

**Office of Secure Transportation  
Policy Information**

Policy Background	
<b>Document Title:</b>  <b style="color: #800000;">Protection of Communications Equipment and Information</b>	<b>Document Number:</b> <i>(Assigned by POPD)</i> <b style="color: #800000;">OST P 6.14A</b>
<b>Document Owner(s):</b> <i>(Identify by name and organization)</i> J. Hart, VSB	<b>Policy Approval Authority:</b>  Craig A. Tucker, ADA
<b>Notify of Changes to Policy:</b> OST federal and contractor employees	
<b>Record Document(s):</b> See Internal and External Record Documents on attached.	

Policy History		
Rev	Date	Description of Change <i>(Include name of individual making the revision)</i>
0	3/05	Initial Policy. ESTD
A	05/13/08	Revised Policy to define access approvals and equipment sanitization requirements concerning communications security. J. Hart, VSB

## OFFICE OF SECURE TRANSPORTATION

### POLICY NUMBER: OST P 6.14A

**TITLE:** Protection of Communications Equipment and Information

**EFFECTIVE DATE:** 05/13/08

**PURPOSE:** This Policy establishes the guidelines for security requirements for software, hardware, frequencies, and encryption codes used to support the Office of Secure Transportation (OST) secure communications.

**SCOPE:** This Policy applies to all OST federal and contractor employees who support OST secure communication systems.

**PROPONENT:** Vehicle Systems Branch (VSB)/Engineering Systems and Technology Division (ESTD).

#### EXTERNAL RECORD DOCUMENTS:

- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information (UCNI)*

#### INTERNAL RECORD DOCUMENTS:

- CG-TSS-3, *Transportation Safeguards System Classification and UCNI Guide*
- OST P 6.13, *Non-Agent Handling of Tractors and Escort Vehicles*
- OST P 6.16A, *Off-Site Security Plan*
- OST SOP 6.00.01, *Equipment and Vehicle Sanitization for Communications Security*

### POLICY

#### 1. Objectives/Expectations

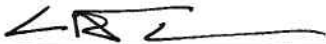
- a. Per CG-TSS-3, specific OST frequencies, Advanced Encryption Standard (AES) codes, and Data Encryption Standard (DES) codes are UCNI. This Policy addresses the requirements for access to frequency and code information and sanitization of equipment and vehicles.
- b. Access to frequencies and codes shall be limited to:
  - (1) VSB.
  - (2) OST Radio Shop personnel.
  - (3) OST Consolidated Depot personnel.
  - (4) Contractor engineering personnel.

#### 2. Responsibilities

- a. General:
  - (1) OST frequencies and codes shall be protected and secured in accordance with UCNI criteria.
  - (2) Access to specific and detailed frequency and code information shall be restricted to only those on the approved access list.

- (3) When vehicles with communication equipment are in non-mission status, such as training or liaisons and must be parked without having been sanitized, the responsible party named within the scope of this Policy must have a site security plan.
- b. Director, ESTD or designee can authorize exceptions to requirements.
- c. OST Radio Shop Managers, OST Consolidated Depot Manager, and Engineering Managers shall:
  - (1) Obtain OST frequencies and encryption codes for personnel in their respective areas through VSB.
  - (2) Sanitize OST equipment and/or vehicles as required when equipment and/or vehicles will be in the unrestricted custody of non-OST personnel.
  - (3) Provide a list of names to the Chief, VSB of personnel in their respective areas that will have access to OST frequencies and codes.
  - (4) Designate a primary and secondary point of contact on their lists.
- d. Chief, VSB shall authorize outside requests for OST frequencies and codes.
- e. VSB personnel shall provide operational and training radio-programming software, shipping software, AES and DES codes to authorized points-of-contacts.

**APPROVING OFFICIAL:**



Craig A. Tucker, Assistant Deputy Administrator  
Office of Secure Transportation

5/13/08

Date