Chapter 9
Technical Surveillance Countermeasures

This chapter covers the Technical Surveillance Countermeasures (TSCM) Program in place at DOE HQ to fulfill the requirements of DOE Manual 470.4-4A, *Information Security Manual*, Section D–Technical Surveillance Countermeasures (hereafter called the *TSCM Manual*), which is OUO and therefore is not available electronically through the DOE directives system website. A copy of the *TSCM Manual* is available through the Points of Contact listed below or by requesting a copy through the DOE directives system. It is distributed only to those authorized to receive OUO information.

Certain TSCM procedures and activities are OUO or classified and thus are not included in the HQFMSP.

The HQ Technical Security Program is assigned to AU-1.2. The TSCM Program Manager is also designated as TSCMOM for HQ.

The TSCM Program provides expert technical and analytical capability to detect, deter, isolate, and nullify technical surveillance penetrations directed at classified and sensitive unclassified information and technical security hazards within DOE facilities. It also educates employees about the TSCM Program and associated technical and physical security risks and vulnerabilities.

The TSCMOM carries out the requirements of the TSCM Program for HQ and serves as the point of contact for HQ TSCMOs. The TSCMOM must ensure that TSCMOs receive the required training to fulfill the responsibilities for their respective HQ element.

Any area or item may qualify for TSCM services or experience a TSCM incident; consequently, all HQ employees should be familiar with the TSCM Program and its procedures and requirements.

HQ Implementation Procedures

Technical Surveillance Countermeasures Officer:

The Head of each HQ element must appoint, in writing (see Attachment 900-1), a TSCMO to serve as the liaison between the TSCMOM and the HQ TSCM Team for all activities requiring TSCM support.

TSCMO responsibilities are fully identified in the *TSCM Manual*, but the following responsibilities are emphasized:

- Prior to the beginning of each fiscal year and or when an area requiring TSCM service is identified or deactivated, provide a list of these areas requiring recurring TSCM services to TSCM Program Manager as outlined in the *TSCM Manual*.

- Coordinate onsite assistance for the HQ TSCM Team to ensure strict adherence to need-to-know and OPSEC principles for TSCM activities.

- Ensure that all permanent personnel located within an area designated for a TSCM service are aware of TSCM requirements, with emphasis on reporting procedures and OPSEC.

- Coordinate unrestricted access within service areas during TSCM services.

- Coordinate the introduction of any equipment necessary for TSCM activities or services to be carried out.

NOTE: TSCMO training is provided periodically by the TSCMOM and HQ TSCM Team or upon request by a TSCMO.

Requesting TSCM Services:

Anyone may request TSCM service because of circumstance or specific events. Such a request should be made through the element's TSCMO, since possible classification issues or sensitivities are involved with the request. Information regarding an upcoming TSCM service may be classified, and information must be disseminated on a strict need-to-know basis.

All requests for TSCM services must be made in writing to the TSCMOM in AU-1.2 for approval and scheduling. A *TSCM Service Request Form*, available from the TSCMOM, can be used to request TSCM services. The *TSCM Service Request Form* can be obtained through the Points of Contact, below. A derivative classifier must review and appropriately classify all requests for TSCM services before submittal. Where unforeseen TSCM services are required and time or sensitivity is a consideration, verbal requests are authorized over a STE or in person. In either case, the request must not be made from the same area where the requested service is to be conducted or an item is to be inspected. A written request, appropriately classified, must follow a telephonic or in person request.

The requestor should make a request as far in advance as possible so that the HQ TSCM Team has time to resolve any scheduling conflicts for TSCM services. The requestor must coordinate access to the area as required by the HQ TSCM Team and ensure any other security requirements are met.

The TSCMOM validates requests for services by activity, sensitivity of information, threat, locations, etc. Requests are not necessarily validated based on classification levels of activities.

After a request has been submitted, validated, and approved, a member of the HQ TSCM Team is designated as a point of contact for the request, develops a date/time for the service, and makes any other necessary arrangements. All TSCM activities are then coordinated through the element's TSCMO and/or a designated point of contact identified in the request.

Some of the reasons to request a TSCM service in an area identified as a TSCM area may include, but are not limited to:

- Renovations or modifications to the area.
- Renovations/upgrades to equipment, furniture, and/or protection systems within the area.
- Unrestricted/unescorted access by unauthorized individuals.
- Changes to security operations procedures that could facilitate the compromise of information and material.
- Discovery or suspicion of a technical penetration, an unauthorized device, or a technical security hazard.
- Items received from foreign governments as gifts.
- Classified/sensitive briefings, conferences, meetings, and seminars.

Available TSCM Services:

TSCM services are tailored to meet local operating conditions based on the level of threat and potential vulnerabilities. TSCM services are categorized as "recurring" or "special." Recurring TSCM services are conducted on a schedule that provides the highest protection standards for highly sensitive information as outlined in the *TSCM Manual*. Special TSCM services are conducted on a non-recurring basis or for a unique reason.

The following TSCM services are available at HQ:

1. TSCM Survey – A TSCM Survey, which includes anomaly resolution and penetration investigations, is the most comprehensive of the TSCM operational activities. The TSCM Survey includes thorough instrumented, physical and visual examinations by the HQ TSCM Team to identify the presence of technical surveillance devices, technical security hazards and weaknesses, and physical security weaknesses.

