BY ORDER OF THE SUPERINTENDENT

HQ UNITED STATES AIR FORCE ACADEMY INSTRUCTION 16-1404

12 APRIL 2023

Operations Support

INFORMATION, PERSONNEL & INDUSTRIAL SECURITY PROGRAMS

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: HQ USAFA/IP

Certified by: HQ USAFA/IP (Bradley S. Wilson, Civ)

Supersedes: USAFAI16-1404, 9 September 2021

Pages: 16

This instruction implements Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*. This publication should be used in concert with DoDM 5200.01V1_AFMAN16-1404 Volume 1, *Information Security Program: Overview, Classification and Declassification*; DoDM 5200.01V2_AFMAN16-1404 Volume 2, *Information Security Program: Marking of Information*; DoDM 5200.01V3_AFMAN16-1404 Volume 3, *Information Security Program Protection of Classified Information*, DoDI 5200.48_DAFI16-1403, *Controlled Unclassified Information (CUI)*, DoDM 5200.02_AFMAN16-1405, *Air Force Personnel Security Program*, 2 Code of Federal Regulation (CFR) Part 117, *National Industrial Security Program Operating Manual (NISPOM)* and AFI16-201_USAFASUP, *Air Force Foreign Disclosure and Technology Transfer Program*. This collection of policy documents provides explicit guidance to execute CUI, information, personnel, and industrial security requirements at the local level. This publication applies to all Air Force, Space Force, civilian, and contractor personnel with access to controlled and classified information. This publication does not apply to Air Force Reserve Command (AFRC) units or the Air National Guard (ANG). Compliance with the attachments in this publication is mandatory. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*. This publication may not be supplemented or further implemented/extended. The authorities to waive requirements in this publication are identified with a Tier 1 (T-1) or Tier 2 (T-2) number following the compliance statement. See DAFMAN 90-161, *Publishing Processes and Procedures*, for a description of the authorities associated with the Tier number. Submit requests for waivers through the chain of command. The waiver authority for non-tiered requirements in this publication is HQ USAFA/IP. Ensure all records generated

from the requirements prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program* and disposed in accordance with the Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System.

1. Activity Security Manager and Security Program Executive (SPE).

1.1. The Director of Information Protection (HQ USAFA/IP) serves as the Activity Security Manager and Security Program Executive for USAFA as defined in DoDM 5200.01V1_AFMAN16-1404V1. The Information Security section (HQ USAFA/IPI) is responsible to and acts on behalf of the SPE for day-to-day management, oversight, and monitoring of the information security related programs.

2. Commanders/Directors.

2.1. Commanders/Directors will appoint a minimum of one primary and one alternate security assistant. Security assistants must have a minimum of a SECRET security clearance and at least 12 months of retainability. Civilian Unit Program Coordinators (UPC) should have security assistant duties identified in their Core Personnel Document (CPD).

2.2. Commanders/Directors will ensure security assistants conduct annual self-assessments, IAW AFI 90-201, *The Air Force Inspection System*, using the local Management Internal Control Toolset (MICT) Self-Assessment Checklist (SAC). The comprehensive local checklist contains requirements for the Controlled Unclassified Information (CUI), Information, Personnel, and Industrial Security Programs. Industrial security program requirements only apply to units with cleared contractors authorized access to classified information IAW a signed DD Form 254, *Department of Defense Contract Security Classification Specification.* Contact HQ USAFA/IP at 333-5601 or email USAFA/IP_for a list of authorized contractors with access to classified.

2.3. Commanders/Directors will ensure their unit Information Security Operating Instruction (OI) establishes training requirements for the receipt of accountable mail [USPS registered, certified, express, and first-class mail with "Return Service Requested" on the outside, or GSA authorized contractor for overnight delivery (i.e., FEDEX or UPS)]. Procedures will ensure sensitive mail is only opened by designated personnel listed on AF Form 4332, *Accountable Communications Receipt Authorization,* immediately upon receipt, or secured in an approved GSA container. Personnel not listed on AF Form 4332 are not authorized to accept nor open any form of sensitive mail or parcel. Refer to DoDM 5200.01V3_DAFMAN16-1404V3, Enclosure 4 for additional requirements.

2.3.1. Units processing and/or storing classified information must ensure their unit operating instruction include provisions for safeguarding classified information during emergency situations. Emergency procedures must be posted near the security container, SIPRNet terminal or classified processing area (CPA). See **Attachment 2** for an example of an emergency plan.

