Chapter 2 Revision History: Revisions by date (Newest to oldest):

June 5, 2020: Revised entire document

March 2, 2020: Revised entire document

February 13, 2020: Revised Section 202, DOE Headquarters Controlled Articles Matrix.

September 13, 2019: Revised Section 205 to update secure phone terminology and contact information.

November 21, 2018:

- Revised Section 202 to add TSP contact (TecSec@hq.doe.gov)
- Revised Section 201
- Added new topic: Accessing an LA/VTR, and subtopic: VTR Access
- Added HSO involvement with TSP area/equipment reviews
- Added Locking and alarming responsibilities
- Added Locked Issues section
- Revised Section 203 to add Unauthorized use
- Revised Section 205 to add TSP involvement
- Revised POC and Contact Lists

Chapter 2
Limited Areas
and Vault-Type Rooms

This Chapter of the DOE Headquarters (HQ) Facilities Master Security Plan (DOEHQFMSP) describes the processes, requirements and responsibilities required to establish, manage, and deactivate Limited Areas (LAs) and Vault-Type Rooms (VTRs) at DOE HQ used for the processing, reproducing, destroying, transmitting/receiving, discussing, reviewing, and/or storing of classified matter.

Limited Area (LA) – An LA is a Security Area (SA) established to protect classified matter. An LA is a designated space with physical barriers and access controls to ensure only authorized personnel are allowed to enter and exit the LA. A means must be provided to detect and deter unauthorized entry into the LA. An LA may be approved for the storage, review, computer processing, destroying, reproducing, transmitting or receiving, and discussing classified information. LAs cannot be approved for open storage of classified matter. Classified matter must be stored in a GSA-approved security container within an LA. Closed storage of Top Secret (TS) classified matter within an LA requires Intrusion Detection System (IDS) protection and Protective Force (PF) response measures in accordance with DOE Order 471.6, *Information Security*.

Vault-Type Room (VTR) – A VTR is a room having combination-locked doors (X10 or X-0 series combination lock) and provided an intrusion alarm system activated by any penetration of walls, floors, ceilings, or openings, or by motion in the room. A VTR may exist within an LA or be a stand-alone facility. VTRs within an LA can be used for the closed storage of TS classified matter if equipped with IDS protection and PF response measures in accordance with DOE Order 471.6; OR locked in a VTR within a property protection area (PPA) or outside of a SA, and the VTR must be under IDS protection with a PF response. A VTR can also be used for the storage of Secret (S) classified matter if it is stored in a manner authorized for TS. Intrusion detection systems are required for VTRs and must be configured to detect movement within a VTR and must provide coverage of the matter being protected. A balanced magnetic switch (BMS) or equivalent device must also be used on each door or movable opening to allow for the detection of attempted unauthorized access. Typically, a VTR is used for the open storage of classified material, equipment, and components up to and including S/RD. In a VTR designated for the open storage of classified matter, protective measures must ensure that the security interest is surrounded by an IDS or that penetration of the entire surrounding perimeter (walls, ceiling, and floor) can be visibly detected. Depending upon the circumstances and approved activities, a VTR may be approved for the storage, reviewing, computer 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 in SAs at HQ facilities. However, on a case by case basis, the open storage of TS matter may be authorized within a VTR if there is a mission essential need and if the situation is approved by AU-40.

LAs and VTRs may also contain Special Designated SAs, i.e., Sensitive Compartmented Information (SCI), and Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST) Protected Area facilities. VTRs may also be approved for managing Special Access Program (SAP) information. Except for the section on controlled articles within this Chapter, security procedures for Special Designated SAs are described in security plans that have limited distribution and are not discussed in this Plan.

The management of LAs and VTRs is documented from the establishment through the deactivation of these areas. A file for each LA or VTR is created and maintained by the HQ SA Program Manager, within the Office of Physical Protection (AU-41), Office of HQ Security Operations (AU-40), Office of Environment, Health, Safety, and Security (AU), that contains all the documentation associated with the LA, and/or VTR. The HQ SA Program Manager also maintains pertinent information about each LA and VTR in the HQ Security Area Database. DOE HQ element Headquarters Security Officers (HSOs) are responsible to maintain their own records regarding their (SA) as well.

