Chapter 2
Limited Areas, VTRs, and Temporary Limited Areas

Chapter 2 describes the security procedures adopted by DOE HQ to implement the requirements of the following DOE directives:

- DOE Order 473.3, *Protection Program Operations*
- DOE Order 471.6, Change 1, *Information Security*
- DOE Order 475.2A, *Identifying Classified Information*
- Classification Bulletin TNP-32, *Classification Guidance for Classified Meeting Locations at DOE/NNSA or DOE/NNSA Contractor Sites or Facilities*, dated May 27, 2010

DOE Manual 470.4-2A, *Physical Protection*, defines seven types of Security Areas that protect DOE employees, facilities, buildings, government property, classified information, nuclear materials and other security interests. Each type of Security Area has its own security requirements, such as access controls, alarms, vehicle controls, construction standards, operating procedures, etc. The seven types of Security Areas include:

- General Access Areas
- Property Protection Areas
- Limited Areas (LAs)
- Vault-Type Rooms (VTRs)
- Special Designated Security Areas
- Protected Areas
- Material Access Areas

All HQ facilities have General Access Areas and Property Protection Areas; however, only the Forrestal, Germantown, and 955 L'Enfant Plaza facilities have LAs, VTRs, and Special Designated Security Areas. At HQ, Special Designated Security Areas consist of Sensitive Compartmented Information Facilities (SCIFs) and Special Access Program (SAP) facilities. LAs, VTRs, and Special Designated Security Areas are not currently permitted in HQ facilities other than the Forrestal, Germantown, and 955 L'Enfant Plaza facilities. There are no Protected Areas or Material Access Areas at HQ.

DOE HQ has also established an LA sub-type area known as a Temporary Limited Area (TLA), which protects classified information for short periods of time. For example, a TLA may be established to allow a senior Departmental official to review classified information in his/ her office, or when an LA is undergoing renovation.

Because of common, local usage, the term “Security Area” at HQ has come to mean an LA, VTR, or TLA.

Chapter 2 describes the processes required to establish, operate, maintain, and deactivate LAs, VTRs, and TLAs at DOE HQ:

- Section 201 describes the procedures for establishing, maintaining, and deactivating LAs, VTRs, and TLAs.

- Section 202 identifies “Controlled Articles,” which are items that are not permitted (or that must remain under strict control) within an LA, TEMPEST Protected Area, or VTR.

- Section 203 describes the procedures for holding classified discussions and meetings in LAs and VTRs.

- Section 204 covers holding classified meetings in locations not pre-approved for classified discussions.

- Section 205 discusses how to obtain Secure Telecommunications Equipment (phones) and other Communications Security services.

HQ security procedures for Special Designated Security Areas (SCIFs and SAP facilities) are described in other security plans with a limited distribution and are not discussed in this HQFMSP.

Section 201
Establishing, Maintaining, and Deactivating LAs, VTRs, and TLAs

Classified matter must be processed, discussed, handled, or stored in designated LAs, VTRs, or TLAs. LAs, VTRs, and TLAs must have security measures in place to detect and deter unauthorized persons from gaining access to the classified matter. This includes measures to prevent unauthorized persons from seeing or hearing classified information. All LAs, VTRs, and TLAs at HQ must be approved by the Office of HQ Security Operations (AU-40) prior to the initiation of classified activities or the introduction of classified material or equipment.

Definitions of LA, VTR, and TLA:

1. Limited Area (LA) – An LA is a Security Area that protects classified matter. LAs are defined by physical barriers encompassing the designated space and have access controls to ensure only authorized personnel enter and exit the LA. A means must be provided to detect and deter unauthorized entry into the LA. In some instances, an LA may also be approved for processing, destroying, reproducing, transmitting or receiving, and discussing classified information.

2. Vault-Type Room (VTR) – A VTR is a DOE-approved room having combination-locked doors and protection provided by a Department-approved intrusion alarm system activated by any penetration of walls, floors, ceilings, or openings, or by motion in the room. Typically, VTRs are used for the open storage of classified materials, equipment, and components up to and including Secret/Restricted Data (S/RD). In some instances, they may also be approved for processing, destroying, reproducing, transmitting or receiving, and conducting amplified discussions of classified information.

   NOTE: As a general rule, the open storage of TS/RD is not approved at HQ facilities.

3. Temporary Limited Area (TLA) – A TLA may be established when it is necessary to review classified information for a limited time period in a room that is not an already approved LA or VTR. Usually, TLAs are established while an LA or VTR undergoes construction or when a cleared employee needs to review classified information no higher than S/RD for a brief period of time. The security measures for a TLA are determined on a case-by-case basis and must be approved by the HQ Classified Matter Protection and Control (CMPC) Program Manager prior to any classified activities taking place in a TLA.

Documenting the Process:

The LA/VTR approval process is documented from initial visit through deactivation. A file for each LA or VTR is created and maintained by the HQ Survey Team within the Office of Information Security (AU-42). Each file contains all the documentation for the review, approval, changes, and deactivation for the LA or VTR. The HQ Survey Team maintains pertinent information about each LA and VTR in the HQ Security Area Database.

NOTE: The Director, AU-42, approves LAs and VTRs based upon the requirements set forth in DOE directives. In cases where all security requirements cannot be met, an Equivalency or Exemption may be requested (see Chapter 16, Equivalencies and Exemptions).

HQ Implementation Procedures

Establishing a New LA or VTR:

When an HQ element determines that a new LA or VTR is required, the following actions must be taken:

- The element HSO submits to AU-42 a Security Area Request Package requesting an Advice and Assistance visit to prepare for the establishment of a new LA or VTR. The Security Area Request Package consists of a memorandum requesting assistance in establishing a new LA or VTR along with two attachments: a Security Area Request/Facility Information Worksheet and a blueprint/drawing of the proposed LA or VTR. Attachments 201-1 and 201-2 provide a sample memorandum and the Security Area Request/Facility Information Worksheet. The drawing can be a copy of a blueprint or a simple, hand-written sketch of the area.

- AU-42 forwards the Security Area Request Package to the HQ Survey Team within AU-42. The HQ Survey Team conducts the appropriate physical security review and walk-through of the proposed LA or VTR before providing an Advice and Assistance Report to the element identifying the physical protection measures needed. It is the element's responsibility to arrange for and complete any needed construction or other physical changes to the proposed LA or VTR.