2.4. Commanders/Directors will incorporate on-site contractors into their unit security programs. They must ensure all personnel (military, civilians, and contractors) complete *DoD Initial Orientation and Awareness Training*, *DoD Annual Security Awareness Training* and annual *Derivative Classification Training* as determined by position sensitivity and scope of

duties. See **paragraph 7** Security Education and Training, for an explanation of training requirements.

2.5. Commanders/Directors will ensure unit in-processing/out-processing checklists include coordination with the unit security assistants. The unit security assistants will require access to vMPF to out-process personnel. These actions are critical to maintaining an accurate accountability of personnel in Defense Information System for Security (DISS).

2.6. Commanders must provide an updated "*Security Container Custodian Designation and Access Authorization*" letter to HQ USAFA/IPI, within 30 days of any change (addition/deletion) in personnel with knowledge of, or access to, their GSA security container combination. Contact HQ USAFA/IP at 333-6342 or email at: **usafa.iptaskers@us.af.mil** for an electronic copy of the "*Security Container Custodian Designation and Access Authorization"* letter.

2.7. Commanders/Directors will ensure personnel who require access to Critical Nuclear Weapon Design Information (CNWDI) complete the CNWDI Indoctrination Form. The unit security assistant must indoctrinate the member for both Restricted Data (RD) and CNWDI in DISS prior to access. When the member no longer requires access to CNWDI, debriefed the member using the same form and remove both RD and CNWDI access in DISS. The signed CNWDI Indoctrination Form must be maintained in unit security files for one year following access to CNWDI and RD. (T-1) Unit security assistants can obtain the CNWDI Indoctrination form from HQ USAFA/IP by calling 333-6342 or email at: **usafa.iptaskers@us.af.mil**.

3. Unit Security Assistants.

3.1. Newly appointed security assistants must complete computer-based training (CBT) prior to attending classroom training conducted by HQ USAFA/IP staff.

3.1.1. DISS is the system of record for personnel security actions and clearance verification. The following CBTs are required for DISS orientation and are located at: **https://securityawareness.usalearning.gov/diss-training/index.html**

3.1.1.1. Module 1: Welcome to DISS

3.1.1.2. Module 4: Subject Management

3.1.1.3. Module 5: Clearance Eligibility and Granting Access

3.1.1.4. Module 8: Visit Requests

3.1.1.5. Module 9: JVS System Reports

3.1.1.6. Module 11: Removing SMO Relationships and Debriefing Access

3.1.2. The National Background Investigation Service (NBIS) system must be utilized to initiate all security background investigations (formerly accomplished utilizing eQIP). The following modules are required for NBIS orientation and are located at: **https://nbistraining.countermeasures.com/courses/home**.

3.1.2.1. NBIS Overview and General Tasks

3.1.2.2. Initiate-Review-Authorize (IRA)

3.1.2.3. Access

3.1.2.4. Interims

3.1.2.5. Visit Management

3.1.2.6. Service Catalog and Active Tasks

3.1.3. Security assistants must also complete the *"Identifying and Safeguarding Personally Identifiable Information (PII) Version 3.0"* CBT course located at: **https://securityawareness.usalearning.gov/piiv2/index.htm**. Personally Identifiable Information (PII) is controlled unclassified information (CUI) and must be marked and safeguarded accordingly. This course will assist security assistants with understanding PII requirements.

3.1.4. Security assistants must send all training certificates to the HQ USAFA/IP organization mailbox **usafa.iptaskers@us.af.mil** before attending classroom training.

3.2. Security assistants must receive approval from their Cybersecurity Liaison (CSL) before connecting any computers, copiers, audiovisual, projectors or similar equipment to the SIPRNet, or other classified equipment or components. Any device introduced to classified information (SIPRNet or another classified device) must be safeguarded and secured as a classified component. (T-2)

3.2.1. SIPRNet Trusted Thin Clients (TTC). Unit using a TTC supplied by 10 CS are not required to store them in a GSA approved container, as long as the SIPRNet token is removed. No user data or applications are stored on the TTC. All data accessed by the end user is stored and processed remotely. Security protections prevent data from being transferred between classification levels.

