BY ORDER OF THE COMMANDER
439TH AIRLIFT WING

439TH AIRLIFT WING INSTRUCTION
16-1404

17 JULY 2025

Information Security

INFORMATION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and Forms are available for downloading or ordering on the e-Publishing website at www.e-publishing.af.mil

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 439 AW/IP

Certified by: 439 AW/CC
(Colonel Gregory D. Buchanan)

Supersedes: 439AWI16-1404, 8 May 2018

Pages: 26

This instruction implements Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*, 31 December 2019. It standardizes the procedure for handling, controlling and safeguarding of classified material/information within all organizations of the 439th Airlift Wing (439 AW). These procedures do not apply to Special Access Programs that are governed by other instructions. These procedures apply to all personnel within the 439 AW that handle/control classified information or who have a security clearance eligibility. Use these procedures with *Air Force Information Security Program*, Department of Defense Instruction (DoDI) 5200.01_AFMAN 16-1404 Vol 1, *Information Security Program: Overview, Classification and Declassification*; DoDI 5200.01_AFMAN 16-1404 Vol 2 – *Information Security Program: Marking of Information*; DoDI 5200.01_AFMAN 16-1404 Vol 3 – *Information Security Program: Protection of Classified Information, Air Force Personnel Security Program***;** Department of Defense Manual (DoDM) 5200.02_DAFMAN16-1405_DAFGM2023-01 (v. 29 NOV 2023), *National Industrial Security Program: Industrial Security Procedures for Government Activities;* DoDM 5220.22 Vol 2_ AFMAN16-1406, Volume 2, *Controlled Unclassified Information***;** DoDI 5200.48, *Controlled Unclassified Information (CUI),* 6 March 2020; Department of Defense Directive (DoDD) 5205.16, *The DoD Insider Threat Program*, 28 August 2017; Department of the Air Force Instruction (DAFI) 16-1402, *Counter-Insider Threat Program Management, 10 May 2024*; *Security Executive Agent Directive 3, (12 June 2017)* Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, *Security Executive Agent Directive 4, (08 June 2017)* National Security Adjudicative Guidelines, *Security Executive Agent Directive 7, (9 November 2018)* Reciprocity of Background Investigations and National Security Adjudications, *Security Executive Agent Directive 8, (18 May 2020)Temporary Eligibility, Air*

Force (AF) Enterprise Authorizing Official Memorandum, Subj; Personally Wearable Fitness Devices, 26 May 2016; along with any base supplements, for the implementation of the Air Force Information Security Program.

This air wing instruction (AWI) is intended to standardize the 439th Airlift Wing, Information Protection (439 AW/IP) functions. If an organization has special handling needs or concerns not covered by this AWI, each commander is encouraged to write additional plans and procedures in conjunction with 439 AW/IP. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, 28 July 2021; and disposed of IAW the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*, 22 September 2009; route AF Form 847 to 439 AW/IP, Westover Air Reserve Base (WARB), 975 Patriot Ave, Box 63, Chicopee, Massachusetts (MA) 01022-1534.

1. Responsibilities. The policies and procedures outlined throughout this AWI apply to all personnel assigned or attached to the 439th Airlift Wing (439 AW). Each person must ensure compliance with these procedures, report any deviations and have the moral and legal obligation to protect classified material.

1.1. Wing, Group and Squadron Commanders will:

1.1.1. Establish the information security program and execute the program to comply with governing DoD and AF policies and instructions.

1.1.2. Review, approve and sign unit operating instruction if an organization has special handling needs or concerns not covered by this AWI.

1.1.3. Appoint primary and alternate security assistants to perform security duties (i.e.: self-inspection officials, preliminary inquiry officials, etc.), as required.

1.1.4. Review security files to determine interim clearance eligibility. Review adverse information to determine if a Security Information File (SIF) should be established.

1.1.5. Ensure security incidents and potential compromises of classified material are properly investigated.

1.1.6. Endorse consolidated compliance reviews and semiannual self-inspection reports, as required.

1.1.7. Provide couriers with verbal authorizations to hand-carry material outside their normal work area; but remaining on the confines of the installation, if required.

1.1.8. Sign courier authorization letters for hand-carrying classified material off the installation.

1.1.9. Implement and actively support the information security education and training program.

1.1.10. Ensure management of classified information is a critical element in performance contracts and/or performance evaluations for all unit personnel who manage classified information.

1.2. Division Chiefs/Flight Commanders will:

1.2.1. Ensure personnel complete initial, refresher, and specialized Security Education and Training.

1.2.2. Ensure Standard Form (SF) 701, *Activity Security Checklist*, 1 November 2010, is completed when security containers are present and destroyed IAW AFRIMS RDS.

1.2.3. Coordinate with the security assistant to ensure civilian employment positions are designated correctly for position sensitivity. Assist the security assistant in the timely submission of SF 86 up-dates per regulatory requirements.

1.2.4. Evaluate cleared personnel to ensure they remain trustworthy for access to classified information. Report knowledge of adverse information to the commander and assist the commander in determining appropriate measures when an individual's action reflects non-compliance with adjudication guidelines.

1.2.5. Ensure all newly assigned personnel/employees in-process and out-process through the security assistant.

1.2.6. Verify newly assigned individual's personnel security eligibility and access status with the security assistant and assure access is granted only at the appropriate level.

1.2.7. Ensure subordinate personnel who require access to classified information are properly cleared and are given access only to that information, to include sensitive information, for which they have a need to know. Make sure work center personnel are advised when newcomers are not cleared.

1.2.8. Ensure subordinates are trained in, understand, and follow work center security procedures and requirements of the information security program.

1.2.9. Provide or arrange for specialized security training when subordinate's duties involve the derivative classification of material or are assigned security container custodian duties.

1.2.10. Continually observe subordinates for personal problems, adverse conduct, or other derogatory information that could have a bearing on their continued eligibility for access to classified information or occupy a position of trust. Any derogatory information will be reported to the respective unit commander, security assistant or 439 AW/IP at (413) 557-2189.

1.3. Individuals will:

1.3.1. Comply with security requirements and remain proficient in their duties and security responsibilities to prevent unauthorized disclosure of classified information.

1.3.2. Not accept custody of classified material or participate in classified discussions for which they are not properly cleared.

1.3.3. Report, without delay, to the unit commander or security assistant:

1.3.3.1. When they become aware of or believe that there may have been a compromise, loss, unauthorized disclosure or other infraction affecting the safeguarding of classified information.

