Introduction

This local addendum is keyed to relevant paragraphs in the Overlook Systems Technologies, Inc. Standard Practice Procedure (SPP). It is intended to spell out details of local procedures and does not supercede or override any requirements identified in the basic SPP.

Many of the procedures contained herein will normally be performed by the Facility Security Officer (FSO) as part of the FSO’s duties. However, in the absence of the FSO, other Overlook employees must be able to step in and properly control, receive, safeguard, and transmit classified information as necessary.

Therefore, all Overlook employees assigned to the Vienna office are responsible for the contents of this addendum. Cleared employees, in particular, must be aware of all requirements and procedures for safeguarding classified information. Employees who visit from other sites and will require access to classified information must also read and comply with these local requirements.

Ronald T. Hansson
Facility Security Officer
Vienna, VA
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-200.</td>
<td>SAP and SCI Directives</td>
</tr>
<tr>
<td>1-300.</td>
<td>Reporting Procedures</td>
</tr>
<tr>
<td>2-200.</td>
<td>Pre-employment Screening for Security Clearance Eligibility</td>
</tr>
<tr>
<td>2-300.</td>
<td>FOCI and the SF-328</td>
</tr>
<tr>
<td>5-100.</td>
<td>Physical Security Specifications.</td>
</tr>
<tr>
<td>5-101.</td>
<td>Warning Signs</td>
</tr>
<tr>
<td>5-102.</td>
<td>Random Inspections for Unauthorized Classified Transmission</td>
</tr>
<tr>
<td>5-103.</td>
<td>Annual Perimeter Control Review</td>
</tr>
<tr>
<td>5-104.</td>
<td>End of Day Security Checks</td>
</tr>
<tr>
<td>5-105.</td>
<td>Emergency Procedures</td>
</tr>
<tr>
<td>5-200.</td>
<td>Procedures for Receipt of Signature/Classified Mail</td>
</tr>
<tr>
<td>5-201.</td>
<td>Document Accountability Numbers (DANs)</td>
</tr>
<tr>
<td>5-202.</td>
<td>Classified Material Database Record (CMRD)</td>
</tr>
<tr>
<td>5-203.</td>
<td>Document Accountability Database</td>
</tr>
<tr>
<td>5-204.</td>
<td>Generation of Classified Material</td>
</tr>
<tr>
<td>5-205.</td>
<td>Working Papers</td>
</tr>
<tr>
<td>5-300.</td>
<td>Storage and Handling of Classified Material</td>
</tr>
<tr>
<td>5-301.</td>
<td>Identification of Classified Work Areas</td>
</tr>
<tr>
<td>5-400.</td>
<td>Transmission of Classified Material</td>
</tr>
<tr>
<td>5-401.</td>
<td>Preparation and Receipting</td>
</tr>
<tr>
<td>5-402.</td>
<td>Addressing Classified Material</td>
</tr>
<tr>
<td>5-403.</td>
<td>Use of Commercial Passenger Aircraft for Hand-carrying Classified Matl.</td>
</tr>
<tr>
<td>5-404.</td>
<td>Local Courier Authorizations and Briefings</td>
</tr>
<tr>
<td>5-600.</td>
<td>Reproduction of Classified Material</td>
</tr>
<tr>
<td>5-700.</td>
<td>Destruction</td>
</tr>
<tr>
<td>5-800</td>
<td>Special Procedures for Top Secret Material</td>
</tr>
<tr>
<td>6-100.</td>
<td>Incoming Visitors</td>
</tr>
<tr>
<td>6-200.</td>
<td>Government Sponsored Meetings at Overlook Vienna Facility</td>
</tr>
<tr>
<td>6-201.</td>
<td>Scheduling Classified Meetings</td>
</tr>
<tr>
<td>6-202.</td>
<td>Notifications of Classified Meetings</td>
</tr>
<tr>
<td>6-203.</td>
<td>Planning for Classified Meetings</td>
</tr>
<tr>
<td>6-204.</td>
<td>Meeting Day Procedures</td>
</tr>
<tr>
<td>10-700.</td>
<td>NATO Storage</td>
</tr>
<tr>
<td>App A.</td>
<td>Classified Material Database Record (CMRD)</td>
</tr>
</tbody>
</table>
1-200. SAP and SCI Directives. The NISPOM, corporate SPP, and this addendum to the SPP spell out requirements and procedures for the handling and safeguarding of collateral classified information. Overlook Vienna currently works with both Special Access Program (SAP) and Sensitive Compartmented Information (SCI) data. When performing work in these arenas, Overlook employees will refer to the relevant Standard Operating Procedures (SOP) for these functions, as well as to the appropriate government issued directives regarding them. These SOPs are available from the Principal Corporate Security Officer (PCSO), who acts as the Overlook Vienna Contractor Program Security Officer (CPSO) for SAP contracts and Contractor Special Security Officer (CSSO) for SCI tasks.

