Chapter 9 Revision History: Revisions by date (Newest to oldest):

July 22, 2024: Chapter was reformatted to be in alignment with the Chapter Guide.

April 15, 2024: Updated office code to EHSS-54 and changed “OUO” references to “CUI.”

March 20, 2021: Added Attachment 900-4 *Modified Secure Phone Work Order*

February 2, 2021: Added Attachment 900-3 *Medical Device Worksheet*

September 3, 2019: Revised “Points of Contact”

November 2, 2018: Revised “Available TSCM Services” section

November 2, 2018: Added Attachment 900-2 *TSP Gift Review Worksheet*

October 16, 2018: Added revised Attachment 900-1 *Equipment Worksheet*

October 16, 2018: Attachment 900-1 removed.

June 28, 2017: Updated Points of Contact

Chapter 9
Technical Surveillance Countermeasures

This chapter of the U.S. Department of Energy (DOE) Headquarters (HQ) Facilities Master Security Plan (HQFMSP) describes technical security requirements and processes for requesting technical security services at DOE HQ facilities. Additionally, personnel responsibilities are detailed below and must be followed to ensure the safeguard and security of classified information. The requirements within this chapter are the implementation of *DOE Order 470.6, Technical Security Program* (TSP) and various national policies. This chapter is applicable to all DOE personnel, visitors, and tenants located in DOE HQ areas where classified information is discussed, processed, viewed, or stored. This chapter is maintained by the Office of Technical Security (OTS), EHSS-54.

Section 901 – TSP Support Services and Request Processes

Section 902 – TSP Requirements for Headquarters Elements

Section 903 – TSP Requirements for Personnel with Access to Classified Areas

Attachments – Listing of DOE HQ Technical Security Services Request Worksheets

Definitions:

Certified TEMPEST Technical Authority (CTTA): An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with the Committee on National Security Systems (CNSS) approved criteria and has been appointed by the head of a U.S. Government Department, Agency, or designee to fulfill CTTA responsibilities.

Communications Security (COMSEC): Designed to protect and control the means and materials used to provide encrypted communications.

Compromising Emanations (CE): Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information system equipment.

Controlled Cryptographic Item (CCI): Secure telecommunications or information system, or associated cryptographic component, that is unclassified and handled through the COMSEC Material Control System (CMCS), an equivalent material control system, or a combination of the two that provides accountability and visibility. Such items are marked “Controlled Cryptographic Item”, or, where space is limited, “CCI.”

Medical Electronic Device (MED): Medically prescribed electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to: hearing aids, blood glucose monitors, external heart monitors, etc. These devices should not be confused with life-saving devices such as implanted defibrillators or pacemakers.

Officially Designated Federal Security Authority (ODFSA): Federal employees that possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation. The ODFSA is charged with responsibility for physical, technical, personnel, and information security matters affecting the location identified in the delegation.

Delegation authority for these positions is originated according to direction from the accountable Undersecretary who also provides direction for further delegation of the ODFSA designations. All delegations of authority must be documented in writing.

Portable Electronic Device (PED): Electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to: pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders.

Protected Distribution Systems (PDS): Designed to protect unencrypted classified signal/data lines that exit secure areas and traverse through areas of lesser security.

Technical Surveillance Countermeasures (TSCM): Designed to detect, deter, isolate, and nullify technical surveillance penetrations and technical security hazards.

Technical Surveillance Penetrations: Any instance of information leaving an area by unauthorized technical means for monitoring by unauthorized entities, either through installation of a technical surveillance device, manipulation of software, interception and monitoring of fortuitous emanations, or intentional creation of a hazard.

TEMPEST: Designed to prevent the unauthorized intercept of compromising emanations that may be present in information processing communication equipment, systems, and components. A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

Wireless Security (WiSec): Designed to test/evaluate the impact of mobile and fixed wireless communication devices used in or near classified and sensitive unclassified activity areas for the purpose of determining risks and countermeasures.

Section 901
TSP Support Services and Request Processes

The Office of Technical Security (OTS), EHSS-54 provides operational support for technical security activities at HQ facilities. Support includes TSCM, TEMPEST, WiSec, PDS, and COMSEC. Personnel who frequent DOE HQ locations must be familiar with HQ technical security requirements to ensure the protection of classified information.

Technical Surveillance Countermeasures

TSCM services are tailored to meet local operating conditions based on the threat level and potential vulnerabilities. TSCM services are conducted by the HQ DOE technical security team with oversight from the Office of Technical Security Team (OTS), EHSS-54.