This Chapter is organized as follows:

A. Establishing LAs and VTRs
B. Managing LAs and VTRs
    Access and Security
    SA Entry Locks
    Secure Desktop Phones
    Controlled Articles
    Photography in an LA
    Classified Meetings
    Modification of LAs and VTRs
C. Deactivating LAs and VTRs

A. Establishing LAs and VTRs

The establishment of LAs and VTRs at DOE HQ must be approved by the Director, AU-41 prior to the initiation of classified activities or the introduction of classified matter into an area. The approval is based upon the requirements set forth in DOE directives. In cases where security requirements cannot be met, a deviation, i.e., equivalency or exemption, may be requested by the DOE HQ element in accordance with the applicable directive (see Chapter 16, Equivalencies and Exemptions, of this Plan).

The following description identifies the overall responsibilities and processes required for the establishment of a new LA or VTR.

1. The DOE HQ element HSO reviews the Facility Data and Approval Record (FDAR) to determine if it meets or exceeds the facility clearance level and category of the proposed LA or VTR. If not, the FDAR will need to be updated if the LA or VTR is approved.
2. The DOE HQ element HSO submits an SA Advice and Assistance (A&A) Request

Package to the Director, AU-41 requesting a review to prepare for the establishment of a new LA or VTR. The SA A&A Request Package consists of a memorandum requesting assistance in establishing a new LA or VTR (Attachment 1), an SA A&A Request Worksheet (a fillable PDF form available from AU-41), and a blueprint/drawing of the proposed LA or VTR. The proposed LA or VTR may be indicated on blueprints obtained from the Office of Management (MA) Property Management Officer (MA-432) or in a simple, hand-drawn sketch.

3. The AU-41 Director forwards the SA A&A Request Package to the AU-41 HQ SA Program Manager. AU-41 may coordinate with the DOE HQ element HSO and a team of representatives from the AU Office of Technical Security (AU-1.22), MA-432, and/or NA-IM, National Nuclear Security Administration (NNSA). The AU-41 HQ SA Program Manager will conduct a physical security review and walk-through of the proposed LA or VTR. After the security review, AU-41 will provide an SA Action Report to the DOE HQ element HSO that identifies the physical protection measures required to be installed/implemented before the space can be certified as an SA.

   The DOE HQ element HSO coordinates with MA and AU-1.22, as applicable, to arrange for needed construction, other physical changes, and services for the proposed LA or VTR. Procedures for obtaining AU-1.22 Technical Security Program (TSP) Team services are provided in Chapter 9, Technical Surveillance Countermeasures, of this Plan. Requirements for Technical Security Program (TSP) services are determined based upon the activities (discussions, copying, destruction, STE/vIPer, etc.) that will take place within the proposed area. If the area/equipment, as applicable, requires TSP services, the HSO will continue to coordinate with the TSP Manager to obtain those services *(following the procedures established in Chapter 9, Technical Surveillance Countermeasures)*.

   Non-amplified discussions (Sound Transmission Class - STC-45 rating) refers to normal voice levels while discussing classified information within the security area.

   Amplified discussion (STC-50) refers to the use of microphones, polycoms, speaker phones, or any other means used to amplify the sound while discussing classified information within the security area.

4. HSOs are responsible for reporting bi-weekly status updates to the SA PM to be able to track progress of the security area during the approval process.

5. The DOE HQ element HSO notifies the HQ SA Program Manager in writing, i.e., via memorandum or e-mail, upon completion of physical security upgrades for the proposed LA or VTR.

6. The HQ SA Program Manager coordinates with the DOE HQ element HSO and other appropriate representatives to inspect the LA or VTR to verify that all specified physical protection requirements have been addressed. Upon verification, the HQ SA Program Manager provides an SA approval memorandum, report, and certificate to the requesting DOE HQ element HSO. In addition, the HQ SA Program Manager updates applicable DOE HQ databases to include the new SA.

