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

February 15, 2024: Revised Advice &Assistance (A&A) Submission process and added the Random Review Process

January 25, 2021: Webcam User Agreement added to Chapter 2 download page

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
- 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 (HQFMSP) 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 – 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 and/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 CHG 4 (LTDCHG), *Information Security*.

Vault-Type Room – A VTR is a room having combination-locked doors (X-09 or X-10 series combination lock) and 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* TS can be locked in a VTR within a property protection area (PPA) or outside of a SA, as long as the VTR is 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 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 EHSS-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. An electronic file in SharePoint for each LA or VTR is created and maintained by the HQ SA Program Manager, within the Office of Physical Protection (EHSS--41), Office of HQ Security Operations (EHSS-40), Office of Environment, Health, Safety, and Security (EHSS), 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:

- Establishing LAs and VTRs
- 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
- Deactivating LAs and VTRs
- Random Review Process

Section 201
Establishing LAs and VTRs

The establishment of LAs and VTRs at DOE HQ must be approved by the Director of EHSS-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

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.

1. The DOE HQ element HSO submits an SA Advice and Assistance (A&A) Request Package requesting a review to prepare for the establishment of a new LA or VTR via the Security Areas SharePoint page (access is limited to only HSOs.) The SA A&A Request Package consists of the Security Area Request Memo requesting assistance in establishing a new LA or VTR, the Security Area Request Worksheet (available on the aforementioned SharePoint page, and a blueprint/drawing of the proposed LA or VTR. These documents will be uploaded to the SA SharePoint Worksheet page (attachments are added at the bottom of page.) 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.
2. Notification of the SA A&A Request Package comes to the SA Program Management Team via the Security Area Mailbox. EHSS-41 may coordinate with the DOE HQ element HSO and a team of representatives from the EHSS Office of Technical Security (EHSS--54), MA--432, NA-IM, and/or the National Nuclear Security Administration (NNSA). The EHSS--41 HQ SA Program Management Team will conduct a physical security review and walk-through of the proposed LA or VTR. After the security review, EHSS-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 EHSS-54, as applicable, to arrange for needed construction, other physical changes, and services for the proposed LA or VTR. Procedures for obtaining EHSS-54 Technical Security Program (TSP) Team services are provided in Chapter 9, Technical Surveillance Countermeasures, of this Plan.

   Requirements for 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)*. For example, 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.

3. 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.
4. 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.
5. The HQ SA Program Management Team 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 and certificate to the requesting DOE HQ element HSO. In addition, the HQ SA Program Manager updates applicable DOE HQ databases and SharePoint library to include the new SA.

Section 202
Managing LAs and VTRs

Approval Certificate

The Sample SA Approval Certificate must be prominently displayed at eye level near or as close as possible to each entrance of the LA or VTR to inform personnel of 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. For an LA, one escort is required per five visitors; for a VTR, the escort ratio will not exceed one escort to three visitors. Need to know must be established before permitting entry into a VTR. DOE Order 473.1A requires access controls at VTRs to include a log and record of all visitors. There is no specified format for the log, however, at 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).

For more on escort requirements reference Chapter 1, Section 107, HQFMSP.

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.

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 are 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 (only X-09 or X-10 series locks are approved as X-07/X-08 are end of life) is starting to fail, the HSO needs to be notified so that he/she can initiate the process to have the lock examined/repaired before it totally fails. The HSO will need to communicate with the organization's 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 EHSS-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 within the Office of Corporate Security Strategy (EHSS-54).

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 their email mailbox using the Secure Phone Workorder Request (Chapter 9)

Residential vIPer Services

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 their email mailbox), the Director, EHSS-41, and the EHSS-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.
    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. Username 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.
    d. 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, EHSS-40, or designee, 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 the Director, EHSS-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:

- EHSS-54 TSP Team personnel,
- DOE HQ security personnel installing, maintaining, testing, or removing access control and intrusion detection systems (IST),
- 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

- EHSS-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.

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 described in the Controlled Article Matrix maintained by the EHSS-54 TSP Team. This Matrix describes controlled Article use and prohibitions in LAs and VTRs at DOE HQ.

The EHSS-54 TSP Team conducts an annual technological review of the authorized Controlled Articles and their features to determine whether the policy and matrix requires revision.

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 EHSS-40. The device will be reviewed and analyzed by the EHSS-54 TSP Team and the Office of Classification (EHSS-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, an Initial Report if Headquarters Security Incident as described in Chapter 11 on page 11-3 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 EHSS-40 and/or the EHSS-54 TSP Team. DOE HQ element HSOs may request formal reviews by the EHSS-54 TSP Team of devices or capabilities not already listed in the matrix (see Chapter 9).

Matrix 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 Controlled Articles:

The Office Director requesting authorization for Controlled Articles or the use of selected device features must submit the request via memorandum to the Director, EHSS-41. The HSO of the requesting organization must be copied on the memorandum. The Sample Memo Request for Authorization of Controlled Articles in a Security Area 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 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, EHSS-41, and EHSS-54 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 EHSS-54 TSP Team will inspect the item in accordance with Chapter 9 of this Plan. If approved, the DOE HQ element HSO will develop a risk assessment, mitigations, and a memorandum from the DOE HQ element manager to the Director, EHSS-40 that contains the:

- Information from the request,

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

EHSS-40 will issue an approval 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 EHSS-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 EHSS-41 by the DOE HQ element HSO via memorandum or email.

