



Department of Energy

Washington, DC 20585

JUN 6 2006

MEMORANDUM FOR ROBERT M. LINGAN
ACTING DIRECTOR
OFFICE OF SECURITY OPERATIONS
OFFICE OF SECURITY AND SAFETY
PERFORMANCE ASSURANCE

FROM:

John D. Lazor
JOHN D. LAZOR, DIRECTOR
OFFICE OF HEADQUARTERS SECURITY OPERATIONS
OFFICE OF SECURITY OPERATIONS

SUBJECT:

ACTION: Approve the Deviation Request for Introduction of Certain Portable Electronic Devices into Headquarters Security Areas

BACKGROUND:

Issues have been raised at Headquarters regarding restrictions on Portable Electronic Devices (PEDs) in security areas imposed by current policy. Responding to these issues, and recognizing the proliferation of certain PEDs, (specifically cellular telephones and BlackBerry-type devices) at Headquarters, the Office of Headquarters Security Operations has reconsidered the issue of permitting certain PEDs in security areas.

ISSUE:

DOE M 470.4-2, Chapter 4, section 1.b., Controlled Articles, states that "Portable electronic devices, both Government- and personally-owned, capable of recording information or transmitting data (e.g., radio frequency, infrared, and/or data link electronic equipment), are not permitted in LAs, EAs, PAs, Vital Areas, MAAs, SCIFs, or SAPFs without authorization."

Previously, authorization to allow cell phones to be carried (but not used) in a Headquarters' security area was implemented via the Headquarters Facilities Master Security Plan (HQFMSP). In that the above policy was published subsequent to the date of the HQFMSP, it has been determined that this issue is more appropriately addressed by a deviation than in the HQFMSP.

To compensate for the risks associated with bringing certain PEDs (those utilizing Radio Frequency (RF) technology) into security areas, the proposed deviation requires that they be placed in standby mode, powered down, or have their batteries removed, and be secured in a RF Transmission Attenuation Bag. The deviation also requires individuals who have been assigned an RF Bag to sign a User's Code of Conduct (attached) acknowledging their responsibilities.



Procedures will also be put into place to address devices brought into security areas by visitors.

SENSITIVITIES:

None. The risk of compromise due to a cell phone or BlackBerry-type device being inadvertently turned on while in a security area is felt to be adequately mitigated by the use of RF bags.

There will be a cost impact to the organizations that take advantage of the proposed deviation. Depending on the number of RF bags purchased, and which supplier is chosen, that cost may be substantial. (Note that all RF Bags must be purchased from a company approved by the HQ Technical Surveillance Countermeasures Team.)

RECOMMENDATION:

Approve the attached deviation allowing the introduction, but not the utilization, of cell phones and BlackBerry-type devices meeting specified criteria, into Headquarters Limited Areas and Exclusion Areas with the compensating measure that they be stored in RF Transmission Attenuation Bags.

DEVIATION REQUEST

Request Number HQ-06-004
(This number will be assigned by SP-21)

1. **Type of Deviation.** Waiver
2. **Directive Citation.** Department of Energy (DOE) Manual 470.4-2, dated August 26, 2005, Chapter 4, section 1.b., Controlled Articles, states:

Controlled Articles. Portable electronic devices, both Government- and personally-owned, capable of recording information or transmitting data (e.g., radio frequency, infrared, and/or data link electronic equipment) are not permitted in LAs, EAs, PAs, Vital Areas, MAAs, SCIFS, or SAPFs without authorization. DOE line management must use the following criteria in authorizing the use of this equipment:

- (1) the equipment, including those electronic devices having multiple built-in electronic recording and transmitting capabilities, is essential to the mission;
- (2) the equipment is Government-owned or -leased; and
- (3) documented risk analysis has been performed, identifying vulnerabilities inherent to the characteristics and operation of the device along with defined countermeasures.

NOTE: Authorization for use of such devices in one security area does not apply to all other security areas.