B. Managing LAs and VTRs:

Approval Certificate

The SA Approval Certificate (Attachment 2) must be prominently displayed at eye level near or as close as possible to each entrance of the LA or VTR to inform personnel the type of area they are entering and the classified activities approved for the area.

Access and Security

Only personnel with proper access authorization / clearance and relevant need-to-know should be provided access to an LA or VTR.

Authorized individuals entering an LA or VTR through an electronically controlled access must not allow unauthorized individuals into the SA unescorted. In some cases, authorized individuals may admit another individual into an LA or VTR after ensuring that individual's security badge bears the individual's photo, indicates the proper level of security clearance required to enter the area, and is not expired. However, some LAs and VTRs have restricted access based on need to know or other programmatic requirements. In these cases only specified individuals are allowed free access to the SA. Other personnel, even those with valid badges and access authorizations, are required to be escorted.

Escorting personnel, for whatever reason, in an LA is permitted but is not to exceed the ratio of one escort for five visitors. VTR escort ratio will not exceed one escort to three visitors.

The DOE HQ element HSO is responsible to maintain and keep the SA access list memorandums updated. Access Control systems, procedures, and information regarding an Access Authorization Memoranda is covered in Chapter 1.

Access procedures for emergency response personnel to enter SAs are covered in Chapter 5.

Need to know must be established before permitting entry into a VTR. DOE Order 473.3 requires access controls at VTRs to include a log and record of all visitors. There is no specified format for the log, however, as a minimum, it must contain the entrant's: name, signature, DOE office symbol or organizational affiliation, purpose of visit, arrival time, departure time, and name of escort (if applicable).

SAs need to be locked and alarmed, as appropriate, at the end of the workday or when no one is present in the space to control access (see Chapter 5, Classified Matter Protection and Control, of this Plan). VTRs found to be in access mode at the end of the workday or when no one is present will result in the issuance of an Incident of Security Concern in accordance with Chapter 11 of the HQFMSP. The incident may require a list of corrective actions that should be taken to preclude recurrence, including retraining, issuance of a security infraction, or other disciplinary actions.

SA Entry Locks

The DOE HQ element is responsible for the maintenance, repair, and replacement of entry locks for assigned SAs. Maintenance of SA entry locks is coordinated between the applicable DOE HQ element HSO and the MA Office of Facilities Management Operations (MA-431).

If the security area occupant becomes aware that the functioning of a combination lock (cypher/X-0 series Kaba-Mas lock) is starting to fail, the HSO needs to be notified so that they can initiate the process to have the lock examined/repaired before it totally fails. The HSO will need to communicate with the organization resource management team (finance/budget) for completion of a funding request and MA-431 is contacted to request a certified locksmith. The HSO will need to coordinate with the space occupants and MA to provide an escort for access into the security area. The organization will need to provide an escort for the locksmith until the work has been completed and the locksmith departs the building or complex (GTN).

If a malfunctioning SA entry lock results in the SA not being secured, the DOE HQ element HSO and AU-41 will coordinate to implement compensatory measures.

Secure Desktop Phones

Secure desktop phones 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 secure desktop phone services, guidance, and assistance, is managed by the Technical Security Program (TSP) within the Office of Corporate Security Strategy (AU-1.2).

The COMSEC program ensures the secure transmission of classified and sensitive information. Secure desktop phones 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.

Requesting Secure Desktop Phone Services:

Secure desktop phone 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 TSP and are coordinated between the DOE HQ element HSO and the DOE HQ Secure Phone Group via email at: HQSecurePhone@hq.doe.gov.

The following information is required to be submitted by the DOE HQ element HSO for the identified services.