1-300. Reporting Procedures. In accordance with the NISPOM and the Overlook SPP, all cleared employees are responsible for reporting specified information to their FSOs. When making such reports, the reporting parties must bear in mind that a compilation of data regarding a security violation or incident, or the possible compromise of classified information, could itself be classified. Therefore, initial reports made via unsecured means, such as email or telephone, must be limited to identification of the type of incident and its seriousness. Detailed reporting must be made face-to-face with the FSO or via secure telephone (STE).
2-200. **Pre-employment Screening for Security Clearance Eligibility.** Currently, Overlook contracts U.S. Homeland Investigations (USHI) to conduct pre-employment investigations of potential new hires to confirm education and work eligibility. This is a Human Resources function and cannot be used to determine security clearance eligibility. Therefore, the hiring manager will forward a candidate’s SSN to the FSO, who will conduct a JPAS check for current status. The FSO may only inform the hiring manager of the candidate’s current clearance status and eligibility for reinstatement. Any other information in JPAS must be held in confidence. The FSO is responsible for protecting identity information, whether or not the candidate is hired. If and when a candidate is determined not to meet hiring criteria, any personal information about the candidate held by the FSO will be destroyed.

2-300. **FOCI and the SF-328.** Since the FSO for the Vienna office also serves as the PCSO, collection of data regarding Foreign Ownership, Control, or Influence (FOCI), contracts with foreign persons, and foreign investments will be made by the Vienna FSO, who will update the SF-328 and send copies to the Defense Security Service (DSS) and other Overlook facilities.
5-100. Physical Security Specifications. Overlook Systems’ office in Vienna is located on the fourth floor of a multi-tenant office building at 1950 Old Gallows Rd. The immediate area is predominantly office buildings and retail stores, with some smaller professional and retail buildings. The building is open and access is uncontrolled between the hours of 7:00 a.m. and 6:00 p.m. Monday through Friday. At all other times, the doors are locked and access is by a proximity card access control system. Elevators are not restricted. Access to the employee-only door of the Overlook suite is by key lock. From 8:00 a.m. to 5:00 p.m., the main entrance to the suite is controlled by a keypad electronic door release, with a call button for visitors. The Executive Assistant normally sits in the suite lobby and responds to the call button. In the absence of the Executive Assistant, the Accounting Assistant responds to the call button. Additionally, the internal hallway leading from the key actuated door is CCTV monitored by the FSO, as well as the portion of the lateral hallway immediately adjacent to the SCIF/SAPF and Alarmed Room. The FSO issues keys to employees and recovers them when individuals terminate employment. Due to the small number of employees, no badging system is in place, either for employees or for visitors. All employees are charged with challenging unescorted visitors, whether recognized or not. Visitors to the Overlook Systems Vienna office must be escorted at all times to preclude inadvertent access to classified, For Official Use Only, Proprietary, or Privacy Act protected information.

5-101. Warning Signs. The following warning sign will be posted prominently in the main lobby and at the employee only entrance. “All persons who enter or exit the facility are subject to inspections of their personal effects, to include bags, parcels, briefcases, totes, computer cases, and luggage, to preclude the unauthorized introduction or removal of classified material.”

5-102. Random Inspections for Unauthorized Classified Transmission. The FSO will conduct random sample inspections of persons entering or departing, including visitors, employees, vendors, and consultants, for the purpose described above. Results of these inspections will be maintained in FSO files for two years.

5-103. Annual Perimeter Control Review. The FSO will perform an annual review of perimeter access control measures, in conjunction with the annual self-inspection, to determine if these measures should be altered or upgraded to reflect changes in access requirements.

5-104. End of Day Security Checks. Since all classified material is stored within the SCIF/SAPF and the Alarmed Room, it is the responsibility of the individuals who opened these areas to ensure that all classified material containers are closed and locked and the areas secured at the end of the day. The FSO will perform an end-of-day security check of the SCIF/SAPF door and the Alarmed Room door to ensure that they are locked and that the responsible party has recorded the action in the Open/Closed Record. In the absence of the FSO, another designated cleared employee will conduct the end-of-day checks. The FSO will periodically conduct random end-of-day corporate office checks to ensure that no classified material is left out of secure storage.
5-105. Emergency Procedures. The basic premise in the following procedures is that safety of life and limb takes precedence over safeguarding classified material. With that in mind, all cleared employees will make reasonable attempts to secure classified material prior to evacuation in the event of an emergency.

a. Sounding of Emergency Evacuation Alarm.

(1) When the building emergency evacuation alarm sounds, all personnel will immediately begin preparations for evacuation. If classified material can be stored in containers, the SCIF/SAPF or designated restricted area (Alarmed Room) evacuated, AND the appropriate area spin-dial lock secured within 30 seconds, all efforts will be made to do so.

(2) When classified computer processing is in progress, normal downgrading and shutdown procedures will usually exceed these time constraints. Therefore, the system will be immediately powered off and, if possible, the removable hard drive and other media returned to secure storage.

(3) If the volume of classified material in use precludes storage in containers, then the AIS system will be powered off, containers locked, and the SCIF/SAPF or Alarmed Room evacuated.

(4) The doors to these facilities should always be locked upon evacuation; however, the alarms should NOT be set.