1.3.3.2. If they believe they have been contacted by an intelligence collector or other unauthorized individual seeking to gain access to sensitive government information.

1.3.3.3. Any information that could adversely reflect on their or a co-worker's suitability for continued access to classified information.

1.3.4. Follow the proper reporting procedures of security violations.

1.4. The Program/Project Assistant will:

1.4.1. Coordinate/discuss program or project security requirements with the security assistant prior to program/project implementation.

1.4.2. Ensure program/project personnel have sufficient classification guidance when programs involve access to classified information.

1.4.3. Notify the security assistant when any contractors will work within the unit.

1.4.4. Ensure prior to conducting a classified meeting the individual hosting the meeting contact the security assistant and ensure proper procedures are followed. See **paragraph 5** of this wing instruction.

1.5. The Security Assistant will:

1.5.1. Oversee all aspects of the unit information, personnel, and industrial security programs and be responsible for developing security policy, establishing procedures, and providing program guidance. Act as the single point of contact for the security program to outside organizations. Advise and assist the Commander and unit personnel on security matters under their purview.

1.5.2. Ensure security training is conducted and develop specific organizational security training plans as required. Provide or request assistance from outside agencies in providing specialized security training (i.e. derivative classifiers, courier briefings, foreign travel briefings, preliminary inquiry or investigating officials, etc.). Advise the commander on the status of the unit's security training program. Ensure training is documented and records are properly maintained.

1.5.3. Implement the personnel security program and provide support to the service security activity. Use Defense Information System for Security (DISS) or successor system to review the status of personnel security clearances. Notify the Commander of any unfavorable information that could impact an individual's security clearance or access to classified information.

1.5.4. Ensure annual security self-inspections are scheduled and conducted at the required intervals and provide the inspecting official with the appropriate directives, self-inspection checklists, and any required guidance or assistance. Initiate corrective actions to any findings, if required.

1.5.5. Coordinate classified equipment copier approval with unit Commander. The security assistant will approve secure shredders and all classified destruction devices by ensuring all equipment is on the NSA/CSS Evaluated Product List (EPL).

1.5.6. Conduct access and termination briefings for government civilians and military personnel. The security assistant will execute an AF Form 2587, *Security Termination Statement*, 1 September 1981 to terminate an individual's access to classified material. If individual refuses to sign the AF Form 2587, the briefer and a witness will sign the AF Form 2587 documenting the refusal, the form will be forwarded to the appropriate agency and the commander will be notified.

1.5.7. Provide guidance to Preliminary Inquiry Officials on conducting Security Inquiries and ensure a briefing is provided by 439 AW/IP. The security assistant will coordinate with the Original Classification Authority (OCA), when required, for classified material involved in a security violation.

1.5.8. Ensure secure areas/rooms have requisite security approvals prior to storing and/or processing classified information.

1.5.9. Provide technical guidance on all information and personnel security related issues. Act as the conduit between the 439 AW/IP and unit personnel for clearance and access issues.

1.5.10. Attend scheduled security assistant meetings as requested.

1.5.11. Ensure visual aids are posted and authorization letters are obtained for security type equipment located in the work area.

1.6. The Security Container Custodians will:

1.6.1. Be knowledgeable of security procedures involving access, safeguarding, protection and marking of classified information. The primary safe custodian must be a government employee.

1.6.2. Be listed on the SF 700, *Security Container Information*, 01 April 2001.

1.6.3. Manage classified holdings by periodically reviewing material for currency, need, and proper marking.

1.6.4. Establish and maintain document suspense/receipt and destruction files, as required.

1.6.5. Prepare and post required forms for each security container or secured area. Required forms:

1.6.5.1. SF 700, filed in each locking drawer or on locking door.

1.6.5.2. SF 701, located adjacent the entryway of room/area where security containers are located or on a clipboard if end-of-day check duty is rotated.

1.6.5.3. SF 702, *Security Container Check Sheet*, 1 January 2020, located on each locking drawer/door.

1.6.5.4. Optional Form (OF) 89, *Maintenance record for Security Containers/Vault Doors*, 01 September 1998; located in each locking drawer.

1.6.6. Ensure the combination to the security container is changed as required (upon departure of anyone with the combination who may have access to area where the security container is located, when the combination is suspect to compromise, or when brought into or removed from service). Combinations of all new containers and those being removed from service are set at 50-25-50.

1.6.7. It is the custodian's responsibility to ensure security containers are properly maintained. If maintenance is not being performed as required, contact your unit security assistant. Security Container maintenance can be conducted by contacting a General Services Administration (GSA) certified inspector/technician (unit funded). If you require assistance with contacting a GSA certified inspector/technician, contact your unit security assistant or 439 AW/IP at 557-2189 or 557-2310. Maintenance on security containers must be IAW AFI 16-1404, Operation Visual Inspection (OVI) Checklist for Security Containers, Vault Doors, and Secure Rooms, preventive maintenance inspection upon receipt of DODI 5200.0_AFMAN 16-1404 and every 5 years thereafter.

1.6.8. 439 AW/IP is responsible for assessing discrepancies reported by security assistant(s) and determining if a GSA approved technician is needed to fix the security container or vault door.

1.6.9. Ensure the combination is protected at the same level as classified stored in the container.

1.6.10. Oversee the periodic purge of files in the classified storage containers/areas and, as a minimum, during the designated annual clean-out days (reference **paragraph 15.6**.). In conjunction with each retention review, ensure appropriate downgrading/declassification actions are taken.

1.6.11. Ensure all personnel receive training prior to giving access to the security container. Training will include opening/closing procedures, properly marking of classified materials, completing security container documentation, reporting of security violations, and proper safeguarding of classified information. Prior to unit appointments, security container custodians will complete courses Storage Containers and Facilities, located on the Center for Development of Security Excellence (CDSE) website. All personnel who create derivative classification documents or are issued a Secret Internet Protocol Router Network (SIPRNet) token must receive derivative classification training every year. This training is located on the Defense Counterintelligence Security Agency (DCSA) website.

1.6.12. Inspect containers when removed from service to ensure they are free of classified material and have combination changed to factory setting.

2. Access. Use DISS or successor system as the primary source for confirming access eligibility for DoD military, DoD civilians, and DoD contractor personnel.

2.1. The holder, not the potential receiver of the information, determines the need–to–know and is responsible for verifying the personnel security eligibility and access of the potential receiver.

2.2. Classified information shall only be released to individuals who meet all of the following requirements:

2.2.1. Possess a valid personnel security eligibility and access (equal to or greater than the information being disclosed) that has been verified in DISS or successor system.