1. Installation of an STE or vIPer for a new user at DOE HQ facilities.
    a. User's name, work email address, work email user identification, contact number and organizational routing symbol.
    b. DOE HQ building and room number where the equipment is to be installed.

c. Documented proof showing that the location where the equipment is to be installed is approved for classified discussions (preferably the SA Approval Certificate).

d. Key level required and any special needs, i.e., the need to talk to North Atlantic Treaty Organization (NATO) countries, other countries via the Combined Communications Electronic Board (CCEB), or SCI.

e. Approvals in place for a secure fax to be connected to a facsimile machine or computer, as applicable.

f. Preferred dates and times for the installation.

2. Transfer of an STE or vIPer to a different user at DOE HQ facilities.

a. Name, contact number and organizational routing symbol of the previous and new user.

b. DOE HQ building and room number for the previous and new user. If the equipment is moving to a different location, include documented proof showing that the location where the equipment is to be installed is approved for classified discussions (preferably the SA Approval Certificate).

c. Equipment serial number.

- The STE serial number is found on the back and starts with the letters "STEA" or "STEB" followed by a 10 digit number.
- The vIPer serial number is on the back of the phone and starts with the letters "GSN: FNBE", the numbers "21," and then an additional 8 digit number.

d. Key level required and any special requirements, such as need to discuss NATO, CCEB, or SCI information.

e. Preferred dates and times for the installation.

3. Removal of an STE or vIPer at DOE HQ facilities.

a. User name and contact number.

b. DOE HQ building and room number.

c. Equipment serial number.

- The STE serial number is found on the back and starts with the letters "STEA" or "STEB" followed by a 10 digit number.
- The vIPer serial number is on the back of the phone and starts with the letters "GSN: FNBE", the numbers "21," and then an additional 8 digit number.

d. Preferred dates and times for the removal.

<u>Residential vIPer Services</u>

A vIPer may be installed at an employee's private residence, at the expense of the DOE HQ element, for the purpose of listening to classified information discussions only as discussing classified information at a residence is strictly prohibited.
Requests for these services are coordinated between the DOE HQ element HSO, the DOE

HQ Secure Phone Group (via email at: HQSecurePhone@hq.doe.gov), the Director, AU-41, and the AU-41 HQ SA Program Manager

The following information is required for the identified services.

1. Installation of a vIPer at a private residence.
   a. User's name, work email address, work email user identification, contact number and organizational routing symbol.
   b. Address where the equipment is to be installed.
   c. Completed Residential vIPer Telephone Equipment Security Plan (Attachment 3).
   d. Key level required and any special requirements, such as need to discuss NATO, CCEB, or SCI information.
   e. Preferred dates and times for the installation.
2. Removal of a vIPer from a private residence.
   a. User name and contact number.
   b. Address where the equipment is located.
   c. Equipment serial number located on the back of the phone starting with the letters "GSN: FNBE", the numbers "21," and then an additional 8 digit number.
   e. Preferred dates and times for the removal.

Controlled Articles

Controlled Articles (not to be confused with Prohibited Articles identified in Chapter 1) are electronic devices that are capable of recording or transmitting audio, video, radio frequency, infrared, and/or data signals.

At DOE HQ, the Director, AU-40 or designee, is the official responsible (ODFSA) 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 the Director, AU-40 or designee, are based on risk assessments of the devices and the areas where they will be used.

Exemption from Controlled Article Policies

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

- AU-1.2 TSP Team personnel,
- DOE HQ security personnel installing, maintaining, testing, or removing access control and intrusion detection systems,
- DOE HQ Incident Command Team,
- DOE HQ Protective Force personnel,
- Special Agents performing personal protection or investigative duties,

- Emergency responders, such as Emergency Medical Technicians, firefighters, and police officers, and
- AU-41 SA Program Manager and physical security personnel.

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.

Controlled Articles Matrix

The Controlled Article Matrix, maintained by the AU-1.2 TSP Team, provides a guide on controlled Article use and controls in LAs and VTRs at DOE HQ. The AU-1.2 TSP Team conducts an annual technological review of the authorized Controlled Articles and their features to determine whether the policy and matrix needs to be revised.