3.2.2. Security assistants and their CSL will identify procedures to purge memory from reproduction equipment and determine if the toner cartridge retains any part of the classified data. If memory/toner cannot be purged, the device CANNOT be used for classified reproduction, unless specifically approved by the commander. Similarly, if procedures to sanitize the reproduction equipment and/or toner cartridge have not been identified, both components must be safeguarded until confirmed. **NOTE:** Any leased equipment or devices on contract that do not have volatile memory cannot be used for classified processing or reproduction. The unit commanders will designate and approve reproduction equipment in writing. Contact the Cybersecurity Office at 333-9880 or email USAFA/A6 (Cyber Security) if you have any questions pertaining to device capability or for clarification on the latest guidance. (T-1)

3.2.3. Security assistants will label all IT equipment, components, devices, disks, and hard drives in classified processing areas with one of the following labels:

3.2.3.1. SF 706, *"TOP SECRET"*

3.2.3.2. SF 707, "*SECRET"*

3.2.3.3. SF 708, *"CONFIDENTIAL"*

3.2.3.4. SF 710, *"UNCLASSIFIED"*

3.2.3.5. Contact HQ USAFA/IP at 333-6342 for labels.

3.3. Security assistants will verify members are indoctrinated and granted access in DISS before granting physical access to classified information or to classified information systems.

3.3.1. Security assistants will ensure members have eligibility, a need-to-know, a signed Standard Form 312, *Classified Information Nondisclosure Agreement,* on file in DISS and completed *DoD Annual Security Awareness Training,* before granting access to SECRET or TOP SECRET information. Security Assistants will use SAR Codes found on the Unit Manpower Document (UMD) to establish need-to-know and level of access. Contact the HQ USAFA/IP at 333-2405 or email at **usafa.iptaskers@us.af.mil** for assistance.

3.3.1.1. SF 312s should be signed digitally. If digitally signed by the member, there is no requirement for a witness or attestation signature.

3.3.1.2. Completed SF 312s by military members must be uploaded in DISS prior to mailing the form to AFPC.

3.3.1.2.1. Send all SF 312s completed by military members to the following address:

HQ AFPC/DP1ORM
550 C ST, WEST, SUITE 21
JBSA-Randolph, TX 78150

3.3.1.3. SF 312s completed by civilian members must be uploaded into DISS.

The member also needs to upload a copy into their eOPF via myPers. SF 312s for civilians do not have to be mailed.

3.4. Security assistants will maintain a security electronic file folder as part of their unit's official file plan. The electronic files will contain the documents listed below along with accompanying *AFRIMS* RDS disposition instructions for each: (T-2)

3.4.1. Security assistant appointment letter. (T-2)

3.4.2. A list of storage containers, vaults, and secure rooms. The list will include the primary and alternate custodian, as well as members authorized the combination to the container(s) signed by the unit commander/director. (T-2) Contact HQ USAFA/IP for an electronic copy of the *Security Container Custodian Designation and Access Authorization* memorandum. Call 333-6342 or email at: **usafa.iptaskers@us.af.mil**.

3.4.3. A copy of the unit's security operating instruction. (T-2)

3.4.4. A signed copy of the most recent HQ USAFA/IP self-inspection report.

3.4.5. Security assistant training certificates. (T-2)

3.4.6. Units with cleared contractors requiring access to classified information in performance of assigned duties will maintain a copy of the associated DD FM 254, *Department of Defense Contract Security Classification Specification*, and Visitor Group Support Agreement or, Memorandum of Understanding Security Requirements, as applicable. (T-2)

3.4.7. AF IMT 2587, *Security Termination Statement.* Upon retirement, termination of employment, suspension of access to classified information, or administrative withdrawal of security clearance eligibility, cleared personnel must be provided a termination briefing

and sign the AF IMT 2587. The original copy is given to the member for his or her final out-processing appointment. Maintain the forms for two years IAW *AFRIMS* RDS, Table 31-04, Rule 13.00.

3.4.8. Previous 3 months of SF 701, *Activity Security Worksheet* and SF 702, *Security Container Work Sheet.*

3.5. Security assistants will ensure self-assessments are accomplished IAW the latest HQ USAFA/IG and HQ USAFA/IP policy. (T-2)

3.6. Security assistants will provide oversight of classified meetings and discussions conducted by their assigned personnel. Security assistants will provide a copy of the classified meeting/discussions checklist to the cleared member hosting the discussion/meeting and will verify attendee eligibility for access to classified in DISS prior to the start of the classified meeting/discussion. The classified meeting/briefing checklist can be obtained from DoDM 5200.01V3_AFMAN 16-1404V3, Appendix 1 to Enclosure 2.