- Requirements for Technical Surveillance Countermeasures (TSCM) services are determined based upon the activities that will take place within the proposed area. If the area requires TSCM services, the HQ Survey Team coordinates with the HQ TSCM Program Manager to obtain those services.

- The HSO notifies the HQ Survey Team by e-mail when the physical security upgrades are complete. The HQ Survey Team inspects the LA or VTR to verify that all physical protection requirements are met. The HQ Survey Team then provides a Security Area approval memorandum and "Security Area Approval Certificate" to

the requesting HQ element. A sample Security Area Approval Certificate is shown in Attachment 201-3.

- When an LA or VTR has been accredited, the Security Area Approval Certificate must be prominently displayed inside the area, preferably near the main entrance.

Establishing TLAs:

Occasionally, an organization may request to review classified information on a limited basis in a location not yet approved as an LA or VTR. If the proposed location, classified activity, and alternative protection measures establish that the classified information can be protected as it would in an approved LA or VTR, the Program's HSO may request approval of a TLA to review classified information up to but no higher than S/RD.

To request approval for a TLA, an HSO must complete a Security Plan for the proposed area. Attachment 201-4 provides a Sample Security Plan for TLAs. The Security Plan must be signed by the employee(s) who will be working in the TLA and the requesting HSO, and submitted to AU-42 for approval by the HQ CMPC Program Manager.

The request for the TLA is approved by AU-42 on a case-by-case basis after careful analysis of the information described in the Security Plan. If the analysis determines that the classified information can be protected as it would be in an approved LA or VTR, approval may be granted.

Maintaining LAs, VTRs, and TLAs:

After an LA, VTR, or TLA has been approved, two situations may affect its continued ability to remain accredited:

- Physical changes, such as adding or rearranging large items of furniture or equipment, may affect the integrity of the space.

- LAs, VTRs, and TLAs are approved for specific classified activities at specific classification levels and categories. If different classified activities must be performed or there is a change in the classification level or category of the classified matter to be handled within the LA, VTR, or TLA, a new survey and *Security Area Approval Certificate* is required.

In either case, the element's HSO submits a new Security Area Request Package, as described above, to AU-42. The memorandum will briefly state the nature of the modification to the LA, VTR, or TLA and have a Security Area Request/Facility Information Worksheet attached. AU-42 forwards the Security Area Request Package to the HQ Survey Team for action.

The HQ Survey Team conducts the appropriate physical security review and takes one of the following actions:

- If the security posture of the area is unaffected by the physical changes, no further action is required and a memorandum stating this fact is transmitted to the HSO of the requesting HQ element.

- If the security posture of the area is affected by the proposed physical changes, an Advice and Assistance Report identifying the required physical protection measures is transmitted to the HSO of the requesting HQ element. Once the HSO determines all work necessary to bring the area into compliance has been satisfactorily completed, the HQ Survey Team is notified by e-mail. The HQ Survey Team conducts a follow-up review or walkthrough of the area and issues a new Security Area approval memorandum and Security Area Approval Certificate that are transmitted to the requesting HSO. Once reaccredited as an LA, VTR, or TLA, the new *Security Area Approval Certificate* must be prominently displayed inside the area, preferably near the main entrance, and all superseded certificates destroyed or returned to the HQ Survey Team.

  NOTE: If the physical changes affect the ability of the area to continue classified activities and no compensatory measures are feasible, the LA, VTR, or TLA must be deactivated. All classified activities must cease or be relocated to an accredited Security Area until identified physical protection measures have been implemented and the area re-approved.

  NOTE: If the change in activities requires the Security Area to become a TSCM serviced area, the HQ Survey Team forwards the request to the TSCM Operations Manager for appropriate action; this may require the element's TSCM Officer to submit a new request following the procedures established in Chapter 9, Technical Surveillance Countermeasures.

Deactivating LAs, VTRs, and TLAs:

When an LA, VTR, or TLA is no longer required, all classified matter must be destroyed or relocated to another approved LA, VTR, or TLA, and all classified activities must cease. The HSO of the element takes the following steps to complete the deactivation:

- Submit a new Security Area Request Package, as described above, to AU-42. The memorandum will briefly state that an existing LA, VTR, or TLA requires deactivation and have a Security Area Request/Facility Information Worksheet attached. AU-42 forwards the Request Package to the HQ Survey Team for action.

- The HQ Survey Team conducts a review of the LA, VTR, or TLA to ensure all classified matter has been removed and all classified activities have been terminated. When satisfied, the HQ Survey Team transmits a memorandum to the element's

HSO approving the deactivation of the LA, VTR, or TLA. A copy of this memorandum is provided to the Office of Physical Protection (AU-41).

- When the HSO receives the deactivation approval memorandum, all intrusion detection and access control equipment can be removed. The HSO must confirm that removal has been satisfactorily completed and then e-mail the HQ Survey Team advising of that completion. The HQ Survey Team updates the HQ Security Area Database to reflect the deactivation and notifies AU-41 of these actions.

  NOTE: The HSO must ensure that all classified matter has been properly disposed of or relocated and that all other classified activities have been terminated prior to the removal or deactivation of any security equipment.

  NOTE: If the HSO is unsure of the appropriate course of action to complete the deactivation, the HQ Survey Team completes an Advice and Assistance Report providing specific guidance.

Points of Contact

For the names and contact information for those assigned the positions identified in this section, call (301) 903-7189 or (301) 903-2644.

Forms/Samples/Graphics

Sample Security Area Request Memorandum (see Attachment 201-1)

Security Area Request/Facility Information Worksheet (see Attachment 201-2)

Sample Security Area Approval Certificate (see Attachment 201-3)

Sample Security Plan for Temporary Limited Areas (see Attachment 201-4)

ATTACHMENT 201-1

Sample Security Area Request Memorandum

MEMORANDUM FOR (NAME), DIRECTOR
OFFICE OF INFORMATION SECURITY
OFFICE OF HEADQUARTERS SECURITY OPERATIONS

FROM: (NAME), HEADQUARTERS SECURITY OFFICER
NAME OF ELEMENT

SUBJECT: Security Area Request

The Office of _____ is requesting your assistance in establishing a Security Area in Room _____ at the _____ Building. Attached is a Security Area Request/Facility Information Worksheet identifying the various activities that may need to be performed within the Security Area. Also attached is a diagram of Room _____ and the surrounding area.

If you have any questions on this matter or need assistance in examining the proposed area, please contact me on x3 or 6- _____.

