Office of Secure Transportation
P.O. Box 5400
Albuquerque, NM 87185

AUG 1 7 2009

Directive Memorandum: 6.05

MEMORANDUM FOR: OST Federal and Contractor Employees

FROM: Jeffrey P. Harrell
Acting Assistant Deputy Administrator
Office of Secure Transportation

SUBJECT: Controlled Articles at Office of Secure Transportation Controlled Security Areas

1. **General Information**
   a. Within the Department of Energy (DOE), the term "Security Area" applies to property protection areas, limited areas, exclusion areas, protection areas, vital areas and material access areas.
   b. Failure to comply with this Directive Memorandum (DM) may result in an Incident of Security Concern.
   c. This DM applies at all OST facilities. At security areas not controlled by the Office of Secure Transportation (OST), OST personnel shall follow host site rules and procedures.

2. **Requirements**
   a. Unauthorized controlled articles shall be removed from DOE sites immediately upon discovery.
   b. The Facility Security Officer (FSO) shall be notified when unauthorized controlled articles are found within DOE/OST security areas. The FSO shall initiate the Incident of Security Concern inquiry protocol.

3. **Official List of Controlled Articles**
   Except as authorized in paragraph 4 of this document, neither portable electronic devices nor alcohol[1] are permitted in any OST security area. For purposes of this DM, portable electronic devices are both government and personally-owned devices capable of recording information or transmitting data, to include but not limited to:
   - Cameras.
   - Video Cameras.
   - Recording devices such as tape recorders.
   - Electronic devices with hard drives such as iPods, MP3 players, etc.
   - Personal computers, to include Personal Digital Assistant (PDA).

[1] May be permitted in living quarters and billets, as applicable and as specified by memorandum or SSP.

- Cellular phones[2].
- Two-way electronic communications devices.

4. Government-Owned Equipment

Government-owned controlled items may be permitted within OST security areas. The specific terms and conditions for use, if any, will be described within the applicable Site Security Plan (SSP). General terms and conditions are provided below.

a. Government-owned cellular phones and PDAs must:
   (1) Be issued in accordance with OST Policy 6.09.
   (2) Have a property accountability tag affixed to the instrument.
   (3) Have the battery removed from the device (except as noted in paragraph 4b and 4d, below) when inside security areas.
   (4) Be used for "off-site" Official Use Only communication.

b. Configuration for Recharging Cell Phones:
   (1) Batteries may be inserted in the device while it is in the charger and is recharging.
   (2) Chargers will be placed in a designated area where sensitive conversations are not allowed.
   (3) Batteries will be removed prior to issuing or returning the device to the owner.

c. Federal Agents (FA) or Contractor Transportation Utilization Personnel operating vehicles equipped with government cellular/mobile telephones must turn off these instruments and remove the battery prior to entering security areas.

d. FA performing mission duties at DOE security areas may possess government-issued communication devices unless those devices have been specifically prohibited due to site-specific requirements.

e. All mission communication devices will follow the FA Standard Operating Procedure (SOP) pre-trip, trip and post-trip requirements.

f. Requirements in the FA SOP (Chapter 3, Section 2) regarding communication safe distances when trailer vault doors are open shall be followed. The Technical Publication (TP) 45-51B providing electromagnetic radiation safe distances shall be followed. When the FA SOP and Site Specific requirements are different, the more stringent requirements shall be followed.

5. Government and personally-owned pagers

Government and personally-owned one-way (receive only) pagers are permitted in DOE/OST security areas.

---

[2] Government-issued cell phones are permitted, but the battery must be separated from the phone.

6. **Personal Cell Phone Use During Mission Status**
   Control of personal cell phones during mission status must meet the provisions of OST DM 08-001 and the current Office of Mission Operations Hot Sheet.

7. **Approval for Usage of Controlled Articles**
   A Facility Security Representative (FSR) or Facility Security Manager (FSM) may grant permission for temporary use of established controlled articles within OST security areas. The term "established" refers to controlled articles that have previously been approved for use and storage within the security area. Established controlled articles are those that are controlled by personnel who reside within the security area.
   a. Exceptions must be based on the need for mission accomplishment.
   b. Time periods must be specified.
   c. Personnel who will use the controlled article must be specified.
   d. Permission for use should be granted in writing.
   e. Personnel using the controlled article should have a printed copy of the request and permission (may be in e-mail form) and be prepared to show it if challenged.

8. **Approval to Introduce an Outside Controlled Article into an OST Security Area**
   A FSR or FSM may grant permission for temporary use of outside controlled articles within OST security areas. The term "outside" refers to controlled articles that are controlled by personnel who do not reside within the security area, such as when Headquarters personnel visit commands, or vice-versa.
   a. Approval cannot be granted for anything other than government-owned or issued audio and video recording devices, cameras, and cell phones.
   b. If the exception request is for any type of device not shown in this DM or in the SSP, the request must be denied and the device description must be forwarded to the OST FSO, for analysis.
      - OST Security Branch and/or Command and Control, Communications, Computers, Cyber Security Branch will conduct a risk-based analysis and make a determination for suitability of security area usage.