Personnel using allowable Controlled Articles in an LA, TEMPEST Protected Area, or VTR must be cognizant of their surroundings and take into consideration classified activities that are occurring before using the devices. It is the individual's responsibility to adhere to the proper controls identified in the matrix.

If any Controlled Article 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 DOE HQ element HSO or an official under the supervision of AU-40. The device will be reviewed and analyzed by the AU-1.2 TSP Team and the Office of Classification (AU-60) to ensure that no classified information was captured during the unauthorized activity. 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 (see Chapter 11) will be initiated. The confiscated item may be sanitized and/or destroyed, in accordance with applicable policy.

Questions regarding the use of listed Controlled Articles or of devices not identified on the matrix in LAs, TEMPEST Protected Areas, or VTRs should be directed to the DOE HQ element HSO who will, as necessary, confer with AU-40 and/or the AU-1.2 TSP Team. DOE HQ element HSOs may request formal reviews by the AU-1.2 TSP Team of devices or capabilities not already listed in the matrix (see Chapter 9).

DOE Headquarters Controlled Articles Matrix

Please note that the below is strictly a guide. All TSCM and TEMPEST requirements within DOE Order 470.6 must still be adhered to. Please relay any questions or concerns to the Technical Security Program.

Controlled Articles and Uses	Area Type			Controls Required
	Vault Type Rooms (VTRs), SCIFs, and SAPs (TS, SAP, Sigma 14 or above) and TSCM areas.	Limited Areas that are Non-TSCM Areas	General Access Areas and Property Protection Areas	
Wireless Accessories (Wireless Earpieces and Microphone Enabled Headsets)	Prohibited		Allowed	No stipulations
Making Audio/Video Recordings	Prohibited			**Prohibited at all times.**
Radio Frequency (RF) Wireless Keyboards	Prohibited			**Prohibited at all times.**
Infrared (IR) Wireless Keyboards	Prohibited	Controlled (See #1 and 2 on right)	Allowed	1. Requires TSP approval. 2. Must remain in the OCIO installed configuration and be used in accordance with User Agreements.
Mobile, Wireless Capable Personal Electronic Devices (Cell Phones, Smart Phones, Laptop Computers, Music Players, E-book Readers, Tablets, etc.)	Prohibited (See #1,2,and 3 on right)	Controlled (See #1, 2, and 3 on right)	Controlled (See #1 on right)	**1. These devices must NOT be operated as wireless access points or hotspots in any area.** Must be secured during classified conversations or processing. Acceptable methods of securing include: 2. Placed in aircraft mode or turned off and stored in approved RF bag. 3. Removed from the area
Microphone Enabled Headsets	Prohibited (See #1,2,and 3 on right)	Controlled (See #1, 2, and 3 on right)	Allowed	**1. Any headsets with microphones connected to UNCLASS computer is prohibited.** **2. Any headset with noise cancelling at the earpiece is prohibited.** 3. Any headsets with noise cancelling control at microphone, with TSP approval, are allowed.
Electronic Medical Devices (See Note "A" below)	Prohibited		Allowed	No stipulations
Medical Devices (See Note "B" below)	Controlled (See #1 on right)		Allowed	1.Notify the elemental HSO or the TSP prior to introducing the device into the area. The TSP conducts a security review to ensure the device will not impact the security of classified systems or information within the area.
Personal Employee Assistance Devices (See Note "C" below)	Controlled (See #1 and 2 on right)		Allowed	1. Notify the elemental HSO or the TSP prior to introducing the device into the area. The TSP conducts a security review to ensure the device will not impact the security of classified systems or information within the area. **2. Any model that operates as a two-way wireless connection utilizing an internal microphone to transmit audio is PROHIBITED**
Non-Transmitting Devices (One-way Pagers, Radios, etc.)	Controlled (See #1 on right)		Allowed	1. Notify the elemental HSO or the TSP prior to introducing the device into the area. The TSP conducts a security review to ensure the device will not impact the security of classified systems or information within the area.
Wireless Mice	Controlled (See #1 on right)		Allowed	1. Must remain in the OCIO installed configuration and be used in accordance with User Agreements.
Other Remote Control Devices (TV/AV Remotes)	Controlled (See #1 and 2 on right)		Allowed	1. Requires TSP approval. **2. Any model that operates as a RF and/or two-way wireless connection is PROHIBITED**
DOE Owned Electronic Devices (i.e Laptops, Desktops, IPads) [4]	Controlled (See #1 on right)		Allowed (See #1 on right)	1. Permitted items are outlined by the ODFSA. Permitted items must used and maintained in accordance with the OCIO approved User Agreement which specifies applicable security precautions.
Dedicated and Wired Telephone and Video Teleconferencing Equipment (VOIP, POTS, ISDN, etc.)	Controlled (See #1 and 2 on right)		Allowed (See #2 on right)	1. Requires TSP approval. *(See Chapter 2, Section 205 of HQS Facilities Master Security Plan for instructions and form to submit for TSP approval)* 2. Must remain in the OCIO installed configuration and be used in accordance with User Agreements.