4. Cleared Members.

4.1. Members with access to national security information or hold sensitive positions are obligated to self-report specific life events on themselves and on other cleared members IAW Security Executive Agent Directive (SEAD) 3. A copy of SEAD 3 reporting requirements can be located at **https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf**

4.2. Periodic Reinvestigations (PR). Maintaining security clearance eligibility is a personal responsibility. PRs are required every 5 years for both SECRET and TOP SECRET security clearances. Personnel have 14 duty days to complete their PRs, upon notification from the security assistant or HQ USAFA/IP. Extensions must be approved by the commander/director via an email to USAFA/IP (Org Mail).

5. Contractors.

5.1. Security assistants will establish either an "Owning" or "Servicing" relationship with all on-site contractors under their purview in DISS. Refer to the *"Help"* tab at the top of the DISS landing page for step-by-step instructions for adding and removing relationships.

5.1.1. If the contractor does not require access to classified, select, or create the category titled "Non-DoD Affiliated Contractor." Once created, add an "Owning" relationship under the Non-DoD Affiliated Contractor category.

5.1.2. For contractors associated with an approved DD FM 254 and requires access to classified, add a relationship by selecting the "Industry" category. Upon selecting "Industry" add a "Servicing" relationship and make sure to select their current contract company.

5.1.2.1. Review DISS to ensure cleared contractors working under DD Form 254 authorization and with access to classified have an SF 312, *Classified Information Non-disclosure Agreement* (NdA), annotated and have been granted access (indoctrinated), by their company's Facility Security Office (FSO) before granting physical or administrative access to classified information or classified information systems on USAFA.

6. Security Containers.

6.1. Security container custodians must maintain SF 700, *Security Container Information* (**Part 1**), for each security container (safe) and/or for each locking drawer of a multi-drawer security container. Part II of the SF 700 must be completed, marked SECRET, and courtesy stored in a different container. Combinations for empty safes and drawers of a multi-drawer container will be reset to 50-25-50 and NOT left unlocked. Contact HQ USAFA/IP at 333-6342 for assistance.

6.1.1. Units with COMSEC containers will follow COMSEC disposition rules. (T-2)

6.2. Security assistants will ensure security container custodian(s) maintain an OF 89, *Maintenance Record for Security Containers/Vault Doors,* inside each container/safe. An OF 89 is specific for each container and will be used to document all maintenance performed by a certified GSA technician.

6.2.1. Security container custodian(s) will conduct an annual visual inspection of each security container, safe, utilizing DoDM5200.01V3_DAFMAN16-1404V3, Appendix 2 to Enclosure 3, *"Security Container and Vault Door Visual Inspection Checklist."* Documentation (Memo For Record or email to Security Assistants) of the visual inspection must be uploaded into MICT and made available upon request or during HQ USAFA/IP annual inspection.

6.2.2. The Information Protection Office (IPO) will assist security assistants in contacting a certified GSA technician when a container malfunctions or is not operating properly. If a container malfunctions, all classified holdings must be immediately transferred to another GSA container or secure room.

6.3. The Commander/Director must notify the IPO when a vault or secure room is no longer used for classified storage. (T-2)

6.4. **Annual Cleanout.** Each unit with classified holdings must dedicate at least one day each year to dispose of any unneeded classified material ("clean-out day"). For USAFA, the annual clean-out day will be the second Friday of July each year. Security container custodians will document completion on a memorandum for record, which will be maintained in the security assistant file plan.

7. Security Education and Training.

7.1. All DoD civilians, military and on-site contractors shall receive security training based on the member's authorization, position sensitivity and scope of duties. All training will be completed utilizing the following url: **https://securityawareness.usalearning.gov**. Members must provide training certificate(s) to their Unit Training Manager (UTM) for documentation and training metrics in myLearning. (T-2). Security training metrics will be verified by HQ USAFA/IP during annual inspections. Security training requirements have been incorporated in the HQ USAFA/IP local MICT checklist.

7.1.1. *DoD Initial Orientation and Awareness Training:* Initial orientation must occur within 90 days of employment start date. All personnel, regardless of access requirements, must receive initiation information security orientation.