The following TSCM services are available at DOE HQ facilities:

- **TSCM Survey** – A TSCM Survey, which includes instrumented anomaly resolution and technical penetration investigations, is the most comprehensive of the TSCM operational activities. The TSCM Survey includes a thorough technical, physical, and visual examination of the area to identify technical and physical security hazards and the presence of technical surveillance devices.

- **TSCM Inspection** – A TSCM Inspection is a limited activity addressing specific concerns. An inspection evaluates the changes to an operating environment to identify if vulnerabilities were inadvertently created due to modifications or upgrades of the area. Inspections 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 DOE HQ technical security team. Medical devices are considered electronic equipment and must be inspected prior to bringing these items into a Limited Area (LA), Vault-Type-Room (VTR), or a Sensitive Compartmented Information Facility (SCIF) – Attachment 900-3 OTS WS - Medical Device Review Worksheet. Areas subject to recurring services are required to have TSCM inspections of equipment, furnishings, etc., when items enter the facilities – Attachment 900-1 OTS WS – Equipment Inspection Request Worksheet. TEMPEST and TSCM item inspections are usually accomplished simultaneously.

- **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.

- **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.

- **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.

- **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).

Request Process: It is critical that TSCM requests are appropriately controlled to ensure the integrity of the TSCM service. **TSCM SERVICES AND REQUESTS ARE GENERALLY CLASSIFIED AND WILL REQUIRE REVIEW BY A DERIVATIVE CLASSIFIER PRIOR TO SUBMISSION.** Foregoing the derivative classifier review could result in a classified information spillage resulting in a security infraction. Routine and general requests for TSCM services should be submitted via the DOE HQ TSCM Service Request worksheet Attachment 900-5 OTS WS – TSCM Service Request through the elements TSCM Officer (TSCMO). Requests should be made as far in advance as possible to account for scheduling conflicts. Telephonic or in-person requests for time sensitive TSCM services are authorized; however, must **NOT** occur in the area where the service is to be conducted (refer to section 903 of this chapter for specific requirements), must occur over a classified medium, and must be followed with a written request using the DOE HQ TSCM Service Request worksheet. Discussions and emails of pending TSCM activities must **NOT** occur in the requested inspection area prior to the service.

After a request is submitted, validated, and approved by the OTS, a member of the DOE HQ technical security team will coordinate details of the service with the TSCMO or designated point of contact identified in the request.

NOTE: All items and systems (personal and government-owned) located in an area undergoing a TSCM service are subject to inspection by the DOE HQ technical security team. All unauthorized items presenting a vulnerability are subject to confiscation. The item may be sent to a laboratory for analysis, including destructive analysis, if necessary.

TEMPEST

TEMPEST is the study of unintentional CE, which is produced by all electronic / electromechanical telecommunications and automated information processing equipment. These emanations may possess intelligence-bearing information, that if intercepted and analyzed, may disclose classified information.

The following TEMPEST services are available or are required at DOE HQ facilities:

- **TEMPEST Reviews –** Classified facilities, information systems, activities, and discussion areas, will be evaluated by a CTTA to determine compliance with CNSS policies and what, if any, TEMPEST countermeasures are necessary.
    - TEMPEST Reviews are required:
        - TEMPEST facility countermeasure reviews must be conducted by a CTTA annually.
        - If wireless technologies operate within 100' of areas where classified information is discussed or processed.
        - Prior to the procurement of National Security Systems; computers, laptops, printers, servers, etc.
        - Prior to construction or modification of a facility or area designated to process classified information.
        - Upon a change in approved classified activities.
        - Additions or changes to National Security Systems equipment.
        - Reviews may also be required due to a change in threat level or national policy.
- **TEMPEST Inspection –** Electrical/Electronic equipment, Portable Electronic Devices (PEDs) and Medical Electronic Devices (MEDs) with wireless, recording, or microphonic technologies must be reviewed prior to entering a security area. TSCM and TEMPEST item inspections are often conducted simultaneously by the DOE HQ technical security team or CTTAs.

Request Process: Request for TEMPEST reviews or inspections can be accomplished by submitting the appropriate request (Attachments 2,3,4) to TecSec.

NOTE: TEMPEST plan development and reporting must be accomplished in accordance with the TEMPEST checklist for SCIFs, regardless of the classification of the designated space, contained within the IC Technical Specifications for Construction and Management of SCIFs or successor documents when appropriate

Wireless Security (WiSec)

WiSec is generally referred to the protection of wireless National Security System (NSS) information, most notably classified and unclassified wireless access points, but also encompasses wireless devices in proximity to areas where classified information is discussed, displayed, or processed.