Or

The Office of _____ is requesting your assistance in modifying the Security Area currently located in Room _____ at the _____ Building. Attached is a Security Area Request/Facility Information Worksheet identifying the nature of the proposed changes in activities in Room _____. Also attached is a diagram of Room _____ showing the proposed relocation of the existing _____.
(furniture, safes, filing cabinets, etc.)

If you have any questions on this matter or need assistance in examining the proposed area, please contact me on x3-_____ or 6- _____.

Or

The Office of _____ is requesting your assistance in deactivating the Security Area in Room _____ at the _____ Building. Attached is a Security Area Request/Facility Information Worksheet identifying the various activities to be deactivated.

If you have any questions on this matter or need assistance in examining the proposed area, please contact me on x3-_____ or 6- _____.

Official Use Only Stamp

Attachment(s)

OFFICIAL USE ONLY (When filled in)

ATTACHMENT 201-2

Security Area Request/Facility Information Worksheet

ITEM	ACTION

All applicable item numbers 1-7 must be completed and attached to the Security Area Request Memorandum.

1. DATE:
   NAME (HSO):
   ALTERNATE:
   ORGANIZATION:
   BLDG/ROOM #:
   PHONE:
   EMAIL:

2. What action is requested? (Select one) **(MUST ATTACH FLOOR PLAN)**

   ☐ Change in Activities. ☐ Approve Security Area. ☐ Decertify an existing Security Area.

   ☐ Modification to Area. ☐ Security Incident. ☐ Advice and Assistance. ☐ Other.

3. If a change to an existing Security Area is being requested, briefly describe the changes.

4. Provide the following information regarding the Security Area location:

   BUILDING (GTN, FORS, etc.): ROOM NUMBER: POC:

5. What type of area is being requested? (Select one)

   ☐ Limited Area ☐ Vault-type Room

6. What classified activities will be conducted in this area? (Select all that apply) For each activity requested indicate the highest classification level, category, and caveats as applicable. **If this is a request to change classified activities, complete the blocks describing what activities are currently approved then complete section 7 describing the change.**

Activities

☐ Reproduction of Classified Matter

Level: ☐ Top Secret (TS) ☐ Secret (S) ☐ Confidential (C)
Category: ☐ Restricted Data (RD) ☐ Formerly Restricted Data (FRD) ☐ National Security Information (NSI)
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Destruction of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Faxing of Classified Matter, Auto-answer: ☐ Yes ☐ No

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Closed Storage of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Open Storage of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Classified Computer Processing

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Classified Discussions

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Use of Secure Telephone (select all that apply) ☐ Amplified ☐ Nonamplified ☐ RG Encryptor

☐ Video Teleconferencing (select one) ☐ Classified ☐ Unclassified

☐ Other Classified Amplified Sound: Explain:

7. What classified activities will be changed in this area? (Select all that apply) For each activity requested, indicate the highest classification level, category, and caveats as applicable.

Activities

☐ Reproduction of Classified Matter

Level: ☐ Top Secret (TS) ☐ Secret (S) ☐ Confidential (C)
Category: ☐ Restricted Data (RD) ☐ Formerly Restricted Data (FRD) ☐ National Security Information (NSI)
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Destruction of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Faxing of Classified Matter, Auto-answer: ☐ Yes ☐ No

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Closed Storage of Classified Matter

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Open Storage of Classified Matter

Level: ☐ TS ☐ S ☐ C

Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Classified Computer Processing

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Classified Discussions

Level: ☐ TS ☐ S ☐ C
Category: ☐ RD ☐ FRD ☐ NSI
Caveats: ☐ NATO ☐ SAPS ☐ SIGMAS (☐ 14 ☐ 15-20) ☐ Other:

☐ Use of Secure Telephone (select all that apply) ☐ Amplified ☐ Nonamplified ☐ RG Encryptor