NOTES:

A) Electronic Medical Devices are Medical Devices that have capabilities that may pose risks to National Security Information Systems.

B) Medical Devices are intended for use in the diagnosis of diseases or other conditions; or in the cure, mitigation, treatment, or prevention of disease; or intended to affect the structure or any function of the body which does not achieve its primary intended purpose.

C) Personal Employee Assistance Devices are those devices that may serve a medical purpose, but are not necessary on an uninterrupted basis. They offer convenience (i.e., fitness trackers) or offer relief from a disability.

D) DOE Owned Electronic Devices - Even if equipment is provided and owned by DOE, DOE Order 470.6 must still be followed and all equipment coming into Limited Areas must be inspected prior to entering the area.

Wireless transmitters within 100 feet of classified systems require a Transmitter Review by the DOE Certified TEMPEST Technical Authority

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-41. 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 HSO must coordinate with the Technical Security Program (TSP) to have the item inspected/approved as identified in the Chapter 9, HQFMSP. Requests to use a prohibited Controlled Article in an LA, TEMPEST Protected Area, or VTR must be coordinated between the DOE HQ element HSO, AU-41, and AU-1.2 TSP Team. The request must contain the following information:

- Detailed description of the Controlled Article,
- Name and contact information of the individual directly responsible for the item,
- DOE HQ building and room(s) where the item will be used,
- Justification for its use, and
- How long it will be needed.

The AU-1.2 TSP Team will inspect the item in accordance with Chapter 9 of this Plan. If approved, the DOE HQ element HSO and AU-41 will develop a risk assessment, mitigations, and a memorandum from the DOE HQ element manager to the Director, AU-41 that contains the:

- Information from the request,
- Description of the risk assessment,

- Mitigating processes/actions, and
- Certification of acceptance of the risk.

AU-40 will issue an approval certificate/memo to the DOE HQ element HSO that must be readily available upon request as long as the item remains in use.

The approved request is valid for the specified time period, not to exceed one year. Renewal requests must be submitted to AU-41 at least 90 days prior to the expiration of the existing approval to permit proper review.

Permanent removal of the approved item will be communicated to AU-41 by the DOE HQ element HSO via memorandum or email.

Photography in an LA

Photography is not permitted in SAs approved for TS, SCI, or SAP information or in TEMPEST Protected Areas. Photography in permitted SAs for such events as birthdays, promotions, award ceremonies, etc. requires written approval from the DOE HQ element HSO (Attachment 4).

The request to conduct photographic activities in a permitted SA must originate from a Federal employee in a supervisory position and contain the following information:

- Date(s) the camera will be used,
- Building and room number(s) where the camera will be used,
- Purpose of photography,
- Name of the person using the camera, and
- Description of the equipment to be used. (Note: Only digital photography equipment is allowed. It is preferred that cameras maintained by AU-40 at both the Forrestal and Germantown facilities, be used as these devices have already been approved for use in permitted SAs. Use of a personally-owned camera will require approval of AU-41 in accordance with the controlled article process described in the previous section of this Chapter, i.e., Authorization for Use of a Prohibited Controlled Article.)