(5) When classified material cannot be secured in containers prior to evacuation, the cognizant employee(s) will notify the FSO at the evacuation mustering point.

(6) When notified that classified material could not be properly secured within the SCIF, the FSO will contact a senior member of the Emergency Response Team (usually, the fire department) to determine the likelihood that the SCIF perimeter was breeched by the team during response actions.

(a) If the SCIF perimeter was not breeched, the FSO will thank the ERT for their assistance, conduct an Administrative Inquiry of the circumstances, determine the probability of loss or compromise of classified data, and report within 24 hours to DSS.

(b) If perimeter penetration DID occur, the FSO will arrange interviews of the responding ERT members to determine the probability of compromise and report immediately to DSS.

(c) If ERT members gained access to classified information, they will be briefed on their responsibilities to protect it and asked to sign an Inadvertent Disclosure debriefing form.

(d) In all cases, as soon as access to the building is authorized, the FSO will work with at least one other cleared employee to open the SCIF/SAPF and Alarmed Room, inventory all unsecured classified material, and secure it properly.
(7) When an employee is reading or editing classified material in an office at the time the Evacuation Alarm is sounded, he or she will collect the material in the expansion folder carrier and take it to the evacuation muster site, maintaining personal control to preclude inadvertent access. The FSO must be immediately notified of this situation. In most cases the FSO will take custody of the material.

(8) If sufficient damage has occurred to the facility or building that access to the SCIF/SAPF, Alarmed Room, or work spaces is no longer possible, the FSO will notify DSS of the situation and immediately establish procedures for protection of the perimeter of the building and safeguarding of the facility.

(9) In all cases, the FSO will conduct a post-evacuation review to determine whether all appropriate procedures were followed, whether they were adequate to the situation, and whether or not revisions or changes are indicated.

b. Natural or Man-made Disaster Occurring When the Facility is Unoccupied.

(1) Whenever the unoccupied facility is struck by a disaster (earthquake, hurricane, tornado, fire, etc.) the FSO will make every effort to determine the current status of classified material.

(2) When access to the facility or building is no longer possible, the FSO will notify DSS of the situation and immediately establish procedures for protection of the perimeter of the building and safeguarding of the facility.

(3) Whenever possible, if the FSO can gain access to the facility, but its integrity no longer affords sufficient safeguarding protection for classified material, the FSO will make arrangements to transport the classified material to an alternate storage site. At this time, that site is the OSD/CIO facility in Arlington, VA.

(4) In all cases where safeguarding is no longer possible, the FSO will notify DSS immediately.

5-200. Procedures for Receipt of Signature/Classified Mail.

a. Authorized Signatories. Since U. S. Postal Service signature mail of any type, as well as FedEx and other courier service packages, may contain classified material, only cleared employees are authorized to sign for them. As a rule, the FSO will open signature mail to determine if it contains classified material and take action appropriately. In the absence of the FSO, the Executive Assistant or the Accounting Assistant will sign for and take action on signature mail. Although Overlook Systems does NOT have an authorized FedEx classified mailing address, many government and non-government agencies are less than observant in this regard and may transmit classified material by any of these means. Therefore, packages and envelopes delivered by FedEx, UPS, and similar carriers must be signed for by a cleared Overlook employee.

b. Opening Mail Containing Classified Material. Prior to opening any envelope or package which could contain classified material, the FSO or designated signatory, will check the package to determine if the wrapping has been tampered with. In the event tampering is indicated, the FSO will immediately be notified and a report of the circumstances prepared in accordance with NISPOM reporting requirements. If not
tampering is indicated, the package will be opened, the inner wrapping checked for tampering, any attention lines on the inner wrapping address noted, and the classified material removed. Wrappings will be checked to ensure they contain no classified material and will then be disposed of as waste. The FSO or designated signatory will then check the enclosed Classified Material Receipt (CMR) against the document(s) contained in the package. If there are no discrepancies, the FSO will then sign and date the CMR, mail the original signed CMR to the mail originator and keep a copy for record purposes. Each incoming document will be assigned a Document Accountability Number (DAN) as described below, the DAN printed on the document, and an appropriate Classified Material Cover sheet completed and applied to the front and back of the document. A Classified Material Database Record (CMDR) will be completed as described in paragraph 5-202, and the document stored in the designated GSA container.

5-201. Document Accountability Numbers (DANs).

a. Purpose. DANs are used to identify and help locate classified documents and material within Overlook Systems facilities. While not required by the NISP as a security function for Secret or Confidential material, they greatly facilitate retrieval of material for reference and use, as well as enabling efficient reviews of document holdings upon completion of contracts, etc.

b. Prefix. DANs begin with an alphabetic prefix which identifies the category of material and the Overlook location as follows:

OSVA = Overlook Systems Virginia (Collateral Documents)
OSVATS = Overlook Systems Virginia (Collateral TS Documents) (now unused)
OSVASC1 = Overlook Systems Virginia (SCI Documents)
OSVASAP1 = Overlook Systems Virginia (SAP1 Documents)
OSVASAP2 = Overlook Systems Virginia (SAP2 Documents) (now unused)