---

☐ Video Teleconferencing (select one) ☐ Classified ☐ Unclassified

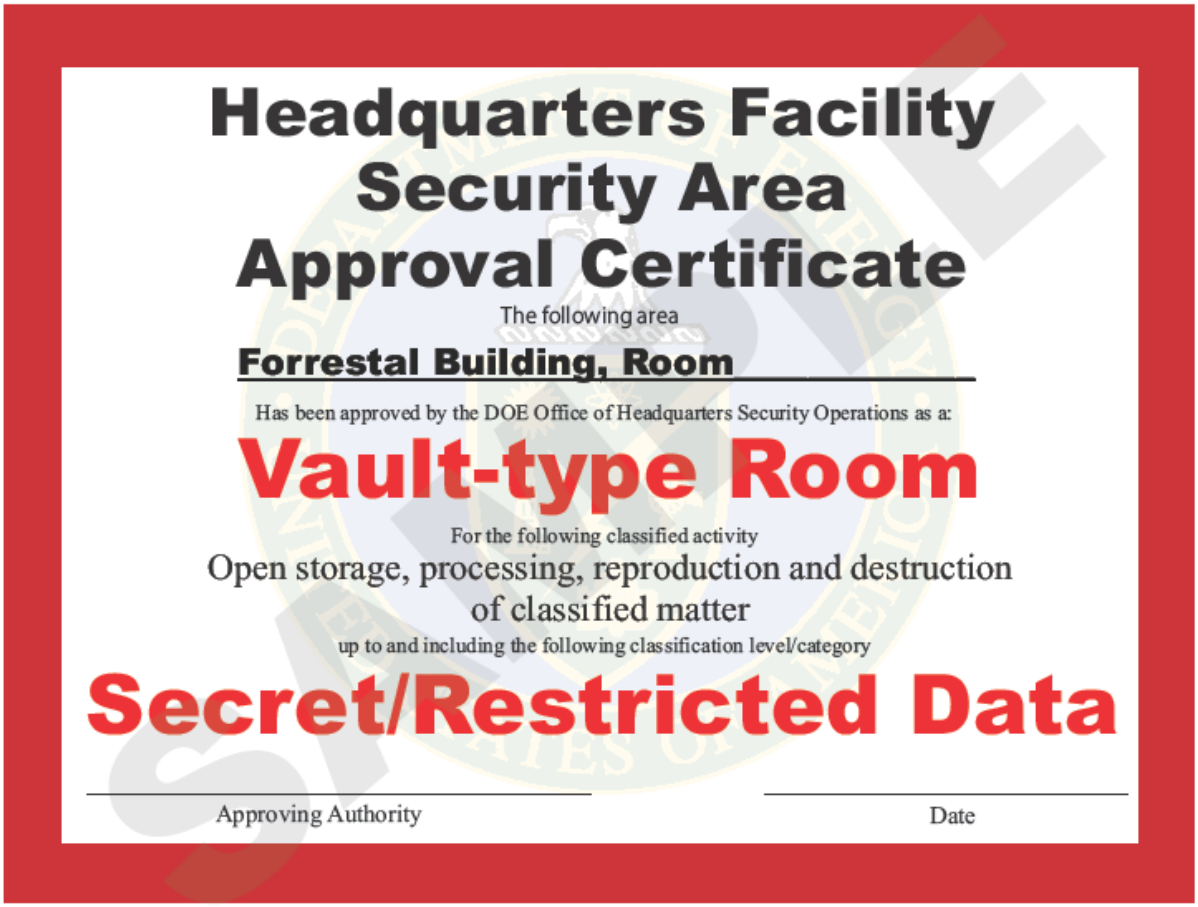
---

☐ Other Classified Amplified Sound: Explain:

8. Additional Comments:

ATTACHMENT 201-3

Sample Security Area Approval Certificate



Headquarters Facility Security Area Approval Certificate

The following area

Forrestal Building, Room _____

Has been approved by the DOE Office of Headquarters Security Operations as a:

Vault-type Room

For the following classified activity

Open storage, processing, reproduction and destruction of classified matter

up to and including the following classification level/category

Secret/Restricted Data

_____ Approving Authority

_____ Date

ATTACHMENT 201-4

Sample Security Plan for Temporary Limited Areas

SECURITY PLAN FOR THE
(INSERT OFFICE NAME)
TEMPORARY LIMITED AREA (TLA)
LOCATED IN (INSERT FORRESTAL OR GERMANTOWN) ROOM (INSERT ROOM NUMBER)

I. PURPOSE

Currently, all (insert Office symbol) classified activities must occur within its designated Limited Areas. However, in order to perform (his/her) assigned responsibilities, (insert individual's name) requires access to classified information outside of the designated (insert Office symbol) Limited Areas. As such, (insert HSO's name, title and Office symbol) has requested (insert individual's name) located in (insert Forrestal or Germantown room number), be designated as a Temporary Limited Area (TLA) so that (he/she) can access classified information within (his/her) office. Classified activities within the TLA are limited to reviewing classified documents at the (insert classification level and category) level and below. This Security Plan sets forth (insert individual's name) specific Classified Matter Protection and Control (CMPC) responsibilities while reviewing classified documents within the designated TLA. These specific responsibilities are in addition to the overall CMPC responsibilities contained in DOE Order 471.6, *Information Security*, and the HQFMSP.

II. RESPONSIBILITIES

A. (Insert Individual's Name) shall:

1. Ensure that all individuals (DOE employees and visitors) who do not have an appropriate security clearance are escorted while they are in the TLA to ensure that they are not allowed access to classified information.

2. Ensure that only personnel with the appropriate security clearance and need-to-know are present when classified documents are reviewed in the TLA.

3. Ensure that classified matter is constantly attended, is under control, and is never left unattended until it is returned for storage in an approved security repository within an approved Limited Area.

4. Shut office door(s) and hang "Please Knock before Entering" sign(s) on exterior door(s) whenever classified documents are reviewed in the TLA.

5. Ensure that classified documents transported between (insert Office symbol) Limited Areas and the TLA are transported in designated candy striped envelopes or other approved methods for transporting classified matter within Headquarters facilities.

6. Ensure that only documents classified as (insert classification level and category) but cannot be higher than S/RD level and below are viewed in the TLA.

7. Ensure that all Controlled Articles in the TLA are handled in accordance with the HQFMSP Section 202, Controlled Articles.

8. Ensure that all classified material is returned to one of (insert Office symbol) approved Limited Areas and properly stored within a GSA-approved safe when finished working with classified documents in the TLA.

9. Ensure that an SF-701, Security Area Checklist, is posted in the room and is initialed at the end of each day classified information is reviewed within it. Initialing the SF 701 will certify that all classified matter has been removed from the room and properly secured in an approved Limited Area.

I acknowledge that I have read this Security Plan and understand my responsibilities for protecting classified information:

_____	_____	_____
Printed Name	Signature	Date

I verify that I have reviewed this Security Plan with the occupants of the proposed TLA and that they fully understand their responsibilities for protecting the classified information entrusted to them.

_____	_____	_____
Headquarters Security Officer	Signature	Date

Approved By:

_____	_____	_____
HQ CMPC Program Manager	Signature	Date

cc:
HQ Survey Program Manager, AU-42
HQ Physical Protection Program Manager, AU-41

This page intentionally left blank.

Section 202
Controlled Articles

This section describes the implementation at HQ facilities of the DOE Order 473.3 requirements on Controlled Articles. Controlled Articles are Government, company, and personally-owned electronic devices that are capable of recording or transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment). At HQ, the Director, AU-40, is the official responsible for establishing the procedures for bringing Controlled Articles into and/or using them within an LA, TEMPEST Protected Area, or VTR. The decisions made by AU-40 are based on risk assessments of the devices and the areas where they will be used.

Personnel Exempt from the LA, TEMPEST Protected Area, and VTR Controlled Article Policies

When performing official duties, the following categories of personnel and their equipment are exempt from the LA, TEMPEST Protected Area, and VTR policies and procedures on Controlled Articles:

- HQ TSCM personnel
- HQ security personnel installing, maintaining, testing, or removing access control and intrusion detection systems
- The HQ Incident Command Team
- The HQ Protective Force
- Special Agents performing personal protection or investigative duties
- Emergency responders, such as Emergency Medical Technicians, firefighters, and police officers
- Personnel and physical security personnel conducting official business.

HQ Implementation Procedures

DOE Owned Electronic Devices:

DOE owned electronic devices configured by the HQ Office of the Chief Information Officer (OCIO) for day-to-day operation in HQ LAs, TEMPEST Protected Areas, or VTRs are permitted as long as they are used and maintained in accordance with the OCIO approved User Agreement, which specifies applicable security precautions (see Attachment 202-1.)

NOTE: No changes to the OCIO installed configuration are permitted.

Controlled Articles:

Other electronic devices capable of recording or transmitting data, including devices from OGAs and other DOE sites, are controlled as follows.