2.2.2. Possess a valid need-to-know for the information in order to perform a lawful and authorized government function.

2.2.3. Sign a SF 312, *Classified Information Nondisclosure Agreement*, 1 July 2013, verify through DISS or successor system or accomplished in person. If a person refuses to sign the SF 312, they will not be granted access to classified information.

2.2.4. The Commander must approve access on a one-time or continual basis, this task cannot be delegated.

2.2.5. Initial Access briefing will be signed by the individual.

2.2.6. Verify identity by checking a government issued identification card.

2.2.7. The unit security assistant will verify these elements. Personal assurance shall not be accepted for personnel security eligibility and access verification.

2.2.8. Classified information will not be released to a contractor without concurrence of the government security representative.

2.2.9. All personnel will immediately report to their Commander**,** supervisor or security assistant any contact with individuals, regardless of nationality, when illegal or unauthorized access is sought to obtain classified or controlled unclassified information (CUI).

3. Incoming Visit Requests. Visit requests are normally accomplished through DISS or successor system and are accomplished by the Unit Security Assistant or 439 AW/IP. In the few cases where visit requests are not routed through DISS, unit security assistants will ensure personnel are properly cleared prior to classified access. If the visit is a Wing wide visit, contact 439 AW/IP.

3.1. Receiving Visitor requests:

3.1.1. Incoming visit requests can also be sent to the 439 AW/IP office via DISS or successor system, Security Management Office (SMO) code: W5MF8WN5.

3.1.2. Visit authorization letters will not be used to pass security clearance information unless DISS or successor system is not available. Procedures to send visit requests, if DISS is not available, send visit requests to the 439 AW/IP office at commercial number (413) 557-2310 or DSN 589-2189.

3.1.2.1. Visit requests for contractors:

3.1.2.1.1. Unclassified contractor visit must be on company letterhead and signed by the Facility Security Officer (FSO) or a designated representative excluding the visitor(s).

3.1.2.1.2. Classified contractor visit must be transmitted through DISS or successor system, accompanied by a Defense Department (DD) Form 254, *Department of Defense Contract security Classification Specification*, 1 April 2018, listing WARB as a contract performance location.

3.1.2.2. Visit requests for DoD civilian and military personnel should be on the service specific form and signed by a security representative.

3.1.2.3. The request must include, as a minimum: full name, social security number, date/place of birth, organization/office symbol (DoD employees only), citizenship, security clearance level and date granted, purpose of visit, date of visit and a point of contact (POC) within the unit.

3.2. The disclosure of information to visitors will be restricted in scope to that information directly related to the purpose of the visit and limited to their personnel security eligibility, access, and need-to-know.

3.3. Visit sponsors (hosting agencies) are responsible for determining personnel security eligibility and access, need-to-know, and identification validation before releasing classified information to visitors. The security assistant will conduct clearance/access eligibility verifications upon request.

3.4. The visit sponsors, with the assistance and advice of the security assistant, will arrange for installation and facility access.

3.5. Visitors with classified material arriving after hours should be directed to the Westover Air Reserve Base, Command Post, Building 1610 for temporary overnight storage.

4. Outgoing Visit Requests. When a government employee requires access to classified information at:

4.1. A non-DoD contractor activity, the supervisor or security assistant must contact the office to be visited to determine the desired clearance verification.

4.2. The unit security assistant will complete a DISS or successor system visit request for personnel needing to visit another government or contractor facility. The traveler must provide the security office purpose of the visit, sponsor's name and phone number, the duration of the visit, a list of the traveler's names and social security numbers and the SMO code. SMO code can be obtained from the sponsor's security assistant.

5. Classified Meetings. Prior to conducting a classified meeting, the individual hosting the meeting, will contact the security assistant and ensure proper procedures are followed.

5.1. Room/Areas must be checked to determine if sound will travel through the walls/vents/doors. If discernable sound can be heard outside the meeting area, a cleared monitor individual with eligibility and access to the same level of information must be posted outside the door/vent/wall to ensure all loitering and/or unauthorized entry is prohibited.

5.2. The security clearance of all attendees must be verified prior to the meeting. Visit requests are to be on file with the security office for all non-government/military meeting participants. If foreign nationals are required to attend, contact 439 AW/IP to ensure all appropriate action/requirements are met prior to the meeting.

5.3. Prior to the start of the meeting, the meeting area will be checked by the host for suspicious objects or obvious recording devices.

5.4. At the beginning and end of the meeting, the facilitator of the meeting must announce classification level of information to be discussed.

5.5. Note taking should be discouraged. If note taking is necessary, all participants must understand that notes become classified working papers and must be marked and protected accordingly.

5.6. All presentation materials must be marked properly. If used, all electronic equipment (computers, projection equipment, etc.) must be certified and accredited to the proper security level.

6. Safekeeping and Storage (Internal Control of Classified Material). Classified material will be under the constant observation of a cleared individual with proper eligibility and access or locked in a GSA approved security container or accredited secure room. This includes classified material aboard an aircraft parked in a restricted area. Any deviations must be reported to the Commander and/or security assistant.

6.1. Personnel will coordinate with the security assistant prior to relocating a container or placing new containers in service.

6.2. High value items and items susceptible to theft (funds, guns, drugs, precious metals, etc.) will not be stored in the container with classified material.

6.3. Temporary storage of classified material is available at the Westover Command Post (439 AW/CP), phone (413) 557-3571 or DSN 589-3571. The Command Post also provides temporary overnight storage for visitors arriving after normal duty hours.

6.4. Ensure the SF 702, *Security Container Check Sheet*, is located on top of the security container.

6.5. An SF 704, *Secret Cover Sheet*, 01 August 1985, or SF 705, *Confidential Cover Sheet*, 01 August 1985 (as appropriate) will be attached to all classified documents removed from the security container.

6.6. Use the SF 702, *Security Container Check Sheet*, to record openings and closings for all GSA approved security containers, vaults, and approved secure storage rooms.

7. End of Day Security Checks (Daily Security Checks): Before departing, personnel who work with classified material will check their work area (trash cans, desktops, in-baskets, printers and computers) to ensure all classified material has been secured. This security measure is in addition to, not in lieu of, the formal end-of-day security check regardless of whether the container is opened or not.