2. TSCM Inspection – A TSCM Inspection is a limited activity addressing specific concerns. An inspection evaluates the changes to the operating environment and ensures that no vulnerabilities were created by modifications. Inspections also are required to assess the technical integrity of furnishings, electronic equipment,

proposed or completed construction, gifts or installation of items not previously examined by the HQ TSCM Team.

Areas subject to recurring services are required to have TSCM inspections of equipment, furnishings, etc., when items enter the facilities.

3. TSCM In-Conference Inspection – A TSCM In-Conference Inspection is a limited service, normally provided in conjunction with classified/sensitive briefings, conferences, meetings, and seminars, in an area that is not normally secured but must be employed due to the size of the specific activity or the unavailability of suitable space in secure areas. This is primarily a limited inspection of the technical attributes of the facility before, during, and (as necessary) after the activity.

   The requester must coordinate access to the area as required by the HQ TSCM Team and ensure that any other security requirements/approvals are met and that any required security measures (e.g., seals on the doors, signs, sealing doors at night, escorts) are completed.

4. TSCM Advice and Assistance – TSCM Advice and Assistance is a service conducted before and or during construction or renovation of a new or existing area to ensure that appropriate physical and technical security standards or vulnerabilities are addressed prior to procurement to avoid costly modifications. This service is also appropriate prior to the purchase, replacement, installation, and going "live" with electronic systems, such as video teleconferencing systems and telephone systems.

   This service includes a review of proposals, blueprints, plant-in-place records, as-built drawings, or any documentation in place before and during construction.

5. TSCM Education – TSCM educational efforts include presentations, briefings, literature, or other means by which the HQ personnel become familiar with the TSCM Program and the technical threat to their facilities, equipment, or activities to minimize the possibility of compromising sensitive information.

6. Special TSCM Services – These services occur infrequently. They are conducted to meet unforeseen circumstances or protection needs according to conditions of local threat or vulnerabilities, regardless of classification level, and are usually event driven. These services do not nullify the requirements of other security disciplines where a temporary increase in protection levels must be applied because of the specific nature of the activity (classified or sensitive).

TSCM Policies:

Application and recommendations of the technical and physical security standards for special service areas and services are subject to the discretion of the TSCMOM, based on recommendations of the HQ TSCM Team.

All items and systems (personal and government-owned) located in an area undergoing a TSCM service is subject to inspection by the HQ TSCM Team. If an item is found to be compromising information, the device is subject to confiscation. The item may be sent to a laboratory for analysis, including destructive analysis, if necessary.

Activities or events that prevent the adequate conduct of the service required or requested may be terminated by the HQ TSCM Team and will be annotated in the TSCM activities report.

A TSCM service is considered compromised when individuals, associated with or located within the area where the service is being conducted, carelessly or deliberately make reference to the fact of the service, including use of abbreviated and familiar terms (bugs, sweeps, taps, etc.). Such compromises, whether inadvertent or deliberate, may result in a security infraction. The HQ TSCM Team Chief determines whether a TSCM service has been compromised. In the event of a compromise, termination of the service may be necessary and will be annotated in the TSCM service report.

Discovery or Suspicion of a Technical Surveillance Device:

Discovery of a technical surveillance device or system or suspicion of the existence of such a device or system in any HQ or DOE contractor facility in the Washington, DC area must be reported immediately to the TSCMOM. The report should be made in person but may be made via a STE phone. The report must be made from outside the facility where the suspected surveillance exists. Do not voice the discovery within the immediate area, which includes the suspect room and all other rooms/areas above, below, and adjacent to it. Secure the area to preclude any attempts to remove the discovered device(s) and continue normal activity in the area without discussing classified information. The TSCMOM will provide further instructions on how to proceed.

A Special TSCM Service is requested immediately upon the discovery of any technically hazardous condition, regardless of the type of facility where the condition was discovered.

Points of Contact

For the names and contact information for the positions identified in this chapter, call (301) 903-3510 or (301) 903-2644.

Forms/Samples/Graphics

Sample Appointment Memorandum (see Attachment 900-1)

ATTACHMENT 900-1

Sample Appointment Memorandum

MEMORANDUM FOR (NAME), DIRECTOR
OFFICE OF HEADQUARTERS SECURITY OPERATIONS
OFFICE OF HEALTH, SAFETY AND SECURITY

FROM: (NAME)
NAME OF ELEMENT

SUBJECT: Appointment Memorandum for (Enter name of organization)

This memorandum notifies you of the (enter name of element) employees appointed to the following security-related positions:

Headquarters Security Officer (HSO) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Alternate HSO(s) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

HSO Representative(s) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Operations Security (OPSEC) Representative - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Alternate OPSEC Representative - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

Technical Surveillance Countermeasures Officer (TSCMO) - (Enter Employee's Name), Organization Code, Room Number, Phone Number, Fax Number, E-mail Address

cc: HSO
Alternate HSO(s)
HSO Representative(s)
OPSEC Representative
Alternate OPSEC Representative
TSCMO
Office of Information Security, AU-42
Office of Corporate Security Strategy, Analysis and Executive Protection (AU-1.2)