7.1.2. *DoD Annual Security Awareness Refresher*: Required by ALL active duty and civilians in SAR code 5 and 7 positions, and contractors authorized access to classified

IAW an approved DD Form 254. Refer to your UMD to confirm SAR code positions for civilians and contact the HQ USAFA/IP Industrial Security Program Manager at 333-5601 or email at **usafa.iptaskers@us.af.mil**) to confirm contractors access to classified.

7.1.3. *Derivative Classification Training:* Required by everyone (military, civilian and contractors) with a SIPRNet or Global Combat Support System (GCCS) account. Every SIPRNet user is responsible for properly marking classified emails and documents transmitted or saved on SIPRNet. Contact HQ USAFA/IP at 333-6342 or email at **usafa.iptaskers@us.af.mil** for the latest list of SIPRNet Users.

7.1.4. *DoD Mandatory Controlled Unclassified Information (CUI) Training*: Accomplished through myLearning and required by every military, civilian and contractor with access or the potential to access CUI. Personally Identifiable Information (PII), Health Information, Personnel Records and Student Records are examples of CUI. Refer to the Information Security Oversight Office (ISOO) CUI Registry for a comprehensive list of CUI. **https://www.archives.gov/cui/registry/category-list**.

7.1.5. *Insider Threat (InT) Awareness Training:* Required by all personnel (military, civilians, and contractors) within 30 days of hire and annually thereafter IAW AFI 16-1402, *Insider Threat Program Management*, **Paragraph 3.3**.

7.2. ***National Atlantic Treaty Organization (NATO) Awareness Training*:** Required by all SIPRNet users (military, civilian and contractors) and members who deploy where NATO forces are serving. The NATO Awareness Indoctrination Form can be digitally signed, must be saved to unit security assistant e-files, and maintained until the member leaves the organization. Security assistants will indoctrinate members for *"SECRET (NATO)"* access after signing the indoctrination form and debrief the member in DISS when NATO access is no longer required.

7.3. ***Foreign Disclosure (FD) Awareness Training*:** IAW AFI 16-201_USAFASUP, paragraph 1.3.7.4.1., the Dean of Faculty, (USAFA/DF) and Information Protection (USAFA/IP) Directorate's Foreign Disclosure Officer (FDO) will ensure all DF assigned personnel [likely to come into contact with Foreign Nationals (FN)] receive initial and annual refresher FD awareness training. FD awareness training will be documented to include the date and names of attendees.

8. Security Incidents.

8.1. The basic security incident response procedures are to ensure classified information and/or material found unattended, is immediately secured, and kept under constant surveillance or stored in an approved GSA container.

8.2. Unit personnel must be trained to ensure a data spill (classified information found on an unclassified system) includes the immediate disconnection of computers from the ethernet, or disconnect from WIFI/VPN, to prevent the further transmission of the classified information to other unclassified systems.

8.3. Unit personnel must be trained/informed to immediately notify unit security assistants and HQ USAFA/IP at 333-6342 when a suspected security incident has occurred.

8.4. Inquiry officials may be granted an extension to allow more time to complete the inquiry or investigation. The Director, Information Protection grants the extensions. (T-1)

9. Destruction of Classified Material and Components.

9.1. Security assistants must ensure all shredders used for the destruction of classified material are on the approved National Security Agency/Central Security Service NSA/CSS Evaluated Products List (EPL). The EPL is located at: **https://www.nsa.gov/Resources/Media-Destruction-Guidance/NSA-Evaluated-Products-Lists-EPLs/**.

9.2. The destruction of any classified information technology (IT) components (laptops, hard drives, external hard drives, etc.) requires coordination with your unit Information Technology Equipment Custodian (ITEC). The ITECs must accomplish the following procedures prior to degaussing (destroying) classified IT components:

9.2.1. Complete the 'Turn-In' request process through IT Accountability.

9.2.2. Include the following in the e-mail transaction:

9.2.2.1. Unit Security Assistant

9.2.2.2. Unit Cybersecurity Liaison (CSL)

9.2.2.3. HQ USAFA/IP (Org Mail)

9.2.2.4. HQ USAFA/A6 (Cybersecurity)

9.2.2.5. The member turning in the IT component(s)

9.2.2.6. The security clearance information of the person turning in the component(s)

10. Destruction of CUI.

10.1. **There are two authorized methods to destroy CUI paper documents.**

10.1.1. Mobile shredding companies, such as U-Shred It, is an approved method for destruction of CUI. CUI is required to be safeguarded behind at least one locked physical barrier (desk or office) until properly destroyed.