7.1. Administrative Requirements:

7.1.1. The SF 702, *Security Container Check Sheet*, will be posted on all classified security containers and annotated each time the container is opened and closed. NOTE: If a 5-drawer security container contains 5 separate locking drawers, each drawer is considered a separate security container, and each drawer must have its own SF 702, *Security Container Check Sheet*. As a minimum, each container will be checked, verified secure (attempt to open each drawer) and the SF 702, *Security Container Check Sheet*, annotated during the end-of-day security check, regardless of whether the container is opened or not. Use the SF 702 "Checked By" column to verify the security status of containers, vaults, and security storage room during the end-of-day check and annotate it whether or not they were opened during the day.

7.1.2. The SF 701, identifies items to be checked and will be posted at or near the primary entrance/exit point to each room or area where classified material is stored, handled, or processed. Additional areas/equipment may be added to the SF 701, as well as lining through preprinted items that are not applicable. Each area utilizing the SF 701, will add the requirement to check computer systems to ensure Common Access Cards (CAC) and SIPRNet tokens have been removed from workstations.

7.1.3. Branch/Section/Office chiefs must ensure end-of-day security checks are completed.

7.2. Security Check Procedures**.** The designated individual will, as a minimum:

7.2.1. Inspect all equipment and areas where classified is handled, stored, processed or destroyed to ensure classified material is properly secured (desktops, copiers, fax, computers and peripherals)

7.2.2. Spin the dial on security containers with mechanical locks at least four (4) times in one direction (for electro-mechanical locks such as the X-07/08/09 spin the dial to ensure the lock is engaged) and attempt to open each drawer or door manually.

7.2.3. Examine secure communications devices such as Secure Telephone Equipment (STE) and remove crypto key. Also, check classified computers with removable drives, to ensure the drives have been removed and secured in a GSA approved security container if applicable.

7.2.4. Record the check, the time the check was conducted and initials of the person making the check, on SF 701 and SF 702.

8. Information Processing Equipment: Classified information will only be processed on computer(s) approved and specifically designated for processing classified information. Authorized personnel will process classified information IAW the equipment's Designated Approval Authority (DAA) approved security plan.

8.1. Classified hard drives, floppy disks, CD-ROMs and computer-generated products will be properly marked, controlled and safeguarded equal to the level of classified information stored on the item. Review DoDM 5200.01 Volume 2_DAFM 16-1404, V2, *Information Security Program: Marking of Information*, 7 January 2021, for limitations and unique marking requirements.

8.2. The usage of small alternate storage memory (USB) type storage devices is prohibited for storing classified information. Personally owned or unapproved USB devices are not authorized to be used on any government computer.

8.3. Personnel will ensure when utilizing classified computers that the monitors are located in such a way that unauthorized personnel cannot view them. In addition, the equipment will not be repositioned without prior approval of the Emissions Security (EMSEC) Assistant.

8.4. All other small devices must be justified and approved by the DAA for the classified system. In addition to computer security requirements, they will:

8.4.1. Be prominently and properly marked with the highest classification of material stored or to be stored on them.

8.4.2. Be stored in a security container approved for classified storage when not in use.

8.4.3. Inventoried and accounted for at the end of the duty day.

8.4.4. The use of "disguised" storage devices is prohibited in any government system.

8.4.5. Personnel in rooms/areas containing computers processing classified information must remain in attendance or if approved for open storage, ensure area is secured when classified hard drives are in the system.

8.4.6. Personnel using classified computer systems will never download any document to an unclassified computer system. If the document is unclassified on the classified system, you cannot open it on an unclassified system. Contact the security assistant for any questions.

9. Packaging and Transmission of Classified. Packaging and transmission requirements for classified material dispatched via U.S. Postal Service (USPS) or approved overnight courier.

9.1. Classified document/material will be enclosed in two opaque sealed envelopes or similar wrapping, size permitting. If size prohibits, then the classified material must be enclosed in two opaque, sealed containers, such as boxes or heavy wrapping.

9.2. If the classified material is an internal component of a packable item or equipment, then the outer shell or body may serve as the inner enclosure, providing no classified information is revealed.

9.3. All materials used for packing must be of such strength and durability as to provide security and protection while in transit and to facilitate the detection of tampering. The wrappings must also conceal all classified characteristics.

9.4. Classified written information will be folded or packed in such a manner that the text will not be in direct contact with the inner envelope or container. Avoid mailing written materials of different classifications in a single package.

9.5. Inner wrappers will be marked with the highest classification of material contained in the package along with any special warning or control notices. Outer wrappers must not display classification markings but will have the official address of the owner/user.

9.6. DoDM 5200.01 Volume 2_DAFM 16-1404, V2, *Information Security Program: Marking of Information*, for additional information and instructions on modes of transmission and packaging requirements.

10. Receiving Classified: The central 439 AW mail receiving/distribution office is 439th Force Support Squadron (439 FSS), Westover ARB, Building 1408, 570 Patriot Ave, Chicopee, MA 01022.

10.1. All personnel assigned duties to receive office mail will:

10.1.1. Have a minimum of a SECRET clearance.

10.1.2. Be authorized to sign receipts for incoming mail.

10.1.3. Protect all overnight delivery as classified material until proven otherwise. Secure unopened "suspect mail" in an approved security container at the end of the duty day or when the office is unattended.

10.1.4. Receivers of classified material or "suspect mail" will:

10.1.4.1. Inspect packaging for signs of tampering. Contact the security assistant and sender if tampering is detected or suspected.

10.1.4.2. Compare the contents to items listed on AF Form 310, *Document Receipt and Destruction Certificate*, 01 November 1995, note any discrepancies on the receipt; sign and return the AF Form 310 to the sender. Discrepancies are to be reported to the sender and security assistant immediately.

10.1.4.3. Review the material for content and proper markings prior to entering the material into the classified filing system or security container. Contact the sender/originator to resolve marking problems.

10.1.4.4. Initiate a challenge when there is a substantial reason to believe classified information is improperly or unnecessarily classified. Challenges may be either formal or informal, with the informal challenge the preferred first step.

10.1.4.5. Initiate a challenge:

10.1.4.5.1. Contact the material originator, via secure communications, to discuss your concerns.

10.1.4.5.2. If unable to resolve the matter by an informal challenge, initiate a formal challenge. Consult security directives and the security assistant to initiate a formal challenge.

10.1.4.5.3. Classified information undergoing a challenge will be protected and safeguarded at the current classification level and unclassified information will be protected at the proposed classification level, pending final resolution.