AND

DOE Manual 470.4-4, Information Security, Section e, dated August 26, 2005, Chapter 4 – Technical and Physical Security Standards, 4.c.(4), Personal Electronic Devices (PEDs), states:

Personal Electronic Devices. A PED is a generic title used to describe the myriad of electronic items that are equipped with the capabilities to process, store, transmit, receive, and/or manipulate electronic data. It has become difficult to put a label on these electronic items, because the trend is to combine all capabilities into one device. This merging of technologies has caused a re-evaluation of many of the existing policies that pertain to previously disparate types of electronic devices. PEDs are prohibited in accordance with DOE M 470.4-2, Physical Protection, "Controlled Articles," in any area subject to TSCM services as defined in chapter I, 3.b.(1)-(3) of this Section (Manual 470.4-4, Section E).

3. **Impacted Entity.** All Limited and Exclusion Areas, excluding Special Access Program Facilities (SAPFs) and Sensitive Compartmented Information Facilities (SCIFs), that fall under the purview of the Headquarters Facilities Master Security Plan (HQFMSP), dated August 2003.

4. **Deviation Justification.** In an emergency, the need for reliable communications (both official and personal) is critical. For this reason, Portable Electronic Devices, especially cellular phones and BlackBerry-type devices, have proliferated in the Headquarters community. At the same time, rising energy costs are pushing more people to mass transit. These factors, coupled with the lack of suitable storage areas (i.e., lockers) outside of security areas, lead to considering this deviation. Current DOE policy prohibits the introduction of cellular phones and BlackBerry-type devices into areas that conduct classified operations unless specifically authorized by the Cognizant Security Authority. Unprotected, these devices present a security risk for the compromise of classified information. The proposed deviation allows the introduction, but not utilization, of cell phones and BlackBerry-type devices (regardless of ownership) into LAs and EAs (excluding SAPFs and SCIFs) in facilities that fall under the purview of the HQFMSP as long as they are powered down or have their batteries removed and are secured in RF Transmission Attenuation Bags. Testing performed by the Office of Headquarters Security Operations has shown that even if one of these devices is inadvertently powered on, the RF Bags prevent it from connecting to its network.

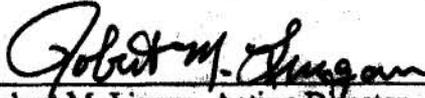
This deviation is restricted to those cell phones and BlackBerry-type devices **that do not have** built-in video recording/storage capability as these devices pose additional risks.

5. **Protective Measures.** The primary protective measure to be applied is that cell phones and BlackBerry-type devices be powered down or have their batteries removed and be secured in RF Transmission Attenuation Bags. These RF bags are designed to attenuate the RF signal generated by these devices to a level that will not allow them to connect to their networks. Additionally, the bags are opaque and will prevent cameras from taking pictures while in the bag. Depending on power and frequency of the device and the size of the security area, the ability of a covert transmitter to be effective when placed in an RF bag will be greatly reduced, rendering it almost useless. Similarly, the RF Bags, coupled with following the separation requirements set by the Certified TEMPEST Technical Authority, will greatly reduce the risk that their carrier waves will be accidentally modulated by other signals from within the security area.

Individuals who are issued RF Bags will be required to sign a user's code of conduct acknowledging their responsibilities. At that time, the HSO will issue the user an RF bag purchased from a manufacturer whose products have been tested and approved by the HQ Technical Surveillance Countermeasures team.

The HSO will also be responsible for ensuring that all visitors to their security areas follow these same guidelines.

6. **Duration.** The duration of this waiver will be 2 years from the date of the final approval.
7. **Risks.** Allowing any electronic device into a security area is a risk, especially when used by an insider determined to commit espionage-type activities. The utilization of the RF Transmission Attenuation Bags reduces the risk of unintentional compromise to virtually zero as long as the cell phones and Blackberry-type devices remain in the bag.



Robert M. Langan, Acting Director
Office of Security Operations

6 Jun 06

Date