DOE Headquarters Controlled Articles Matrix

Controlled Articles and Uses	Area Type		Controls Required
	S/RD and below but NOT TEMPEST and Protective Distributions System (PTS) protected areas	TS, SAP, Sigma 14 or above, TEMPEST and Protective Distributions System (PTS) protected areas	
Non-transmitting devices (one-way pagers, radios, etc.)	Allowed		None
Wireless mice	Allowed		None
Medical devices (hearing aids, pacemakers, insulin pumps, cardiac monitors, etc.)	Allowed		Notify the elemental HSO or the HQ TSCM Team. The HQ TSCM Team conducts a safety review to ensure the device will not be adversely affected by security systems installed within the area.
Non-user programmable remotes	Allowed		NOTE: User programmable devices may be recognized by having a USB or other port which allows them to be connected to a computer for programming. Refer questions about specific remotes to the TSCM Team
User programmable, TV/audio-visual remotes	Controlled		Requires HQ TSCM Team approval.
Dedicated telephone and video teleconferencing equipment (VOIP, POTS, ISDN, etc.)	Controlled		1. Requires HQ TSCM Team approval. 2. Must remain in the OCIO installed configuration and be used in accordance with User Agreements.
Mobile, wireless capable Personal Electronic Devices, including cell phones, smart phones and personal digital assistants, laptop computers, music players, e-book readers, tablets, bluetooth earpieces/headsets, etc.	Controlled	Prohibited	Must be secured during classified conversations or processing. Acceptable methods of securing include: 1) Placed in aircraft mode (RF functions turned off) 2) Batteries removed 3) Turned off and stored in approved RF bag 4) Removed from the area. These devices must NOT be operated as wireless access points or hotspots.
Infrared (IR) wireless keyboards	Controlled	Prohibited	1. Requires HQ TSCM Team approval. 2. Must remain in the OCIO installed configuration and be used in accordance with User Agreements
Radio Frequency (RF) wireless keyboards	Prohibited		Prohibited at all times.
Making audio/video recordings	Prohibited		Prohibited at all times.

NOTE: Personnel in an LA, TEMPEST Protected Area, or VTR where these devices have been introduced must be cognizant of their surroundings before using the devices. It is the individual's responsibility to take into consideration classified activities that are occurring in adjacent areas.

Unapproved Recording/Use:

If any Controlled Article, regardless of ownership, is used in an unapproved manner or for an unapproved activity, either intentionally or unintentionally within an LA, TEMPEST Protected Area, or VTR, that device and any associated media is subject to confiscation by the element HSO or an official under the supervision of AU-40. If the device and associated media are found to contain classified information or determined to have been used in an unapproved manner, a Security Inquiry will be initiated. The confiscated item may be sanitized and/or destroyed, in accordance with applicable policy.

Photography in LAs:

Photography is not permitted in VTRs; LAs where Top Secret (TS), Sensitive Compartmented Information (SCI), or Special Access Program (SAP) information is stored, processed, or discussed; or in LAs that are TEMPEST Protected Areas. If it becomes imperative to use a camera in one of these areas, see "Requesting Authorization for Additional Controlled Articles," below.

A still camera may be used to photograph personal events such as birthdays, promotions, award ceremonies, etc. within LAs where TS, SCI, and SAP information is not stored, processed, or discussed or in LAs not designated as TEMPEST Protected Areas. AU-40 has government-owned cameras available at both the Forrestal and Germantown facilities. HQ personnel are encouraged to use the AU-40 cameras instead of personally-owned devices because the AU-40 devices have already been approved for use in LAs. HSOs can instruct personnel within their element on how to obtain a camera from AU-40.

Written approval from the element HSO is required before using a camera. See Attachment 202-2, for a *Sample Request to Use a Camera in a Limited Area*. These procedures must be followed to obtain permission for use of a camera:

- The request for approval must be signed by a Federal employee in a supervisory position.
- A digital camera must be used.
- Personally-owned cameras must undergo a TSCM inspection prior to taking pictures.
- All classified and sensitive matter must be removed from the camera's view before taking pictures.
- All classified computing within the LA must cease and computer monitors turned off.

- Pictures must not show any security signs that are not visible to the general public.
- Pictures must not show any access control or intrusion detection equipment or sensors that are not visible to the general public.
- Pictures must not show any planning or project calendars.
- An authorized occupant of the LA must be present during all picture taking.
- At the conclusion of the photography, the camera and/or its media must be handled as a classified "working paper" until reviewed by a Derivative Classifier.
- Photographs containing classified or sensitive information must be removed from the camera and/or its media by the HQ TSCM Team.
- The sanitized camera/media is returned to the photographer for picture printing or distribution.

NOTE: The purpose of the review by a Derivative Classifier is to verify that the photographs do not inadvertently contain any of the items listed above.

TSCM Inspections of Controlled Articles:

HQ personnel who are unsure if a device meets the definition of a Controlled Article are encouraged to request a technical inspection before introducing the device into a LA, TEMPEST Protected Area, or VTR. The request must be made through the Technical Surveillance Countermeasures Officer (TSCMO) within the program element. See Chapter 9, Technical Surveillance Countermeasures, for instructions on contacting the HQ TSCM Team.

Requesting Authorization for Additional Controlled Articles:

The Office Director requesting authorization for additional Controlled Articles or the use of selected device features must submit the request via memorandum to the Director, AU-40. The HSO of the requesting organization must be copied on the memorandum. The memorandum describes in detail the controlled article, the reason for its introduction or use, how long it will be needed, mitigations, who will have custody of the article, and what HQ facility and LA, TEMPEST Protected Area, or VTR will be affected. The memorandum must also include a risk assessment for using the article and a statement that the Office Director accepts the risk.

The approved request is valid for the specified time period, not to exceed one year. Renewal requests must be submitted at least 90 days prior to the expiration of the current approval to permit proper review.

Periodic Technology Review

The HQ TSCM Team conducts an annual technological review of the authorized controlled articles and their features to determine whether the HQ Controlled Article policy needs revised.

Points of Contact

For the names and contact information for those assigned the positions identified in this chapter, call (202) 586-8075 or (301) 903-2644.

To determine if a particular room or area is a TEMPEST Protected Area, call (301) 903-3957.