10.1.4.5.4. The security assistant will notify 439 AW/IP when a formal challenge is initiated.

11. Hand-carrying of Classified Material on the Installation.

11.1. When hand-carrying classified material from one building to another on WARB:

11.1.1. Enclose classified material in an inner and outer wrapper/container.

11.1.2. The inner container will be marked with the highest classification of material inside.

11.1.3. The outer container will not contain any external classification markings.

11.1.4. Close or seal the containers to prevent loss or inadvertent access to the classified contents.

11.2. All couriers will be briefed by the security assistant on courier responsibilities and will not make intermediate or convenient stops with classified material in their possession.

12. Hand-carrying of Classified Material off the Installation.

12.1. Hand carrying classified material off the installation will be done as a last resort, only after considering alternatives such as mailing or electronic transmission. When approved:

12.1.1. A courier must carry a DD Form 2501, *Courier Authorization*, 31 March 1988, when traveling off the installation or aboard commercial passenger aircraft. Obtain card from Wing IP.

12.1.2. Material will be double wrapped and addressed as if it were being mailed.

12.2. The DD Form 2501, signed by the 439 AW/IP and will not exceed two years.

12.3. Couriers will coordinate security arrangements with the security assistant and destination when leaving the local area, using commercial transportation, or a trip that requires an overnight stay.

12.4. Couriers will be briefed and must acknowledge their security responsibilities. The security assistant or supervisor will conduct and record these briefings.

13. Reproduction of Classified. Reproduction of classified material should only be done if absolute necessary. Contact your Unit Security Assistant for assistance prior to reproducing any classified information. Reproduction will only be accomplished on equipment specifically designated and approved for classified reproduction. Additional reproduction requirements follow:

13.1. Personnel will maintain constant surveillance and control over reproduction equipment and area where the equipment is located when reproducing classified material.

13.2. Personnel will follow the classified reproduction rules posted on the equipment and ensure the equipment is cleared of any latent images after classified reproduction.

13.3. Account for all originals, copies, and waste before departing the copy area.

14. Equipment Control.

14.1. The security assistant will obtain the necessary equipment approvals and post the appropriate visual aid on unit equipment approved for classified reproduction.

14.2. In the event of an equipment malfunction, personnel will attempt to clear the situation by following the equipment instructions. If classified material cannot be removed, summon assistance. Do not leave the equipment or classified material unattended. Escort maintenance technicians, if required, and ensure they do not access material they are not cleared for.

15. Destruction.

15.1. Classified material will be destroyed when no longer required for operational requirements or by law. The security assistant will obtain the necessary approvals and ensures devices have been approved for the destruction of classified material by referencing the National Security Agency/ Evaluated Products List (NSA/EPL). Contact 439 AW/IP at (413) 557-2310 for assistance. Other destruction requirements are as follows:

15.1.1. One cleared person with proper eligibility and access may destroy CONFIDENTIAL and SECRET classified material.

15.1.2. Equipment operators will inspect the debris during and after the destruction session. The inspections are to ensure the equipment is operating properly and ensure the material is adequately destroyed. When a shredder is used, check the functional areas to ensure that no classified material remains intact.

15.1.3. Check the immediate area before departing the shredder to ensure that no classified remains.

15.2. Controlled Unclassified Information will be destroyed IAW DoDI 5200.48.

15.3. Classified computer disks, CD-ROMs, and magnetic media may be destroyed in Building 3400, Room 150 (439 CS/SCXS).

15.4. When transporting material outside the facility for destruction, place it in an opaque bag or box sealed and marked in a fashion to protect the material from loss or unauthorized disclosure during transport. Material must be protected as classified until destruction is complete.

15.5. The 439 AW annual clean-out day will be 15 January of each year. The focus of this event will be a retention review and the disposal of all classified material that is obsolete or unnecessary. This does not preclude the units from establishing their own additional clean out days. Document when clean out is conducted.

15.6. Excess material no longer required by law or mission accomplishment will be identified and subsequently destroyed.

15.7. During the retention review, complete any downgrading/declassification actions noted on the material.

15.8. Container custodians will destroy unclaimed material after consulting with the work center supervisor and security.

16. Security Incidents and Violations. All personnel are personally responsible for the protection of classified information. Reporting procedures for security incidents and violations are as follows:

16.1. Any person who has knowledge of the loss or possible compromise of classified information will immediately report such facts to the security assistant, immediate supervisor, or the Commander.

16.2. A person finding classified material unattended or improperly stored is responsible for protecting it until the responsible custodian or other such official regains proper custody.

16.3. The security assistant will advise the Commander on inquiry/investigative requirements. The security assistant is responsible for reporting the incident to the 439 AW/IP Office no later than the first duty day following the reporting of the incident. In incidents where classified material is lost or out of proper control, all notifications will be made in person or over secure communications.

16.4. The Commander or director must appoint an inquiry official for all security incidents within three duty days from the discovery of the security incident. DoDM5200.01V3_AFMAN16-1404V3, *DoD Information Security Program: Protection of Classified Information*, page 103.

16.5. The inquiry official appointment letter will be accomplished and signed by the appointing authority. Upon notification of appointment, the inquiry official will make an appointment with the 439 AW/IP office for a briefing on the incident and their responsibilities. The inquiry official will provide a copy of their appointment letter to the 439 AW/IP. The inquiry official will also contact the 439th Airlift Wing, Staff Judge Advocate (439 AW/SJA) to receive a briefing, if necessary.

16.6. The inquiry official will prepare a written report. The report will at a minimum be marked “CUI” and be completed within 30 days of appointment. The report will be routed

through the 439 AW/IP to the appointing official. The Information Protection Chief will provide technical reviews of the report and concur/non-concur on the findings and forward it to the appointing official.

16.7. The appointing official reviews the report, concurs or non-concurs with findings, make closing remarks, and identify any corrective actions required. The closed report will be forwarded to the 439 AW/IP.

16.8. The appointing official directs a formal investigation when the initial inquiry is insufficient, and it is believed that more information can be obtained through a formal investigation. Refer to 439 AW/IP and 439 AW/SJA for assistance.

17. CUI. Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. Some examples of CUI are as follows: Law Enforcement Sensitive (LES), DoD Unclassified Controlled Nuclear Information (UCNI), Limited Distribution, as well as some of those developed by other Executive Branch agencies. For guidance on CUI refer to DoDI 5200.48 *Controlled Unclassified Information*, March 20208.

18. Security Education and Training. Commander or equivalents ensure that each individual receives continuing education and training throughout their duty assignment. Flight Commanders, division/branch chiefs, section heads, and supervisors will support and assist in training unit personnel.