(The prefix for Overlook Systems California would be OSCA***)

Note: with the exception of TS collateral documents (which are required by the NISP to be controlled, stored, and identified separately from Secret and below material), documents are not numbered or sorted separately by classification. Also note that NATO and Foreign Government Information (FGI) are included with the collateral documents for numbering purposes, although they must be filed separately.

c. Year Identifier. The next portion of the DAN is the year that the document is recorded, separated from preceding and following portions of the DAN by hyphens. Each calendar year a new series of numbers is assigned. Hence, the identifying year portion of the DAN.

d. Numerical Identifier. The last portion of the DAN is a three-digit one-up series of consecutive numbers, which begins on 1 January each year with 001.

e. Number List. A list of numbers to be assigned for each category is maintained on sheets which are posted above the admin desks of the SCIF/SAPF and Alarmed Room appropriately. When assigning a number, first the classification of the item to be numbered is determined, then the next consecutive number in the appropriate series is lined out. This number is used to prepare a Classified Material Database Record.
5-202. Classified Material Database Record (CMDR).

a. Purpose. The CMDR is used as a paper back-up for the Document Accountability Database. It provides all the data necessary for database records and will be used as an input document.

b. Completion of the CMDR. Immediately upon assigning a DAN to a classified item, a CMDR will be removed from the drawer of the admin desk and completed as follows: (See Appendix A)

   (1) DOC NBR – Enter the complete DAN assigned.
   (2) COPY NBR – Enter the copy number of the item. (If more than one copy is printed, complete an additional copy of the CMDR for each copy; only enter variant information for copies 2 through XX).
   (3) DOC TYPE – Enter “PP” for paper, “CD” for Compact Disk, “HD” for Hard drive (only the ISSM is authorized to use this entry), or “O” for other (describe).
   (4) DOC DATE – Date of the material as printed on the document itself or as entered on the electronic media.
   (5) CLASSIFICATION – C, S, TS.
   (6) CAVEATS – Enter caveats, such as NOFORN, REL TO AUS, SI/TK, NATO, etc.
   (7) DECLASSIFY ON – Enter information from Declassify On lines of document
   (8) UNCLASSIFIED TITLE – Self-explanatory.
   (9) CONTRACT – Enter the contract number under which this document was developed or received; for example: W91WAW-10-C-0006. (This is used to identify documents which must be destroyed or moved to another contract upon contract completion.)
   (10) RCVD FROM – If received from another contractor or government site, identify. If created at OSTI Virginia, enter “OSVA”.
   (11) DATE RECEIVED – Enter date received. If created at OSTI Virginia, enter the date document was created (NOT Document Date, which may differ).
   (12) ORIG DOC NR – Enter the Originator’s Document Number (if any) for reference.
   (13) ORIG COPY NR – Similarly, enter the Originator’s Copy Number (if any)
   (14) TRANS METHOD – If received from outside OSTI, indicate “HC” for Hand-carried and the last name of the courier, “RM” for Registered Mail, “EM” for Express Mail, or “O” for Other (describe); if document originated at OSTI VA, enter ORIG.
   (15) KEY PERSON – Enter name of OSTI person most likely to need this material.

The following blocks are used if material is to be immediately moved to inactive status:

   (16) DISPOSITION – Enter “TRANS” for transmitted (either by mail, courier, or hand-carrying), “DEST” for Destroyed (usually by shredding), “INC” for Incorporated into another document, or “LOST.”
   (17) DISPOSITION DATE – Self-explanatory.
   (18) TRANSMITTED TO – Enter the contractor or government site to which the material was transmitted.
   (19) TRANSMIT BY – Enter the same codes as in block 14.
5-203. **Document Accountability Database.** The Document Accountability Database is a Microsoft Access database of all classified material held by Overlook Systems Virginia. It is used to prepare inventories of classified holdings, locate and retrieve specific documents or documents on identified subjects, prepare automated Destruction Reports, and identify documents for return or destruction at the completion of contracts. The database is maintained by the FSO/CSSO/CPSO from data provided by users, usually in the form of the CMDR.

5-204. **Generation of Classified Material.**

**a. Creating a Paper Document from the Classified AIS.** Originators will perform the following steps when creating paper documents.

1. **AIS System Security Plan (SSP) Procedures.** Users must first ensure that all required security procedures are followed when printing any information from the classified AIS.

2. **Assigning Document Account Numbers (DANs).** Prior to printing a document, assign a DAN as described in paragraph 5-201 and enter it as a footer to the document. In the case of documents prepared for signature by government customers, enter the DAN manually on the Overlook copy of the document.

3. **Print the document on the designated cleared printer, following instructions contained in the SSP.**

4. **Preparing the Cover Sheet.** Find the appropriate Classified Material Cover Sheet from the drawer in the admin desk and complete it. Ensure that the Contract Number block is filled in, as this identifies the authority for holding the document for future retention or destruction. Use the date the material was printed as the Date Received.

5. **Complete and file a CMDR as described in paragraph 5-202.**

**b. Creating a CD from the Classified AIS.** Normally, either the ISSM or the FSO will create electronic media, as most other users to not have privileges that allow them to do so. If authorized by the ISSM to do so, create the CD as follows.