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 the HSO Program Manager in AU-41.

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. The following procedures must be adhered to while photographic equipment is being used in a permitted SA:

- All classified and sensitive matter must be removed from the camera's view before taking pictures.
- All classified computing must cease and computer monitors turned off.
- Only still photography is authorized.
- 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 such as card readers, personal identification number (PIN) pads, door locks, secure telephone devices, sensors, motion detectors, etc., that are not visible to the general public.
- Pictures must not show any planning or project calendars.
- An authorized occupant of the area must be present during all picture taking.

At the conclusion of the photography, the camera and/or media must be managed as classified "working papers" and submitted to a Derivative Classifier for review prior to being used for any purpose. If necessary, the AU-1.2 TSP Team will remove any identified classified or sensitive information from the camera and/or media prior to returning the sanitized camera/media to the photographer.

Classified Meetings

Not all LAs and VTRs are approved for classified discussions. The Security Certificate (see Section B. of this Chapter) posted at the entrance for each LA and VTR indicates if the area is approved for classified discussion and the level and category of the classified information allowed to be discussed; and whether the area is approved for amplified discussion, i.e., use of microphones, polycoms, speaker phones, or any other means used to amplify the sound.

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 may be openly announced.

DOE field personnel or employees of other government agencies (OGAs) who are scheduled to attend a classified meeting at a DOE HQ facility, may need to have their security clearances passed through AU-43, Office of HQ Personnel Security Operations, prior to the meeting (see Chapter 3, Section 306, Passing Clearances for Classified Meetings and Visits, of this Plan).

The host of a classified meeting must ensure that:

- All participants have the requisite security clearance and need to know,
- All Controlled Articles are managed in accordance with the requirements indicated in this Chapter,
- 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 manage all notes as classified working papers until they have undergone a classification review, and
- All classified matter is properly protected during the meeting.

Modification of LAs and VTRs

Changes to the physical layout or the type of classified activities conducted; or an increase in the classification level or category of information managed within an established LA or VTR must not be implemented without authorization in order for the area to maintain its SA certification.

Proposed changes must be provided to the DOE HQ element HSO for initial review. If needed, the DOE HQ element HSO will develop and submit a new SA A&A Request Package consisting of the request (Attachment 1) and SA A&A Request Worksheet, (a fillable PDF form available from AU-41) as described in Section A, Establishing LAs and VTRs, in this Chapter, including a justification and describing the modification.

The SA A&A Request will be managed utilizing the same processes described in Section A of this Chapter.

If the proposed changes are allowed, a new SA Approval Certificate may be issued for the area upon completion of the proposed changes, any required security modifications, and/or implemented mitigations.

C. Deactivating LAs and VTRs:

When an LA or VTR is no longer required, the DOE HQ element is responsible for ensuring all classified matter is destroyed or relocated to another approved LA or VTR in accordance with applicable DOE HQ CMPC requirements, and all classified activities cease.

The following description identifies the overall responsibilities and processes required for the completion of the deactivation of an LA or VTR.

1. The DOE HQ element HSO submits an SA A&A Request Package, including the applicable request (Attachment 1) and SA A&A Request Worksheet (a fillable PDF form available from AU-41) to the Director of AU-41, indicating that an existing LA or VTR requires deactivation.
2. The AU-41 Director forwards the SA A&A Request Package to the AU-41 SA Program Management Team for action.
3. HSOs are responsible for reporting bi-weekly status updates to the SA PM to be able to track progress of the SA during the deactivation/decertification.