Forms/Samples/Graphics

Sample User Agreement (see Attachment 202-1)

Sample Request to Use a Camera in a Limited Area (see Attachment 202-2)

Attachment 202-1

Sample DOE Headquarters Desktop Webcam User Agreement

This User Agreement outlines individual user's responsibilities when utilizing webcams while conducting desktop Video Teleconferencing (VTC) sessions in HQ Security Areas specifically approved for desktop VTC sessions. This User Agreement must be completed by each individual user prior to utilizing approved webcam equipment and/or conducting VTC sessions. Upon execution of this agreement (initials and signature), the user acknowledges the following requirements:

Initials:

_____ Only DOE TSCM approved webcam equipment, software and hardwired desktop computer hardware may be utilized. The use of non-government owned/sponsored equipment for VTC sessions is not authorized.

_____ Undocked laptops, integral laptop cameras and Personal Electronic Devices (i.e., Blackberry's, IPhones, IPADs or similar devices) are not authorized for video teleconferencing (VTC) within the Security Area.

_____ Prior to connecting the VTC equipment, the environment where the VTC session will be taking place must be sanitized to ensure that sensitive and classified information will not be exposed during the VTC.

_____ Wireless VTC session are not authorized within Security Areas.

_____ Webcam users must notify occupants in the surrounding areas that an unclassified VTC session will be taking place within the Security Areas and that sensitive and classified information could be compromised if discussed or brought into view during the session.

_____ Signs must be conspicuously posted to warn individuals that unclassified VTC is occurring and to restrict sensitive and classified information and activities in the immediate area.

_____ Immediately upon completion of the VTC session, the software application must be terminated and the webcam and associated VTC specific equipment (headphone, microphones, etc.) must be physically disconnected (i.e, physically unplugged) from the network system.

_____ User has received training in the use of VTC equipment and software associated with the devices.

_____ When not in VTC session use, equipment must be stored in a manner to easily identify that it is physically disconnected.

_____ Approved USB hubs may be utilized to facilitate easier physical disconnection.

_____ Recording of desktop VTC sessions is not authorized.

_____ VTC software automatic answer capability must be disabled.

_____ Failure to follow these requirements outlined in this user agreement will result in a security incident.

ACKNOWLEDGEMENT:

I certify that I have read, understand and will comply with the User Agreement for the Use of Desktop VTC/Webcam Devices within specifically approved DOE Headquarters Security Areas.

_____
(Printed User Name)

_____ _____
(User Signature) (Date)

cc: User's HSO

Note: This User Agreement will be maintained in the Security Area Approval file for the area containing the webcam.

ATTACHMENT 202-2

Sample Request to Use a Camera in a Limited Area

MEMORANDUM FOR (ENTER NAME OF HEADQUARTERS SECURITY OFFICER)
NAME OF ORGANIZATIONAL ELEMENT

FROM: NAME OF FEDERAL SUPERVISOR MAKING REQUEST
TITLE
NAME OF ORGANIZATIONAL ELEMENT

SUBJECT: Request to Use Camera within a Limited Area of the _____ Facility

I hereby request permission to use a camera to take photographs at the _____ Facility. The following information is submitted:

Date Camera Will Be Used: Enter Dates.

Person Using the Camera: Enter Name of Person Using Camera.

Purpose of Photography: Why photography is needed.

Location of Photography: Where the camera will be used. (This cannot be a Vault-Type Room or a Limited Area approved for Top Secret, Sensitive Compartmented Information, Special Access Program information, or a TEMPEST Protected Area).

Equipment to be Used: Preferably a Government-owned digital camera. If a personally-owned camera is to be used, there must be a statement that the camera has been inspected by the HQ TSCM Team and approved for use.

I understand and will comply with the following security rules pertaining to use of a camera in a Limited Area.

- The area will be sanitized before any photographs are taken. This includes covering up or removing from view all classified and sensitive documents or matter. This will include the total shutdown of any classified computer system.
- Only still photographs are authorized.
- I will not photograph any Security Area signs that are not visible to the general public.
- I will not photograph any access control or intrusion detection equipment such as card readers, PIN pads, door locks, secure telephone devices, sensors, motion detectors, etc., that are not visible to the general public.
- I will not photograph any planning or project calendars.
- An authorized occupant of the area will be present during the entire photography session.

- At the conclusion of the photography, the camera and/or its media will be handled as a classified "working paper" and submitted to a Derivative Classifier (DC) for review prior to being used for any purpose.
- The camera and/or its media will be stored as classified matter until a DC determines the photographs are unclassified.
- In the event classified matter appears in any photograph, the camera and/or its media will be sanitized by the HQ TSCM Team.

If you have any questions on this matter, please contact me at (phone number of person making request).

APPROVED: _____

DISAPPROVED: _____

DATE: _____

cc:
Facility Security Manager
User's HSO

This page intentionally left blank.

Section 203
Classified Meetings in LAs and VTRs Approved for Classified Discussions

It is HQ policy to conduct classified meetings (including conferences, presentations, etc.) within LAs and VTRs that have been specifically approved for classified discussions. Not all LAs and VTRs are approved for classified discussions, and there may be restrictions on the level or category of classified information that may be presented within an LA or VTR. There may also be restrictions on the use of audio amplification devices within an LA or VTR. It is incumbent upon the meeting host and all participants to ensure the Area has been approved for discussions at the equal to or higher classification level and category than the matter being discussed and to comply with other technical requirements.

On occasion, a classified meeting must be held in an area that has not been approved for classified discussions. For procedures see Section 204, Classified Meetings Outside of LAs and VTRs Approved for Classified Discussion.

HQ Implementation Procedures

Classified Meetings:

Prior to holding a classified meeting in an LA or VTR, the participants must ensure that the area is approved for classified discussion at the level and category of the information to be discussed. A Security Certificate sign must be posted within each LA and VTR clearly indicating that the area is approved for classified discussion, the level and category of the classified information, and whether the Area is approved for "amplified discussion." Amplified discussion refers to the use of microphones, polycoms, and speaker phones to discuss classified information within the area.

NOTE: Classified meetings involving the discussion of SCI or SAP information must always be conducted in LAs or VTRs specifically approved for these discussions.

If the Area is not approved at the requisite level and category of the classified discussion, an alternate location must be found. For procedures see Section 204, Classified Meetings Outside of LAs and VTRs Approved for Classified Discussion.

When a classified meeting is scheduled within an LA or VTR approved for classified discussions, the date, time, location, discussion topic, and other details of the meeting can be openly announced.

If DOE field personnel or employees of OGAs are scheduled for a classified meeting at a HQ facility, they may need to pass their security clearances through the Office of HQ Personnel

Security Operations (AU-43). See Section 306, Passing Clearances for Classified Meetings and Visits, for instructions on how to pass security clearance information.