1. **AIS System Security Plan (SSP) Procedures.** Be especially careful when creating classified electronic media to follow SSO security procedures.

2. **Assigning DANs.** When creating electronic media, ALWAYS assign a DAN. Electronic media are not to be handled as Working Papers and MUST be accounted for in the database.
3. Labeling the Media. As soon as the media has been written to, immediately affix the appropriate pre-printed media label (located in the Admin Desk) and complete it as indicated below:

   (1) Date: Enter the date media was created (not date of document) as YYYYMMDD.
   (2) Doc Nr: Enter the DAN (see above for DAN procedures).
   (3) CY: Enter the copy number (usually “1”).
   (4) Title: Enter the UNCLASSIFIED title and mark it “(U)”.
   (5) Classified by: Enter the name of the person who created the media:
   (6) Drvd fm: Enter the Derived From information (GPS SCG, etc.)
   (7) Declassify On: Enter the Declassify On information.

   In available blank space, rubber stamp the classification of the media in red. If rubber stamp is not available, print the classification in red. Be sure to include all caveats, such as NOFORN, REL TO ___, etc.

   Ensure that the media is stored in a transparent case so that the markings are clearly visible. If a label is included with the media case, do not obscure the media and its markings.

4. Preparing the Cover Sheet. Find a Classified Electronic Media Cover Sheet from the drawer in the admin desk and complete it as follows:

   (1) Control Number: Enter the DAN which you have assigned to the media.
   (2) Copy Number: Enter the copy number for each separate item of media.
   (3) Date Rcvd: Enter the date media was created (not document date).
   (4) Contract Number: Ensure this is completed, as it identifies the retention authority.
   (5) Declassify On: Enter from the files contained on the media.

   Fold the Cover Sheet in half and staple it to form an envelope. Insert the media into this envelope for storage or transmission.

5-205. Classified Working Papers. Classified Working Papers. Working papers are intended for short-term, temporary use. As such, they must be dated on the date of creation, marked with the overall classification and “Working Papers”, marked with the name of the creator, and destroyed when no longer needed. Retain Working Papers in an expansion folder labeled with the name of the creator/user and file in the appropriate security container. Using a Working Papers inventory form, identify each item contained in the expansion folder and include the inventory form with the WP items. Secret and below Working Papers retained more than 180 days after creation must be entered in the Document Accountability Database. Working Papers must be reviewed quarterly by their originator to ensure that they are still required and that they have not exceeded the 180 day limitation.

5-300. Storage and Handling of Classified material. All collateral classified material will be stored in the designated GSA Class VI cabinets, within the Alarmed Room.
Employees will perform classified processing ONLY on the designated stand-alone computer within the Alarmed Room and according to the procedures established by the SSP.

Authorized personnel may remove Secret & Confidential collateral documents from the Alarmed Room to their offices to read or manually edit them. Such material must have an appropriate classified material cover sheet, designating the classification level, attached to both the front and back of the document and must be transported in a covered expansion folder to preclude inadvertent disclosure during transit. While classified work is in progress, the employee will close and lock (when possible) the office door and post a sign on the door, “Classified Work in Progress – Knock for Entry.” Additionally, he or she will close the blinds to prevent visual access from outside the room. Personnel who do not have both the proper clearance AND need-to-know must be removed from the office. The holder must keep classified material in his or her DIRECT PERSONAL CONTROL at all times. Whenever the employee cannot be present, the material must be returned to the designated container in the Alarmed Room and the container locked.

5-301. Identification of Classified Work Areas. In addition to the Alarmed Room, all offices at Overlook Systems Technologies, Inc. Vienna, VA may be used for reading or manually editing collateral-level classified material, as long as they have doors and can be screened from view from the outside by closing the blinds. Classified meetings may be conducted in either of the two conference rooms, following the same procedures as when work is to be done in an office. Specifically, the doors must be closed and signs posted, “Classified Meeting in Progress, Knock for Entry.”

5-400. Transmission of Classified Material. With the exception of voice transmission via Secure Communications Devices, such as the STE, classified material will normally be prepared for transmission only by the FSO.

5-401. Preparation and Receipting.

a. Wrapping. Classified material will be wrapped in two opaque covers. The sealed inner wrap will include the name and address of both the sender and addressee, as well as the highest classification of material contained, except that, when locking courier pouches are used, the interior bag will not be marked except with the name and work address of the FSO. The outer wrap will contain sender and addressee information, but will not display any indication that it contains classified information. When courier pouches are used, the outer pouch will be identified with the name and work address of the FSO.

1. When paper envelopes or wrapping paper are used, all seams will be covered with paper fiber tape.

2. When courier pouches are used, both inner and outer pouches will be locked with the embedded locks.

b. Classified Material Receipt (CMR). A CMR will be included with each classified package to ensure that it reaches its final destination. The receipt will identify the sender, the addressee, and the document (Overlook control number and copy number, classification, and Unclassified title). Receipts will be held in a suspense system until the signed copy is received. A tracer copy will be sent by the FSO to the addressee whenever a signed receipt is not received within 30 days.
5-402. **Addressing Classified Material.** Classified mail must not be addressed to individuals. The approved classified mailing address must always be used on the outer wrap, while attention lines or “for” lines may be included on the inner wrap or receipt.