Transmitters to be installed within classified facilities, buildings, etc., or in proximity to classified facilities, must not be installed, or powered on until the CTTA has conducted a review and the cognizant security authority has accepted any residual risk in writing.

The following WiSec services are available at DOE HQ facilities:

- **Transmitter Reviews –** Unclassified and classified transmitters reviews must be conducted within DOE HQ facilities, to include tenants, for transmitters that will operate within 100' of classified systems, activities, or discussion areas.
    - Only approved CIO provided wireless access points and cellular repeaters are authorized at HQ facilities. Cellular Hotspot and personally owned wireless access points are not authorized in HQ facilities.

Request Process: It is the requestors responsibility to submit a completed transmitter review request Attachment 900-4 OTS WS – Transmitter Review Worksheet to TecSec.

Protected Distribution Systems

PDSs are designed to protect unencrypted classified signal/data lines that exit secure areas and traverse through areas of lesser security.

PDS's must be approved by the ODFSA and maintained in accordance with CNSSI 7003. Installation of a PDS should **NOT** be common practice and only used as a last resort to meet mission requirements.

Request Process: Contact TecSec with questions related to PDS requirements.

Communications Security

EHSS-54 is the DOE Central Office of Record (COR), the Command and Controlling Authority of all COMSEC material and activities for DOE to include NNSA. EHSS-54 provides information and requirements for the operation and maintenance of DOE, to include NNSA, secure communications activities for the acquisition, storage, assignment, distribution, inventory, control, and accountability of COMSEC material applicable to COMSEC activities of DOE federal and contractor employees.

Some COMSEC equipment is designated as controlled cryptographic items (CCI) and must be accounted for by element COMSEC personnel. These items include secure telecommunications, such as ViPer desktop phones, information systems, or associated cryptographic components. Additional information regarding secure desktop phones can be found in Chapter 2 of the HQFMSP.

Section 902
TSP Requirements for Headquarters Elements

The Head of each HQ element must appoint, in writing, a TSCMO to serve as the liaison between the EHSS-40 and the DOE OTS for all activities requiring TSCM support.

TSCMO responsibilities are fully identified in DOE O 470.6, *Technical Security Program*, 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 EHSS-40 as outlined in the Memorandum of Agreement between the OTS, EHSS-54 and EHSS-40.

- Coordinate onsite assistance for the DOE HQ technical security team to ensure strict adherence to need-to-know and Operations Security (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 OTS, DOE HQ technical security team or upon request by a TSCMO.

Section 903
TSP Requirements for Personnel with Access to Classified Areas

Adherence to technical security protocols by personnel and visitors that frequent DOE HQ facilities is integral to the success of the technical security program. The unintended introduction of controlled/prohibited articles or audible comments of TSCM operational activities could result in the compromise of classified information or a classified activity. Alternatively, personnel and visitors at DOE HQ facilities are ideal reporters to changes in their daily working environments. These keen observers can detect subtle changes in their work areas which may be indicative of a concealed technical surveillance device.

Prompt and discrete reporting is required when addressing a suspected technical surveillance device to ensure the integrity of a thorough technical investigation. The success of most technical security activities requires strict adherence to OPSEC practices. The below are requirements of all personnel and visitors that frequent DOE HQ facilities:

OPSEC

OPSEC is a systematic and proven process intended to deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: (1) identification of critical information; (2) analysis of threats; (3) analysis of vulnerabilities; (4) assessment of risks; and (5) application of appropriate countermeasures. OPSEC practices are a critical component to the DOE technical security program and must be exercised by all DOE contractors, employees, and visitors.

- TSCM activities are generally classified and must be restricted to personnel with the appropriate clearance and need-to-know as established by the DOE OTS Director or staff when delegated by the OTS Director.

- Never discuss TSCM services in areas where the TSCM activity will occur.

    - If a concealed surveillance device was present in the area, the adversary would become aware of the TSCM service and power off the device making it infinitely more difficult to detect.

- Never audibly acknowledge ongoing TSCM activities.

    - Do not ask questions about TSCM equipment or make comments referring to; sweeps, bugs, ghosts, etc. These actions could result in the termination of the TSCM service and a security infraction.

- Always maintain a normal working environment during TSCM activities.

  - Keep computers, printers, and other information technology systems powered on.
  - Do not excuse yourself from the work area due to the TSCM survey.

- If you need to speak with the TSCM technician during a TSCM service, write your question on a piece of paper and hand it to the technician. The technician will respond in writing or accompany you outside the survey area to further discuss this issue.
  - All TSCM services are conducted by cleared personnel and approved by the DOE HQ ODFSA.

