation must be applied to PEDs evaluated to be high and medium risk to reduce the PED risk to low. These assessments could result in a CSA determination to prohibit specific PEDs. Any determination shall be applied to all SCIFs under the CSA's cognizance.

Personally owned PEDs are prohibited from processing classified intelligence information. Connecting personally owned PEDs to an unclassified information processing system inside SCIFs may only be done with approval of the DAA (Director of Central Intelligence (DCID) 6-3 8.B.6.c.2).

Government- or contractor-owned PEDs may be approved to process and/or be connected to government ISs (classified or unclassified) provided specific usage and storage is specified and accredited by DAA before introduction.

SOIC PED mitigation programs must include a formal program to implement policies and procedures governing PEDs in SCIFs under their cognizance. (See section C.)

Outside the United States, the risk to classified intelligence information is higher; therefore, personally owned PEDs are prohibited in SCIFs. If the CSA determines that mission requirements dictate a need, government- and/or contractor-owned PEDs may be permitted if the CSA determines the risk is low or by specific exception.

C. IMPLEMENTATION

This annex:

- Provides SOICs with the flexibility to establish their own mitigation programs.
- Limits risk across the IC (i.e., risk assumed by one SOIC shall not be imposed on another) by allowing the SCIF CSA or CSAs to make PED introduction determinations.
- Allows SOICs to establish portability guidelines for PEDs in SCIFs under their control.

The following levels of vulnerability are based on the functionality of PEDs, regardless of ownership. The CSA and appropriate DAA (when a portable IS is involved) will determine risk level and mitigation requirements for devices not addressed. (See section C.4.)

1. Low-vulnerability PEDs are devices without recording or transmission capabilities and may be allowed by CSAs without mitigation. They include but are not limited to:

   a. Electronic calculators, spell checkers, language translators, etc.

   b. Receive-only pagers

   c. Audio and video playback devices

   d. Radios (receive-only)

   e. Infrared (IR) devices that convey no intelligence data (text, audio, video, etc.), such as IR mouses and remote controls

2. Medium-vulnerability PEDs are devices with built-in features that enable recording or transmitting digital text, digital images/video, or audio data; however, these features can be physically disabled. Medium-vulnerability PEDs may be allowed in a SCIF by the CSA with appropriate mitigations. Examples of medium-vulnerability devices include, but are not limited to:

   a. Voice-only cellular telephones

   b. Portable ISs, such as personal digital assistants (PDAs), tablet personal computers, etc.

   c. Devices that may contain or be connected to communications modems

   d. Devices that have microphones or recording capabilities

   e. Optical technologies such as IR other than those identified in paragraph C.1.e.

3. High-vulnerability PEDs are those devices with recording and/or transmitting capabilities that cannot be adequately mitigated with current technology. The CSA may approve entry and use of government- and contractor-owned PEDs for official business provided procedural measures are in place to reduce the risk to levels established by the CSA and DAA. Examples include, but are not limited to:

a. Electronic devices with transmitting capabilities including wireless devices (WiFi/IEEE 802.11, Bluetooth, etc.)

b. Photographic, video, and audio recording devices

c. Multi-function cellular telephones

4. Mitigation Program

a. CSAs, together with DAAs, shall establish a mitigation program if high- or medium-vulnerability electronic devices are allowed into SCIFs. Mitigation programs must contain the following elements:

(1) Formal approval process for PEDs

(2) Initial and annual training for those individuals with approval to bring PEDs into a SCIF

(3) A device mitigation compliance document listing the specific portable devices, their permitted use, required mitigations, and residual risk after mitigation. (The table at Tab 2 is an example).

(4) A user agreement that specifies:

(a) The US Government (USG) and/or a designated representative may seize the electronic device for physical and forensic examination at the government's discretion.

(b) The USG and/or the designated representative is not responsible for any damage or loss to a device or information stored on personally owned electronic devices resulting from physical or forensic examination.

(5) Optional elements to enhance the protection of classified intelligence information included in the mitigation program may include:

(a) Registration programs that may include:

- Serial number
- Security requirements
- Required mitigations, reporting procedures for loss or suspected tampering

(b) Labeling for easy identification of approved devices

(c) Electronic detection equipment to detect transmitters/cell phones

b. PEDs with physically disconnected wireless capability may be connected to government systems if the PED is:

(1) Government- or contractor-owned

(2) Specified in the System Security Plan as described in DCID 6/3, Protecting Sensitive Compartmented Information Within Information Systems, for the government system to which it is connected

(3) Accredited to meet the requirements of DCID 6/3

D. EXCEPTIONS

Exceptions to this policy shall be in writing and approved by the CSA (and DAA, if appropriate). All requests for exceptions shall:

1. Be approved on a case-by-case basis based on mission requirements
2. Be coordinated with appropriate DAAs for each affected IS within the SCIF
3. Be valid for a limited, specific duration
4. Identify mitigations required, if any
5. Identify risks (after mitigation) to classified intelligence information

E. DEFINITIONS

1. Classified Intelligence Information: Information identified as sensitive compartmented information; information included in special access programs for intelligence and collateral classified intelligence information under the purview of the DNI.

2. Countermeasures: Countermeasures (mitigators) are any actions, devices, procedures, and techniques to reduce vulnerability and/or combat threats.

3. Information Systems: Any telecommunications and/or computer-related device or interconnected system or subsystem or device 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); this includes software, firmware, and hardware.

4. Portable Electronic Devices: All electronic devices designed to be easily transported and may have capabilities to store, record, and/or transmit digital text, digital images/video, or audio data. PEDs include, but are not limited to, pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, PDAs, digital audio devices, watches with input capability, and reminder recorders.

5. Risk: Risk is assessed as a combination of:

   - Threat (the capabilities, intentions and opportunity of an adversary to exploit or damage assets or information)
   - Vulnerability (the inherent susceptibility to attack of a procedure, facility, information system, equipment, or policy)
   - Probability of success of an adverse action, incident, or attack
   - Consequences of such an action (expressed as a measure of loss, such as cost in dollars, resources, programmatic effect, etc.). Risk is reduced by countermeasures.

6. Risk Management: The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.