5-403. **Use of Commercial Passenger Aircraft for Hand-carrying Classified Material.** Due to the extreme sensitivity of the Transportation Security Administration (TSA) to sealed packages being carried onto aircraft, hand-carrying classified by commercial air should be used only as a last resort. When this method is required, the FSO will thoroughly brief the designated courier on the procedures and will prepare an individual Commercial Air Courier Authorization Letter in accordance with Chapter 5-4 of the NISPOM.

5-404. **Local Courier Authorizations and Briefings.** The FSO will identify Overlook personnel authorized to hand-carry classified material within the metro DC area and issue them Metro Courier Authorization cards, upon completion of a courier briefing. When hand-carrying classified material, Overlook personnel must ensure that they have their Courier Cards in their possession, that the classified material is properly marked and receipted, and that there will be an authorized recipient at the trip terminus to accept the material for storage. Other requirements are specified in the courier briefing.

5-600. **Reproduction of Classified Material.** The process of copying classified material on office copiers produces a high risk for loss or compromise of classified information. Copiers no longer transfer images directly to paper, they scan the image, store it in memory, and print it in much the same manner as Automated Information Systems. Therefore, some of the security requirements which are applied to AIS must also be applied to reproduction. **Only the FSO is authorized to copy classified information, whether personally or by immediate supervision of the process.** At a minimum, the following steps must be performed:

a. The scanner, located in the Alarmed Room as part of the accredited classified AIS, will be used to scan the document to an electronic file on the AIS or, through the AIS, directly to the approved printer.
b. The Alarmed Room must be cleared of all unauthorized personnel prior to scanning.
c. Scan and print copies as necessary.
d. Count all pages to ensure all copies/pages are accounted for.
e. Collect any waste copies and store in non-accountable destruction file in the designated Alarmed Room safe.
f. Run three copies of a “test print” type unclassified page; collect as classified waste.
g. Turn power to the printer off.
h. Ensure scanner is turned off.
i. If the printer jams at any time during classified copying, ensure that ALL parts of jammed paper are recovered and that the system is cleared completely of classified material.

5-700. **Destruction.** Destruction of classified material at Overlook Vienna will be performed by the FSO. When a witness is required, the FSO will designate a properly cleared employee with the need to know for the information being destroyed.
a. Paper documents and viewgraphs will be shredded using the approved shredder located in the SCIF/SAPF.

b. Classified electronic media will be forwarded to NSA Classified Material Conversion (CMC) for destruction. Procedures established by the CMC must be followed.

c. A Destruction Report will be prepared identifying all classified material destroyed, the date of destruction, and witness(es) to destruction. Destruction reports will be maintained on file by the FSO until the Document Accountability Database is updated to reflect disposition. Top Secret Destruction Reports will be held for ten years.

d. In the event of an emergency requiring destruction of classified material, if the FSO is unavailable, the most senior cleared employee will record the material destroyed and certify its destruction.
5-800. Special Procedures for Top Secret Material. Due to the extent of damage to national security that can be caused by the loss or compromise of Top Secret information, even greater safeguards are required when receiving, processing, handling, storing, transmitting or destroying it. In essence, the administrative and safeguarding procedures identified in this addendum apply, with the following additions or exceptions:

a. Top Secret SCI or SAP information must be controlled and safeguarded in accordance with appropriate SCI or SAP level directives. Procedures are included in the Overlook Systems Vienna SOP for each SCI or SAP program. Top Secret SCI or SAP information will never be comingled with collateral classified information, including collateral Top Secret information. It must be stored and handled within the SCIF/SAPF.

b. Top Secret collateral information must be read and otherwise handled ONLY within the Alarmed Room. While Secret and Confidential material may be removed to office spaces for review and work, Top Secret material may only be handled within the more secure Alarmed Room.

c. When work on Top Secret information is in progress, the material must be under the direct physical control of a properly cleared Overlook employee with Need-to-Know. If this individual must leave the Alarmed Room at any time, the Top Secret information must be returned to the designated storage container and the container locked. This rule applies, even if the responsible employee is only leaving for a few moments, such as to get coffee or make a trip to the rest room.

d. Receipt, transmission, or destruction of Top Secret collateral material will be performed ONLY by the FSO or a specific FSO-designated employee!

e. Top Secret working papers will be entered on an individual’s Working Papers Log and must be either entered into the Document Accountability System or destroyed within 30 DAYS of origination. Each page of Top Secret working papers will be marked with a page number and an inclusive number of total pages, e.g. “01 of 05” as well as all required classification markings. Top Secret working papers must be placed in a dedicated expansion folder and must not be comingled with working papers of other classifications. Top Secret working papers folders must be stored in the designated Top Secret storage container.