4. The AU-41 SA Program Management Team conducts a review of the LA or VTR. After it has been verified that all classified matter has been removed and all classified activities have been terminated, the AU-41 SA Program Management Team transmits a memorandum to the DOE HQ element HSO approving the deactivation of the LA or VTR.
5. After receiving approval to deactivate the LA or VTR, the DOE HQ element HSO coordinates with the AU-41 Physical Protection Team to have all intrusion detection and access control equipment removed, as necessary.
6. The DOE HQ element HSO informs the AU-41 SA Program Management Team after confirming that the removal of all intrusion detection and access control equipment has been completed.
7. The AU-41 SA Program Management Team updates the HQ SA Database to reflect the deactivation and notifies the DOE HQ element HSO, DOE HQ Protective Force, AU-1.2 TSP, and MA, as appropriate.

Points of Contact

For the names and contact information for those assigned the positions identified in this section, contact AU-41 by email (*preferred method*), or by phone, call (301) 903-1960 or (301) 903-9979.

For the names and contact information for those assigned the positions identified in this section, email TecSec@hq.doe.gov or call (301) 903-9992.

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

For names and contact information for those occupying the information security, personnel security, and TSP positions identified in this section, call (301) 903-1960 or (301) 903-9979.

For the names and contact information for TSP call (301) 903-9992 or the HQ Secure Phone Group at (301) 903-5062.

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

To contact AU-41 SA PM team by phone, call (301) 903-1960 or (301) 903-9979.

Forms/Samples/Graphics:
Attachment 1: Sample SA A&A Request Memorandum
Attachment 2: Sample SA Approval Certificate
Attachment 3: Residential vIPer Telephone Equipment Security Plan
Attachment 4: Sample Request to Use a Camera in a Limited Area

ATTACHMENT 1: Sample Security Area Request Memorandum

MEMORANDUM FOR: (NAME), DIRECTOR
OFFICE OF PHYSICAL PROTECTION
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 Advice and Assistance Request 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 _____.
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 Advice and Assistance Request 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 _____.

Or

The Office of _____ is requesting your assistance in deactivating the Security Area in Room _____ at the _____ Building. Attached is a Security Area Advice and Assistance Request 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 _____.

Official Use Only Stamp

Attachment(s)
OFFICIAL USE ONLY (When filled in)

ATTACHMENT 2: Sample Security Area Approval Certificate

UNCLASSIFIED

Headquarters Facility Security Area Approval Certificate

The following area

EXAMPLE EXAMPLE

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

Vault Type Room

For the following classified activities

Top Secret Restricted Data

Computer Processing, Secret Restricted Data & Sigma	Reproduction, Secret Restricted Data & Sigma 15
Open Storage, Secret Restricted Data	Receipt and Transmit, Secret Nuclear Security Inform
Closed Storage, Top Secret Restricted Data	Discussion Amplified, Secret Restricted Data
Destruction, Secret Restricted Data & Sigmas 15-20	Silent Review, Top Secret NATO / Sigma
Discussion Non-Amplified, Top Secret Nuclear Security Information	
Discussion Amplified with STE/ViPer, Secret Restricted Data NATO/Sigma	
Discussion Non-Amplified with STE/ViPer, Top Secret NATO / Sigma	

Approving Authority

11/7/2016
Date

UNCLASSIFIED

Attachment 3: Residential vIPer Telephone Equipment Security Plan

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

Attachment 4: 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 TSP 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.

1. 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 and the total shutdown of any classified computer system.
2. Only still photographs are authorized.
3. I will not photograph any Security Area signs that are not visible to the general public.
4. 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.
5. I will not photograph any planning or project calendars.
6. An authorized occupant of the area will be present during the entire photography session.

7. 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.
8. The camera and/or its media will be stored as classified matter until a DC determines the photographs are unclassified.
9. In the event classified matter appears in any photograph, the camera and/or its media will be sanitized by the HQ TSP Team.

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

APPROVED: _____

DISAPPROVED: _____

DATE: _____

cc:
Director, Technical Security Program (AU-1.2)
Security Area Program Manager – GTN/FOR (AU-41)
User's HSO
Director, Office of Physical Protection (AU-41)