Discovery of a Suspected Technical Surveillance Device

Discovery of a technical surveillance device, or suspicion of the existence of such a device in any DOE HQ facility, to include tenant areas, must be reported immediately to the OTS, EHSS-54 The report should be made in person but may be made via a secure/encrypted medium such as a STE or ViPer phone. The report must be made from outside the facility where the suspected surveillance device 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. OTS, EHSS-54 will provide further instructions on how to proceed.

A TSCM Survey is requested immediately upon the discovery of a technical surveillance device or evidence that a technical surveillance device was present, regardless of the type of facility where the condition was discovered.

TSCM/TEMPEST Item Inspections

Controlled Articles: items that possess cameras, microphones, storage, recording capability, or wireless technologies are prohibited in classified discussion, viewing, and processing areas unless approved by the DOE HQ ODFSA. Controls to mitigate the threat posed by these devices range from administrative to prohibition and must be approved by the DOE HQ ODFSA. Personnel working in classified areas must submit a completed item inspection request (Attachment 900-1 OT WS – Equipment Inspection Request Worksheet) to TecSec for all items listed in the Controlled Articles Matrix found in the HQFMSP Chapter 2 attachments. **NOTE**: There are additional inspection requirements listed below specific to TSCM areas. These items are not permitted into security areas until the inspection is completed and any residual risk is accepted in writing by the DOE HQ ODFSA.

Please note the following additional information related to TSCM/TEMPEST inspections and controlled articles:

- Personnel working in TSCM areas must submit inspection requests through their TSCMO or HSO for inspections of personal and government owned office furnishings which includes electronic devices, appliances, furniture, etc.

- Requests must be initiated for medical devices with cameras, microphones, storage, recording capability, or wireless technologies.
    - Life-saving devices such as implanted defibrillators must be declared via Attachment 900-3 OTS WS – Medical Device Review Worksheet and will be administratively reviewed.
- Requests must be submitted for gifts received from non-US personnel whose relationships were developed during official business, or when the item was received through unusual circumstances (provided by a stranger, left in hotel room, discovered in luggage, etc.), regardless of electronic/electric capability.
- DOE provided electronics that have not previously been inspected must be inspected to determine if mitigations are required or sufficient.
- Requests are required for equipment that will process or destroy classified information; classified printers, shredders, scanners, etc.
- All wireless transmitters that will operate within 100' of classified activities (may also require an Attachment 900-4 OTS WS - Transmitter Review Worksheet).
- Technical security personnel are authorized to confiscate and conduct destructive and non-destructive examinations of devices, to determine if the device poses a threat to classified or sensitive information.

Desktop VTCs

- Desktop VTCs must be approved in accordance with the DOE HQFMSP, Chapter 2.
- Desktop VTCs must be installed, configured, and comply with CNSSI 5000, Annex J, *Softphone Security Requirements,* or successor documents.
- Desktop VTCs approved for use in classified areas must have a TSG disconnect device between the computer and camera/headset.
- Desktop VTCs must use approved TSG devices as specified in the TSG-6 Telephone List. **NOTE:** The TSG-6 Telephone List is usually updated monthly via email distribution and the online link is not always the most current. Contact the DOE HQ technical security team for the current listing.

COMSEC

- In the event of *suspected* loss of possession, control, or physical compromise of COMSEC items (CCI, ViPer, etc.), the DOE OTS, EHSS-54 will be notified immediately. At the DOE OTS's discretion, a formal report must be completed by the COMSEC account custodian in accordance with national policies.

- **Secure Desktop Communications**
    - Secure desktop phone (ViPer, etc.) users may not connect, disconnect, reconfigure, transfer, or relocate these devices on their own. These actions may only be performed by authorized personnel affiliated with the DOE OTS and are coordinated between the DOE HQ element HSOs and the DOE HQ Secure Phone Group via email to HQ Secure Phone using the Attachment 900-6 - Secure Phone Work Order Request.

Points of Contact

For TSCM, TEMPEST, PDS, WiSec or General technical security requests and support, email TecSec or call 202-586-8437 / 301 903-9992 / 301 903-6581.

For secure phones support (maintenance, installation, removal), email HQ Secure Phone or call 301-903-6581 / 301-903-5062.

For all COMSEC specific inquiries, email Telcom Security or call 301-903-6581 / 301-903-8317.

Attachments

900-1 OTS WS – Equipment Inspection Request Worksheet
900-2 OTS WS – Gift Inspection Request Worksheet
900-3 OTS WS – Medical Device Review Worksheet
900-4 OTS WS – Transmitter Review Worksheet
900-5 OTS WS – TSCM Service Request
900-6 OTS WS – Secure Phone Work Order Worksheet