f. When processing Top Secret information on the approved AIS, authorized users will follow all procedures established by the AIS SP, including using the designated Top Secret removable hard drive. Printouts or transfers of Top Secret information to removable electronic media (other than the designated hard drive) must be approved in advance by the FSO or FSO-designated authority. All printouts must be either controlled and handled as working papers or assigned DANs, marked, and stored as accountable Top Secret classified material. ALL removable media (diskettes, CD’s, Zip disks, etc.) will be properly marked, assigned DANs, and stored in the designated Top Secret storage container.

g. The FSO will perform an annual inventory of all Top Secret material held, investigate and report any discrepancies found as required in the NISPOM, and retain records of inventories until directed by DSS to dispose of them.
6-100. Incoming Visitors.

a. Incoming Visits by Cleared Contractors or Government Personnel. When classified visits or meetings are to be held at Overlook, all employees are responsible to determine that visitors are properly cleared and have a valid Need-to-Know. Overlook employees sponsoring visits or meetings will provide lists of visitor names, social security numbers, and organizations to the FSO in advance of meeting dates. The FSO will then perform JPAS searches and validate the eligibility of each visitor. It is important to know the organization which the individual is representing at the meeting, as some people are listed in JPAS under several different Security Management Organizations (SMOs). For example, a contractor may also be a military reservist or national guardsman, as well as being a paid consultant for a government entity or other contractor. The FSO will ensure that access eligibilities from the organization being represented are adequate to meet meeting or visit requirements. In the absence of the FSO, the Executive Assistant will perform JPAS searches.

b. Incoming Visits by cleared non-DoD visitors whose information is not contained in JPAS. The FSO will require advance notification by official Visit Request from the represented agency. Such Visit Requests will be retained on file for a minimum of one year.

6-200. Government Sponsored Meetings at Overlook Vienna Facility. Conducting a government sponsored classified meeting in the Large Conference Room at Vienna requires substantial scheduling, notification, and planning.

6-201. Scheduling of Classified Meetings. Prior to making any commitments to government personnel, Overlook personnel coordinating a classified meeting must ensure that:

a. the room is available, can support the number of people projected to attend, and is scheduled for this use; the executive assistant maintains a calendar of planned conference room use;

b. any staff members who will need to give presentations or otherwise attend the meeting will be available to do so;

c. the area has received Security approval for this use;

d. any equipment required (such as computers, projectors, etc.) is functioning and available for use.

6-202. Notifications of Classified Meetings. At a minimum, the FSO and ISSM must be notified as far in advance as possible of any meetings involving classified information, especially if AIS (e.g., a classified computer) use is foreseen. These notifications MUST be made AT LEAST one week prior to the meeting date. If government personnel request to hold a classified meeting at Overlook on short notice, both the FSO and ISSM must be consulted as to their ability to support the meeting PRIOR to committing Overlook’s facilities. Additional Overlook personnel who will be asked to participate or support the meeting should also be notified as early as possible.

6-203. Planning for Classified Meetings. From a security standpoint, the following issues must all be addressed when planning a classified meeting:
a. Clearance and Need-to-Know. Prior to granting access to classified information, the meeting coordinator must validate all attendees’ clearances and NTK with the FSO. For DoD personnel and DoD contractors, this is accomplished by researching the JPAS database. Therefore, the coordinator will need to provide a list of planned attendees, the organizations represented, and social security numbers to the FSO at least five working days prior to the meeting date. Since such meetings are by invitation, either issued by or approved by the government sponsor, need to know is thereby certified. Any last minute changes in attendees must be approved by the government sponsor and clearance verified by the FSO. For non-DoD personnel, a valid Visit Request or Visit Authorization Letter, issued by the individual’s organization or company, must be received by the FSO prior to the meeting date. On the meeting date, security personnel or other Overlook staff will check identification of all attendees to assure that they are, in fact, the persons authorized to attend.

b. AIS Support. At least five working days prior to the meeting date, the coordinator must provide to the ISSM:

1. Classification Level Required; this is important as the ISSM and FSO must ensure that the room is properly accredited for the presented material. Each classification level may also levy different presentation requirements.

2. Presentation Programs That Will Be Used; this is required for the ISSM to assure that the programs needed for the presentations are loaded on the system and upgrades applied. While programs like PowerPoint, Acrobat Reader, or WinZip are often automatically and transparently upgraded on the corporate unclassified network, such is not the case for classified AIS, which are not connected to the Internet.

3. Files for Presentation. The ISSM must load presentations prior to the meeting and ensure each works properly. Presentations could rely on upgraded features which may not yet have been installed. This would require the ISSM to obtain and install the upgrade, which could take a few days.

4. Account Under Which Presentations Will be Made. If only one Overlook presenter will be using the AIS, that individual will use his or her own personal account on the system. However, if several Overlook employees will be making presentations, the required log off and log on procedures could impact the meeting’s timing and professionalism. Therefore, in such circumstances, the ISSM will create a conference room temporary account to be used specifically for that meeting. At the end of the meeting, this account will be disestablished and normal classified processing rules will apply.