18.1. Initial Training:

18.1.1. All newly assigned personnel will receive initial security training from the security assistant, during in-processing or before accessing classified material. Training will include cleared or un-cleared Information Security training. Training will be documented.

18.2. Continuing and Refresher Training:

18.2.1. Annual refresher training will be conducted IAW DoDM 5200.1_AFMAN 16-1404, Vol 3 Enclosure 5, par 7. Training will be documented.

18.2.2. Security assistants are encouraged to intermittently distribute training materials to unit personnel and, with the assistance of division/branch section chiefs, and supervisors, ensure all personnel are trained. The security assistant will maintain records identifying the names of personnel trained, subjects presented, and date(s) training were completed.

18.3. Specialized Training:

18.3.1. Security assistant, security container custodian (primary and alternate) and derivative classifiers to include SIPRNet users will complete specialized training as required. All personnel with SIPRNet access/accounts will be identified and trained by established procedures as derivative classifiers.

18.3.2. People needing specialized training should contact the security assistant to schedule training.

19. Safeguarding NATO Classified. No NATO classified information is currently being stored within any organization. Contact your Unit security assistant should a requirement arise to store, discuss, or process NATO classified material. All personnel that require “Access” will receive the

NATO Security Briefing and document the training utilizing the NATO Brief-Re-brief-Debrief Worksheet. Documentation will be maintained by the Security Assistant.

20. Marking Classified. Marking of Classified Information will be IAW DoDM 5200.01, AFMAN 16-1404, V2. Derivative classifiers will refer to the proper Security Classification Guides to ensure appropriate classified markings are in place. Any questions or concerns may be directed to 439 AW/IP at 413-557-2310.

21. Secure Communications. STE/OMNI terminals will be used by unit personnel to discuss classified and sensitive unclassified information.

21.1. Classified and Sensitive Unclassified information will not be discussed via a STE/OMNI in the presence of people not cleared for access to the information.

21.2. Conversations must be conducted at a volume where they will not be intercepted, intentionally or inadvertently, by unauthorized people.

21.3. STE/OMNIs will remain in the non-secure mode unless required for classified/unclassified sensitive information transmission.

21.4. The Wing Communication Security (COMSEC) Officer will provide STE/OMNI training and document the training prior to allowing personnel to use the STE/OMNI. See the unit secure voice responsible officer (SVRO) to coordinate training.

22. Security Self-Inspections. The security assistant will ensure security inspections are scheduled and conducted at the required intervals in Management Internal Control Toolset (MICT).

22.1. The unit commander or civilian equivalents will appoint an individual, to conduct an annual security inspection. A program review may satisfy the requirement for the annual inspections.

22.2. The security assistant will provide the Inspecting Official with the appropriate directives, self-inspection checklists, and any required guidance or assistance.

22.3. Inspecting Officials will document inspection results in a report to the commander.

22.4. After review and endorsement by the commander, the report will be returned to the security assistant for action, if required, and filed.

23. Review of personnel security clearance status. The security assistant will conduct a monthly review of the unit's DISS roster to monitor the 5-year SF 86 requirements and will direct any questions to 439 AW/IP.

23.1. Individuals notified to submit an Electronic Questionnaire for Investigations Processing (e-App) are responsible for completing and submitting all required investigative paperwork to 439 AW/IP upon completion. The security assistant will provide guidance/assistance in the preparation of the e-App. The 439 AW/IP will review/validate the package prior to submission.

23.2. The security assistant will be responsible for preparing the AF Form 2583.

23.3. The individual will complete the e-QIP package as soon as possible (not to exceed 30 days from notification) to avoid their investigation going out of scope. If fingerprints are required, have the individual contact 439 AW/IP for guidance.

24. SIF Establishment.

24.1. The supervisor and/or the security assistant will immediately notify the Commander when derogatory information is revealed, which could have an impact upon an individual's continued security eligibility. Senior Executive Agent Directive (SEAD) 3 list the reporting requirements for personnel with access to classified information or who hold a sensitive position.

24.2. Similarly, any individual who becomes aware of information that may call a person's loyalty, trustworthiness, and reliability into question (i.e., unexplained wealth, personal, criminal or immoral conduct, excessive use of alcohol, use of illegal drugs, mental or emotional instability, misuse of computers, etc.) must report such information to the Commander, security assistant or supervisor.

24.3. The Commander will review and evaluate the derogatory information against the standard security criteria as outlined DoD5200.02_DAFMAN 16-1405, *Department of Air Force Personnel Security Program Management*, 1 Aug 2018. Based on the facts available, the Commander will decide whether to establish a SIF and determine whether or not to suspend the individual's access to classified information/systems, withdraw unescorted access to restricted areas and access to the Local Area Network (LAN).

24.4. Unless otherwise specified by the Commander, the security assistant will act as liaison with 439 AW/IP on SIF actions.

25. Emergency Protection, Removal and Destruction of Classified Material. In case of emergency such as fire, bomb threat, natural disaster, civil disturbance, terrorist activities, or upon direction of the commander, Installation Control Center, or other authority, classified material will be returned to its security container and the container locked. When time is of the essence, material may be secured in any available security container, evacuated with the holder, or as a last resort, left behind. All personnel who work with classified information shall be aware of these procedures.

25.1. DO NOT risk injury or loss of life to secure classified material.

25.2. If the emergency is such that classified material cannot be secured, the holder will evacuate the area taking the material with them. The holder will notify the senior government official at the central evacuation point that they are holding classified material or that classified materials have been left unsecured in the work area. The holder will provide the location, type of classified (media, documents, etc.) and the approximate amount.

25.3. Protect the classified material until the emergency is terminated or take action to secure it in an approved security container. The individual who is responsible for returning the classified information to the proper security container unless otherwise directed by the commander or the security assistant.

25.4. Under no circumstances will the classified material be transported to the holder's private living quarters.

25.5. 439 AW/CP, Westover ARB, Building 1610, 750 Hangar Ave, Chicopee, MA 01022, may be used for the temporary storage of classified material.

25.6. Immediately following an emergency and by direction of the Commander or ranking officer, personnel will return to their work areas and check for any unsecured classified

information. Immediately report to the security assistant or the Commander when un-cleared emergency response personnel obtain access to classified or classified information is lost or destroyed. As soon as possible, obtain the names of all people entering the area for any debriefings which may be necessary.

25.7. In the event the facilities are made uninhabitable, the security assistant will advise the Commander/staff agency chief on protection alternatives.