Unclassified Individual Desktop VTC/Webcam requirements

This guidance only applies to unclassified individual desktop video teleconferencing (VTC) system or "webcams" webcam systems connected to individual office computers on the unclassified systems at HQ. These guidelines do not apply to dedicated/fixed VTC equipment designed for and located in conference rooms, meeting rooms, or otherwise permanently designated offices. Requirements for other than individual desktop activities are not covered in the guidance.

Before individual unclassified desktop audio/visual teleconferencing equipment or "webcams" utilizing OCIO VTC capability can be introduced into and used in areas where any classified or sensitive unclassified information is stored, reviewed, discussed, processed, produced, or displayed, a signed and approved Webcam User Agreement must be in place.

Any changes to hardware/software/configurations/defined area activities or construction require a review of any approved Webcam User Agreements.

Any deviations to these requirements must be approved by the ODFSA on a case-by-case basis for mission requirements.

The list of authorized equipment approved for use for desktop VTC (webcam / headset / disconnect) is contained in Chapter 9.

Other security disciplines and/or the DOE OCIO may institute additional security requirements.

- No Personal equipment is authorized for conducting video teleconferences.
- Government issued devices that utilize internal Webcams/Microphones (laptop, iPad, cellphone etc.) are not authorized for use within security areas for VTC.
- All VTCs within a security area must take place over the DOE hardwired (non-wireless) network.
- Automatic or hands-free answering capability must be disabled from the system and an overt action (mouse click, button push, etc.) by the user is required to establish any video or audio connection once the webcam is connected to the system.
- The VTC equipment must be marked unclassified.

- Desktop VTC equipment may not be used as part of a shared systems bridging classified and unclassified systems utilizing a switch/hub/KVM type device.
- The equipment must be installed and operated by authorized individuals cognizant of the operational functionality of the system, associated software, equipment, and security requirements for conducting desktop VTCs.
- The use of an approved manually operated electrical disconnect device must be used.
- Teleconferencing users must inform individuals in the immediate and surrounding areas that the webcam is in use and that classified information may be subject to compromise during the duration the webcam is connected.
- Webcam must be pointed in a direction to ensure that any sensitive information is not compromised.
- Personally Identifiable Information (PII), and classified matter will not be in view of the Webcam.
- Signs must be placed in and around the area where the teleconferencing is occurring warning individuals to restrict all discussions involving classified information and unclassified control information not part of the VTC session.
- The DOE cognizant security authority will conduct oversight of the teleconferencing activities to ensure that participants and those associated with the activity adhere to established security procedures and policies.

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, see the Sample Request to Use a Camera in a Limited Area.

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 EHSS-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 EHSS-41 in accordance with the controlled article process described in the previous section of this Chapter, i.e., Requesting Authorization for Additional Controlled Article.

EHSS-40 has government-owned cameras available at both the Forrestal and Germantown facilities. HQ personnel are encouraged to use the EHSS-40 cameras instead of personally owned devices because the EHSS-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 EHSS-41.

Written approval from the element HSO is required before using a camera. See the Sample Request to Use a Camera in an LA. 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 EHSS-54 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 EHSS-82, 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 Security Area Request Memo and the Security Area Request Worksheet via the Security Areas SharePoint page 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 201 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.

Section 203
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 Security Area Request Memo and the Security Area Request Worksheet via the Security Areas SharePoint page as shown in Section 201.
2. The EHSS-41 SA Program Management Team will receive notification of the request via the SA SharePoint page.
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 EHSS-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 EHSS-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 EHSS-41 Physical Protection Team to have all intrusion detection and access control equipment removed, as necessary.
6. The DOE HQ element HSO informs the EHSS-41 SA Program Management Team after confirming that the removal of all intrusion detection and access control equipment has been completed.
7. The EHSS-41 SA Program Management Team updates the HQ SA Database and SharePoint to reflect the deactivation and notifies the DOE HQ element HSO, DOE HQ Protective Force, EHSS-54 TSP, and MA, as appropriate. Upon completion, certificates will need to be removed and properly disposed of by the HSO.

Section 204
Random Review Process

1. The SA Program Management Team (PMT) annually generates a list of randomly selected spaces.
2. If selected, notification will be sent in the form of a memorandum that will be emailed to the HSO to inform them of their space(s) being chosen.
3. Coordination will be undertaken between the SA PMT and the HSO to find a mutually agreeable time in which to review the selected LA or VTR.
4. The SA PMT will collect data and generate a report based on the current condition of the space.
5. If lack of compliance is noted:

    a. The possibility of a work stoppage may be implemented.
    b. HSO will identify a plan of action in writing within 45 days of receiving the report.
    c. After the plan of action is received by the SA PMT, the HSO will have 90 days to correct all identified deficiencies.
    d. Should additional time be required, a justification for extension beyond 90 days must be requested to and approved by the ODFSA.

6. An updated Security Area Certification with corresponding date will be provided.

**NOTE* Once a new certificate is provided, this space will be exempt from the random selection process for a period not to exceed 3 years.*

Points of Contact

For the names and contact information for those assigned the positions identified in this section, contact EHSS-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 EHSS-41 SA PM team by phone, call (301) 903-1960 or (301) 903-9979.

Samples/Graphics:

Sample Security Area Request Memo
Sample SA Approval Certificate
Residential vIPer Telephone Equipment Security Plan
Sample Request to Use a Camera in a Limited Area
Sample Memo Request for Authorization of Controlled Articles in Security Area
Webcam User Agreement
DOE Headquarters Controlled Articles Matrix