5. Attendee Provided Presentation Materials. While it is not unusual for attendees, who are giving presentations at a meeting, to prefer to bring their own classified briefings and load them onto the classified AIS at the time of presentation, this procedure is not permitted. As a component of system accreditation, Overlook must ensure that all media is screened for malicious software by the ISSM, prior to use. Therefore, all presentations must be delivered to the ISSM in sufficient time to be screened before the meeting and before the AIS is moved into the Conference Room.

c. Physical Security. Prior to classified meetings, the unclassified telephone in the conference room will be physically disconnected from the telephone wall jack and stored, the speaker phone power unit will be disconnected and the unit stored. The unclassified AIS will be disconnected from projection equipment and Ethernet and removed from the meeting room, along with the Ethernet cable. The wireless mouse hub will be disconnected from power source and stored. Electronic devices are prohibited;
therefore, cell phones, two-way pages, PDAs, Blackberries, computers, laptops, and other recording devices must be left either in the reception area or another location during the meeting.

d. **Classified Meeting Notes.** The coordinator must always make provision for notes taken at a classified meeting. Unless an attendee has a current courier authorization letter or card from his or her own organization AND has approved means to package the notes (such as inner and outer locking courier pouches or a locking courier pouch and locking briefcase, he or she must not remove notes from the meeting area. If the attendee has a courier authorization, but no packaging means, the FSO may, depending on available time and resources, double-wrap the notes for the attendee to hand-carry. Otherwise all attendees must provide an approved classified mailing address for the transmission of classified notes. Such notes will then be transmitted by the FSO within two working days following the meeting.

e. **Administrative Issues.** While not strictly part of the security process, certain administrative issues must also be addressed, including:

   1. Providing for coffee, snacks, and meals, as appropriate. The Executive Assistant coordinates these activities.
   2. Providing maps to the facility, hotel accommodation information, and parking instructions to attendees.
   3. Administrative support, such as preparation and copying of meeting support materials. This function may require security assistance if it involves classified material.

6-204. **Meeting Day Procedures.** On the day of the meeting, the coordinator will work with the FSO, ISSM, and Executive Assistant to ensure that:

   a. All attendees are checked at the door to the facility to verify identification and authorized attendance;

   b. In the interest of protecting proprietary information and intellectual property, attendees are escorted at all times while within Overlook spaces and access limited to meeting information;

   c. Classified meeting support materials are not removed from the Overlook secure facility to the meeting room until such time as they will be constantly controlled by cleared Overlook personnel;

   d. The Classified AIS is not brought to the meeting area until all physical security measures are in place, to include continuous control by cleared Overlook personnel;

   e. The Classified AIS is returned to the Overlook secure facility immediately following the classified meeting (or classified portion of a meeting);

   f. Classified meeting notes and materials are collected and delivered to the secure facility for appropriate storage immediately following the classified meeting.

   g. After all classified AIS and materials have been delivered to and stored within the Overlook secure facility, the meeting coordinator, ISSM, and/or FSO will conduct a
thorough inspection of the meeting area to ensure that no classified material is inadvertently left behind.

(This section will become immediately effective, should Overlook Vienna acquire NATO documents.)

10-700. NATO Storage Requirements. NATO classified information must be segregated from other classified information. Therefore, the two-drawer container in the Alarmed Room has one drawer which is designated for NATO storage. Only cleared personnel who have been briefed for NATO access are authorized to have access to this drawer. While NATO information and documents, as with other Secret and below collateral information, may be removed to office space for reading or manual editing, it is incumbent on the holder to ensure that only NATO briefed personnel gain access to the information while it is outside authorized storage.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOC NBR</td>
<td></td>
</tr>
<tr>
<td>COPY NBR</td>
<td></td>
</tr>
<tr>
<td>DOC TYPE</td>
<td></td>
</tr>
<tr>
<td>DOC DATE</td>
<td></td>
</tr>
<tr>
<td>CLASSIFICATION</td>
<td></td>
</tr>
<tr>
<td>CAVEATS</td>
<td></td>
</tr>
<tr>
<td>DECLASSIFY ON</td>
<td></td>
</tr>
<tr>
<td>UNCLASSIFIED TITLE</td>
<td></td>
</tr>
<tr>
<td>CONTRACT</td>
<td></td>
</tr>
<tr>
<td>RCVD FROM</td>
<td></td>
</tr>
<tr>
<td>DATE RECEIVED</td>
<td></td>
</tr>
<tr>
<td>ORIG DOC NR</td>
<td></td>
</tr>
<tr>
<td>ORIG COPY NR</td>
<td></td>
</tr>
<tr>
<td>TRANS METHOD</td>
<td></td>
</tr>
<tr>
<td>KEY PERSON</td>
<td></td>
</tr>
<tr>
<td>DISPOSITION</td>
<td></td>
</tr>
<tr>
<td>DISPO DATE</td>
<td></td>
</tr>
<tr>
<td>TRANSMITTED TO</td>
<td></td>
</tr>
<tr>
<td>TRANSMIT BY</td>
<td></td>
</tr>
<tr>
<td>DESTROYED BY</td>
<td></td>
</tr>
</tbody>
</table>