25.8. During exercises, classified material will be secured prior to evacuation.

25.9. Emergency Action Plans.

25.9.1. Fire.

25.9.1.1. Whatever actions are taken, give the utmost consideration to the safety of personnel. Security of classified material is secondary.

25.9.1.2. Upon discovering a fire, call 911; notify personnel to evacuate the building and activate the manual fire alarm. Depart the facility and await the arrival of fire department (439 BCE/CEF) personnel at the designated assembly area.

25.9.1.3. Firemen will be granted access to fight the fire. Firemen ***will not*** be delayed entry to secure classified.

25.9.1.4. When the fire has been extinguished and facility reentry is permitted, take a complete inventory of the classified material to ensure it is still accounted for and in a usable condition. Immediately notify the security assistant of destroyed or unusable classified material and/or unauthorized access of classified information.

25.9.1.5. At no time during or after the event will other than authorized personnel be allowed to enter the area without the permission of the on-scene responsible official. Security Forces Squadron (SFS) representatives, if available, will assist in access control. Ensure they are advised if any classified material could not be secured.

25.9.1.6. When the emergency is over, obtain the names of all people entering the area for any debriefings which may be necessary. When facility reentry is permitted, take a complete inventory of classified information.

25.9.2. Natural Disaster.

25.9.2.1. Natural disasters of a magnitude that can disrupt operations can happen with little or no notice. Different types of occurrences will require different actions; thus, the senior person present must use good judgment to determine necessary actions. Whatever actions are taken, give utmost consideration to the safety of personnel and the security of classified material.

25.9.2.2. Many natural disasters are short-lived in nature (earthquakes, tornadoes, severe lightning storms, etc.), but can often create other emergency situations (fire, chemical spills, etc.). Remain alert to quickly changing situations.

25.9.2.3. Other disasters can occur which are not natural but can disrupt operations. Some of these include aircraft crashes, hazardous chemical spills, and radiological accidents. Protective measures for classified material, according to the situation, would be required in these instances also.

25.9.2.4. If a disaster should occur which requires implementation of emergency procedures, at no time during or after the event will other than authorized personnel be allowed to enter the area without the permission of the on-scene responsible official. 439 SFS and/or security representatives, if available, will assist in access control. Ensure they are advised of any classified material which cannot be secured.

25.9.2.5. When the emergency is over, obtain the names of all people entering the area for any debriefings which may be necessary. When facility reentry is permitted, take a complete inventory of classified information.

25.9.3. Bomb Threat.

25.9.3.1. The chances of a bomb threat occurring at WARB are possible. If such an event should occur, the senior person present must use good judgment to determine necessary actions. Whatever actions are taken, give utmost consideration to the safety of personnel and the security of classified material.

25.9.3.2. Bomb threats may be received by various means (e.g., telephone, letters, notes, etc.) which relates to the possible or actual presence of explosive devices. These threats must be considered factual and should be acted upon accordingly. Without prompt and decisive action by the recipient of the communication, the threat could result in injuries or fatalities and destruction of property. If the threat is a prank or hoax, the result will be a temporary disruption of operations.

25.9.3.3. Most bomb threats are received by telephone. The following general rules apply:

25.9.3.3.1. If possible, keep the caller on the phone as long as possible. Using the AF Form 440, *Bomb Threat Aid*, 1 November 1998, located at all telephones, make note of the person's vocal characteristics and background noises. Attempt to find out as many facts as possible about the explosive device.

25.9.3.3.2. DO NOT hang up the phone, even if the caller does.

25.9.3.3.3. If a bomb threat is received, use extreme caution in taking any action. Detonation devices come in many different forms, do nothing more than look for suspicious objects without moving anything. If evacuation is warranted, leave quickly and quietly, open doors carefully. Persons or animals trained in bomb detection will search for the device; this is NOT your responsibility.

25.9.3.3.4. If the communication is received in writing, do not excessively handle the correspondence. Handling the correspondence can easily interfere with law enforcement investigations.

25.9.3.3.5. At no time during or after the event will other than authorized personnel be allowed to enter the area without the permission of the on-scene responsible official. Security Forces and security representatives, if available, will assist in access control. Ensure they are advised if any classified material could not be secured.

25.9.3.3.6. When the emergency is over, obtain the names of all people entering the area for any debriefings which may be necessary. When facility reentry is permitted, take a complete inventory of classified information.

26. Personally Wearable Fitness Devices (PWFD) and Other Personal Portable Electronic Devices (PED) near Classified Processing or Discussion. The use of PED, including PWFD defined in DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, 23 April 2007, in collateral classified processing areas, is prohibited. This prohibition includes in proximity to classified discussion and where proper sanitization of the area or room has not occurred. Units should periodically screen their affected areas for unauthorized devices.

27. Reporting Requirements for Personnel with Access to Classified Information or who holds a Sensitive Position.

27.1. To meet requirements of SEAD 3, all individuals on WARB that have been granted "Access" to classified information must report all "unofficial" foreign travel. Any travel to Puerto Rico, Guam or other U.S. possessions and territories is not considered foreign travel and need not be reported. Unplanned day trips to Canada and Mexico shall be reported upon return.

27.2. AW Form 61, *Required Foreign Travel Reporting Form*, DTBD, part 1, must be completed and approve by Commander, through unit security manager/assistant prior to any foreign "unofficial" travel. While emergency circumstances may preclude full compliance with the pre-travel reporting requirements, the covered individual, at a minimum, shall verbally advise their supervisor/management chain of the emergency foreign travel with all pertinent specifics. In any event, full reporting shall be accomplished when returned.

27.3. AW Form 61, part 2 must be completed within 5 days of return, if possible, no later than the first UTA after travel.

27.4. Unit security manager will file the AW Form 61 in unit's ERM Records Disposition Schedule Table and Rule T-31-08: Security – Personnel Security Program.

27.5. Any Person "Read" into Top Secret (SAP) information will comply with their program managers respective instructions and need not duplicate reporting travel for collateral classified information.

28. Controlled unclassified information (CUI) ***DoDI 5200.48, March 6, 2020*** UNCLASSIFIED information is information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies.

28.1. Before making any document CUI the information must be verified through the CUI registry at **HTTPS://dodcui.dod.mil**

28.2. CUI training is an AF "Total Force Awareness Training" conducted annually and documented.

28.3. All CUI destruction will be in IAW Information Security Oversight Office (ISOO) CUI Notice 2019-03: Destroying Controlled Unclassified information (CUI) in paper form. Dated July 15, 2019.