The host of the classified meeting must ensure that:

- All participants have the requisite security clearance and "need to know".
- All Controlled Articles are removed beyond audible range and have their batteries removed, or must be turned off and placed in an approved Radio Frequency (RF) container (see Section 202, Controlled Articles).
- The classification level and category of the discussion are announced at the start of the meeting.
- A sign is visible to all participants indicating the classification level and category of the information presented during the meeting.
- All presentations given during the meeting bear the proper classification markings.
- Note taking is prohibited unless arrangements are made to protect all notes until they have undergone a classification review.
- All classified matter is properly protected during the meeting.

  NOTE: Notify the TSCM Team when a Top Secret discussion or meeting is planned for an LA or VTR not approved for Top Secret discussions. The TSCM Team must be notified before such discussions occur.

Points of Contact

For names and contact information for those occupying the information security, personnel security, and TSCM positions identified in this section, call (301) 903-7189 or (301) 903-2644.

Section 204
Classified Meetings Outside of LAs and VTRs Approved for Classified Discussions

On occasion, the number of meeting participants exceeds the capacity of the approved area or there may not be an approved meeting area available. An unapproved area can be used for a classified meeting, providing certain security protection requirements and administrative measures are met. This section describes the procedures and security measures that must be met to ensure classified information is protected when discussed in an unapproved area.

This section does not apply to classified meetings held at the facilities of OGAs.

HQ Implementation Procedures

Classified meetings scheduled outside an LA or VTR must be approved by the TSCMO of the HQ element hosting the meeting. The TSCMO must contact the TSCM Operations Manager (TSCMOM) to identify the necessary protective measures.

TSCMOs can approve occasional classified discussions and meetings up to the S/RD level outside of approved LAs or VTRs within the Forrestal and Germantown buildings.

When scheduling a classified meeting outside of an approved LA or VTR, all publicity/notification documents, messages, or e-mails must be handled in accordance with *TNP-32, Classification Guidance for Classified Meeting Locations at DOE/NNSA or DOE/NNSA Contractor Sites or Facilities (U).*

> *NOTE: TNP-32 is not included in the HQFMSP because it is an Official Use Only document. A copy can be obtained by the element HSO through the HSO Program Manager. The HSO Program Manager can be contacted as indicated in the Points of Contact subsection at the end of this section.*

If DOE field personnel or employees of OGAs will be attending a classified meeting at an HQ facility, they may need to pass their security clearances through AU-43. See Section 306, Passing Clearances for Classified Meetings and Visits, for instructions on how to pass security clearance information.

Once the meeting is approved, the TSCMO must coordinate with the host of the meeting to ensure that:

- All participants have the requisite security clearance and “need to know.”

- All Controlled Articles must be removed beyond audible range and have their batteries removed, or must be turned off and placed in an approved RF container (see Section 202, Controlled Articles).

- The area used to conduct the classified meeting must provide acoustical isolation in such a way that classified information is not advertently disclosed. Acoustical isolation can be addressed by a TSCM evaluation of the room, administrative procedures, or combination of both.

- The volume level of approved electronic equipment used in classified presentations (e.g., video cassette/DVD player/computer monitor volume, TSCMOM-approved portable public address systems using hardwired microphones, etc.) must be set so voices are not discernible outside the conference area.

- Public address systems (other than life-safety) permanently installed within the area of the classified discussion are not to be used without specific approval of the TSCMOM. If the TSCMOM does not approve use of these systems, they should be completely disconnected during the classified discussion. Wireless microphones must be disabled if stored within the conference area. The TSCMOM should verify that all these actions are completed.

- The room must have controlled access by the host, either through a locking mechanism or someone physically controlling access to the room.

- Information being presented must be visually protected so that no one outside the area or just entering the area can see it.

- The classification level and category of the discussion is announced at the start of the meeting.

- A sign must be visible only inside the room indicating the classification level and category of the information presented.

- All presentations must bear the proper classification markings.

- No discussions may take place within the hearing range of unauthorized persons.

- All doors and windows are closed and secured during classified presentations and discussions.

- Note taking is prohibited unless arrangements are made to protect all notes until they have undergone a classification review.

- All classified matter is properly protected during the meeting.

- All telephones, speaker phones, etc., must be physically disconnected from the telephone and electrical power removed.

- When classified meetings occur in an area with unclassified Video Teleconferencing (VTC) capabilities, all VTC connections must be (electric, data, etc.) physically disconnected from the network.

- All unclassified laptops must have microphones physically disabled.

- If the conference room is equipped with Wireless Access Point (WAP) or WiFi, those functions must be disabled prior to the start of the meeting.

The HQ element hosting the meeting is responsible for any costs incurred for these security requirements.

For multi-day meetings and conferences, the TSCMO must coordinate with the HQ protective force to seal all entrances and conduct security checks on the area used for the classified meeting. The TSCMO must also arrange for opening the area each day of the meeting or conference.

Points of Contact

For the names and contact information for those occupying the information security positions identified in this chapter, call (301) 903-9990.

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

To contact the HSO Program Manager, call (301) 903-2644.

This page intentionally left blank.

Section 205
Secure Telecommunications Equipment (Phones)

Secure Telecommunications Equipment (STE) and vIPER Universal Secure Phones (vIPERs) are Communications Security (COMSEC) equipment. HQ policies and procedures for their installation, configuration, use, and deactivation are governed by the National Security Agency (NSA). The HQ COMSEC Program, which includes all STE and vIPER services, guidance, and assistance, is managed by the Technical Security Program within the Office of Corporate Security Strategy, Analysis, and Special Operations (AU-1.2).

The COMSEC program ensures the secure transmission of classified and sensitive information. STEs and vIPERs encrypt telephonic and facsimile transmissions of classified information; therefore, these devices must be used when telephonically discussing classified information or transmitting classified information via a facsimile machine.

HQ Implementation Procedures

Requesting STE and vIPER Services:

STE and vIPER custodians 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 HQ Secure Phone Group. The HSO within each HQ element must be advised when STE service is needed. All service requests, which include requests for installation, reconfiguration, relocation, transferring to another user, troubleshooting, and deactivation, must be prepared by the elemental HSO and transmitted via email to the HQ Secure Phone Group for action.