28.4. For the single-step paper destruction method 439 AW units must: a. Use cross-cut shredders that produce 1 mm x 5 mm (0.04 in. x 0.2 in.) particles (or smaller); or b. Pulverize/disintegrate paper using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen.

28.5. The National Security Agency (NSA) maintains an Evaluated Products List (EPL) of equipment it authorizes to destroy hard copy (paper) Classified National Security Information. The most updated SA EPL for "Paper Shredders can be found at: **https://www.nsa.gov/resourccs/evervone/media-destruction/** or contact the 439 AW/IP for the up-dated EPL list.

29. Counter Insider Threat: The DoD Insider Threat Program DoDD 5205.16. Air Force Instruction 16-1402, 17 June 2020. The 439th Airlift Wing, Counter Insider Threat program establishes the following framework to integrate policies and procedures to detect, deter, and mitigate insider threats to national security and Air Force assets and establishes implementing guidance.

29.1. To ensure the protection of classified information or other information specifically prohibited by law from disclosure, covered individuals shall continuously evaluate personnel by alerting commanders/directors, security managers (assistants), or supervisors to the reportable activities of other covered individuals that may be of potential security or counterintelligence concern. For Reportable activates see Enclosure 6 to DoDM5200.02_DAFMAN16-1405_DAFGM2023-01 (v. 29 NOV 2023)

29.2. All suspected Counter Insider Threat's will be reported to the 439 AW/IPO. Once validated, The Wing IPO will be the only Wing agency to submit C-InT reports to AFRC Counter Insider Threat Program Manager who in turn will notify the Air Force counter-insider threat analysis center, referred to as the AF C-InT Hub.

29.3. Any CVIR reports down channeled from DOD CAS via DISS will be triaged by the 439 AW/IP to a potential imminent threat. Once assessed and triaged, based on the DAF C-InT hub references a generated report will be forwarded to AFRC for submittal and action.

29.4. Wing IPO will notify Unit Commanders of any mandatory reporting.

30. For procedures not covered in this AWI, contact the unit security or the 439 AW/IP office for guidance at 413-557-2310 or 413-557-2189.

GREGORY D. BUCHANAN, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 16-14, *Security Enterprise Governance*, 31 December 2019

DoDI 5200.48, *Controlled Unclassified Information (CUI)*, 6 March 2020

Security Executive Agent Directive 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*, (12 June 2017)

Security Executive Agent Directive 4, *National Security Adjudicative Guidelines*, (08 June 2017)

Security Executive Agent Directive 7, *Reciprocity of Background Investigations and National Security Adjudications*, (9 November 2018)

Security Executive Agent Directive 8, *Temporary Eligibility*, (18 May 2020)

Air Force (AF) Enterprise Authorizing Official Memorandum, *Subj; Personally Wearable Fitness Devices*,

Prescribed Forms

439AWForm 61, *Required Foreign Travel Reporting Form*

Adopted Forms

AF Form 310, *Document Receipt and Destruction Certificate*, 01 November 1995

AF Form 440, *Bomb Threat Aid*, 1 November 1998

AF Form 847, *Recommendation to change for Publication*, 22 Sep 2009

AF Form 2583, *Request for Personnel Security Action*, 4 April 2014

AF Form 2587, *Security Termination Statement*, 1 September 1981

DD Form 254, *Department of defense Contract security Classification Specification*, 1 January 1999

DD Form 2501, *Courier Authorization*, 1 March 1998

OF 89, *Maintenance record for Security Containers/Vault Doors*, 01 September1998

SF 312, *Classified Information Nondisclosure Agreement*, 1 July 2013

SF 700, *Security Container Information*, 1 April 2001

SF 701, *Activity Security Checklist*, 1 November 2010

SF 702, *Security Container Check sheet*, 1 August 1985

SF 704, *Secret Cover Sheet*, 01 August 1985

SF 705, *Confidential Cover Sheet*, 01 August 1985

Acronyms and Abbreviations

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRCVA—Air Force Reserve Command Visual Aid

AFRIMS—Air Force Records Information Management System

AFTO—Air Force Technical Order

ARB—Air Reserve Base

AW—Airlift Wing

AWI—Air Wing Instruction

CAC—Common Access Card

CC—Commander

CDSE—Center for Development of Security Excellence

CEF—Fire Department

COMSEC—Communication Security

CP—Command Post

CS—Communication Squadron

CUI—Controlled Unclassified Information

DAA—Designated Approval Authority

DD—Defense Department

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDM—Department of Defense Manual

DSS—Defense Security Service

EMSEC—Emissions Security

EPL—Evaluated Products List

e-QUIP—Electronic Questionnaire for Investigations Processing

FOUO—For Official Use Only

FSO—Facility Security Officer

GIG—Global Information Grid

GSA—General Services Administration

IAW—In Accordance With

InT—Insider Threat

CINT—Counter Insider Threat

IP—Information Protection

IPO—Information Protection Officer

LAN—Local Area Network

LES—Law Enforcement Sensitive

MA—Massachusetts

MICT—Management Internal Control Toolset

NATO—North Atlantic Treaty Organization

NSA—National Security Agency

OCA—Original Classification Authority

OF—Optional Form

OPM—Office of Personnel Management

OPR—Office of Primary Responsibility

OVI—Operation Visual Inspection

PED—Portable Electronic Devices

PR—Periodic Reinvestigation

PWFD—Personal Wearable Fitness Device

RDS—Records Disposition Schedule

SAP—Top Secret

SCXS—Communications Security

SEAD—Security Executive Agent Directive

SF—Standard Form

SFS—Security Forces Squadron

SIF—Security Information File

SIPRNet—Secret Internet Protocol Router Network

SJA—Staff Judge Advocate

SMO—Security Management Office

STE—Secure Telephone Equipment

SVRO—Secure Voice Responsible Officer

UCNI—Unclassified Controlled Nuclear Information

USB—Alternate Storage Memory

V—Volume

VGSA—Visitor Group Security Agreement

WARB—Westover Air Reserve Base

Office Symbols

439 AW/CC—439th Airlift Wing, Commander

439 AW/IP—439th Airlift Wing, Information Protection

439 AW/SE—439th Airlift Wing, Chief of Safety

439 AW/IG—439th Airlift Wing, Inspector General

439 CONF/PKI—439th Contracting Flight, Chief of Contracting

439 OG/CC—439th Operations Group, Commander

439 SFS—439th Security Forces Squadron