To take the requested action, the HQ Secure Phone Group needs (at a minimum) the following information:

1. For installation of a STE or vIPER for a new user:
   a. New user's name.
   b. Room number and name of HQ Building. Attach a scanned copy of the document showing that the room where the STE or vIPER will be located is approved for classified discussions (preferably the Security Area Approval Certificate provided by the Headquarters Survey Team). Note that COMSEC personnel do not install a STE or vIPER in a room that is not approved for classified discussions.
      See the sub-section Residential Installation of STEs and vIPERs, below, for instructions for installing a STE or vIPER in a private residence.
   c. Contact number for new user.
   d. Organizational routing symbol for new user.

e. Key level required and any special needs, such as the need to talk to North Atlantic Treaty Organization (NATO) countries, other countries via the Combined Communications Electronic Board (CCEB), or SCI.
f. If the request is for a STE to be connected to a facsimile machine or computer, the HSO must provide documentation of all approvals in place for a secure fax.
g. When the new installation needs to be done (date or range of dates and best time of day).

2. For transfer of a STE or vIPER to a different user, the e-mail should include:
   a. Previous user's name.
   b. New user's name.
   c. Contact numbers for previous and new users.
   d. Organizational routing symbol for new users.
   e. Room number and building location of previous and new users. If the transfer will be made to a different room, attach a scanned copy of the document showing that the room where the STE or vIPER will be located is approved for classified discussions (preferably the Security Area Approval Certificate provided by the HQ Survey Team). Note that COMSEC personnel will not install an STE or vIPER in a room not approved for classified discussions.
   f. STE or vIPER serial number. The STE serial number is found on the back of the STE and starts with the letters "STEA" or "STEB" followed by a 10 digit number; the vIPER serial number is also on the back of the phone, but starts with the letters "GSN: FNBE", the numbers "21," and then an additional 8 digit number.
   g. The new key level required and any special requirements, such as need to discuss NATO, CCEB, or SCI information.
   h. When the transfer needs to take place (date or range of dates).

3. For removal of a STE or vIPER, the e-mail should include:
   a. Username
   b. Room number
   c. Contact number
   d. STE or vIPER serial number (refer to item 2f, above)
   e. When the removal needs to take place (date or range of dates).

Once the e-mail is prepared, it should be sent to: **HQSecurePhone@hq.doe.gov.**

Residential Installation of STEs and vIPERs:

If an HQ element identifies the need, an employee may have a STE or vIPER installed at his/her private residence *for the purpose of listening only*. ***Discussing classified information on a STE or vIPER at a residence is strictly prohibited.***

The HQ element where the user is assigned must pay for a vIPER installed at a private residence.

To request the installation of a STE or vIPER at a private residence, the HSO must send an e-mail to the HQ Secure Phone Group at **HQSecurePhone@hq.doe.gov** and have the user complete a Residential vIPER Telephone Equipment Security Plan (see Attachment 205-1). The HSO must then submit the completed plan to AU-42 by:

- Intra-office mail to AU-42, Attention: HQ Survey Team, Room F-316, Germantown, or

- Scan it electronically, attach it to an encrypted e-mail, and transmit it to "xxx-2 Operations" in the Microsoft Outlook Global Address List.

Once AU-42 receives the signed user agreement they provide a copy to the HQ Secure Phone Group to make arrangements to install the STE or vIPER. A file of current Residential STE/vIPER user agreements is maintained by the AU-42 HQ Survey Team.

Points of Contact

For the names and contact information for the HQ Secure Phone Group, call (301) 903-5062.

To contact the HQ Secure Phone Group by e-mail, use **HQSecurePhone@hq.doe.gov**.

To contact AU-42 by phone, call (301) 903-9990.

To contact AU-42 by e-mail, use the title "AU-42 Operations" in the Microsoft Outlook Global Address List.

Forms/Samples/Graphics

Residential vIPER Telephone Equipment Security Plan (see Attachment 205-1)

ATTACHMENT 205-1

Residential vIPer Telephone Equipment Security Plan

The following security requirements are in effect for any residential installed vIPer.

_____The purpose for the vIPer instrument in a residential installation is to enable the authorized residential user to receive audible classified information in an **Emergency Situation**. Conversations on the vIPer telephone at the residential site should be limited to brief, **UNCLASSIFIED** responses, e.g., yes/no answers, by the authorized residential user. The risk associated with passively listening to classified information at the residence is minimal; the risk associated with actively discussing classified information at the residence is very high, especially for that of senior management personnel. As such, the discussion of classified information is strictly prohibited and is in direct contravention to DOE Orders and National directives. Authorized discussion of classified information must be accomplished within, approved security areas located in U.S. Government facilities.

_____Maintenance on your residential vIPer by anyone other than authorized DOE personnel is strictly prohibited. All installations, changes, removals, and maintenance will be performed only by the COMSEC Custodian.

_____The vIPer instrument must be installed in a room in which the user can be isolated by physical means from other occupants in the residence while using the vIper telephone equipment. When the terminal is in use in the encrypted mode, the doors and windows to the room shall be closed and only individuals with the appropriate clearances and need-to-know shall be allowed within and/or in close proximity to the room.

_____No other type telephone instrument may be located in the same room as the vIPer instrument. The vIPer instrument must be separated from other electronic devices in accordance with the approved TEMPEST Plan for the residence.

_____The PIN number for the vIPer must be memorized (it cannot be written down).

_____The vIPer instrument must not be moved within the residence or transported out of the residence without the approval of the Headquarters Security Officer and the Communications Security Custodian.

_____, The classification level to which the vIPer instrument is keyed should not be disseminated to anyone within the residence or to anyone without the need-to-know.

_____As communication with another Secure Telephone is established, the residential vIPer authorized user can identify the distant end user and the authorized classification level on the instrument's liquid crystal display (LCD). The distant end user will see "Residence, USDOE, DOE Official" scroll on its vIPer screen followed by "Residence" and a classification level. The LCD on the residential vIPer instruments will display the lower of the two classification levels to which the secure communication instruments are authorized to transmit.

_____Any notes taken during classified use of the vIPer instrument should be unclassified. However, any and all notes taken concerning the substance of the secure communication must be protected as classified until reviewed by a Derivative Classifier. If determined to contain classified information the notes must be appropriately marked and protected, or properly destroyed as classified matter.

Acknowledgement by the vIPer authorized user:

_____ (printed name) _____ (signature) _____ (date)

OFFICIAL USE ONLY
May be exempt from public release under the Freedom of Information Act (5 U.S.C. 712), exemption number category: Exemption 7 – Law Enforcement.
Department of Energy review required before public release.
Name/Org: _____
Date: _____

OFFICIAL USE ONLY