10.1.2. Classified shredders are also an approved method to destroy CUI. Refer to the NSA/CSS approved product list for approved shredders to destroy classified and CUI material. **https://www.nsa.gov/Resources/Media-Destruction-Guidance/NSA-Evaluated-Products-Lists-EPLs/**

10.2. Shredders not listed on the NSA/CSS are not authorized to destroy CUI or classified information.

11. Self-Inspections (SI).

11.1. HQ USAFA/IP will conduct annual self-inspections on units that create, process and/or handle classified information. Units that do not create, process, or handle classified information will receive a SI every two years. The SI will be conducted using a single and comprehensive local MICT checklist to assess information, personnel, and industrial security programs.

11.2. **SI reports will include a summary of findings.** Commanders/Directors will provide HQ USAFA/IP a response to SI finding(s) every 30 days until closed. The Inspector General Enterprise Management System (IGEMS) may be used to identify findings.

BENJAMIN R. JONSSON, Colonel, USAF
Vice Superintendent

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 16-201_USAFASUP, *Air Force Foreign Disclosure and Technology Transfer Program,* 3 August 2015

AFI 16-1402, *Counter-Insider Threat Program Management,* 16 June 2020

AFI 33-322, *Records Management and Information Governance Program,* 27 July 2021

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

DAFI 90-201, *The Air Force Inspection System,* 19 November 2018

DAFMAN 90-161, *Publishing Processes and Procedures,* 14 April 2022

DoDM 5200.01V1_AFMAN16-1404 Volume 1, *Information Security Program: Overview, Classification and Declassification,* 5 April 2022

DoDM 5200.01V2_AFMAN16-1404 Volume 2, *Information Security Program: Marking of Information,* 6 January 2021

DoDM 5200.01V3_AFMAN16-1404 Volume 3, *Information Security Program Protection of Classified Information,* 11 April 2022

DoDI 5200.48_DAFI16-1403, *Controlled Unclassified Information (CUI),* 4 October 2021

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

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

AF Form 2587, *Security Termination Statement*

AF Form 4332, *Accountable Communications Receipt Authorization*

DD Form 254, *Department of Defense Contract Security Classification Specification.*

Optional Form 89, *Maintenance Record for Security Containers/Vault Doors*

Standard Form 86, *Questionnaire for National Security Positions*

Standard Form 312, *Classified Information Nondisclosure Agreement*

Standard Form 700, *Security Container Information*

Standard Form 701, *Activity Security Worksheet*

Standard Form 702, *Security Container Work Sheet*

Standard Form 704, *SECRET Coversheet*

Standard Form 705, *CONFIDENTIAL Coversheet*

Standard Form 706, *TOP SECRET Label*

Standard Form 707, *SECRET Label*

Standard Form 708, *CONFIDENTIAL Label*

Standard Form 710, *UNCLASSIFIED Label*

Abbreviations and Acronyms

AF—Air Force

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

ANG—Air National Guard

CBT—Computer Based Training

CE—Continuous Evaluation

COMSEC—Communications Security

COMPUSEC—Computer Security

CNWDI—Critical Nuclear Weapon Design Information

CPA—Classified Processing Area

CPD—Core Personnel Document

CSL—Cybersecurity Liaison

CUI—Controlled Unclassified Information

CV—Continuous Vetting

DISS—Defense Information System for Security

DIP—Director of Information Protection

EPRM—Enterprise Protection Risk Management

eOPF—Electronic Official Personnel Folder

eQIP—Electronic Questionnaire for Investigations Processing

GCCS—Global Command and Control System

GSA—General Services Administration

FSO—Facility Security Officer

IGEMS—Inspector General Enterprise Management System

IO—Inquiry Official

InT—Insider Threat Training

IP—Information Protection

IPI—Information Protection Section

IPO—Information Protection Office

ISSO—Information Security Oversight Office

IT—Information Technology

ITEC—Information Technology Equipment Custodian

JCAVS—Joint Clearance and Access Verification System

JPAS—Joint Personnel Adjudication System

JVS—Joint Verification System

MICT—Management Internal Control Toolset MICT

NATO—National Atlantic Treaty Organization

NBIS—The National Background Investigation Service

NdA—Non-disclosure Agreement

OI—Operating Instruction

OPR—Office of Primary Responsibility

PII—Personally Identifiable Information

RD—Restricted Data

RDS—Records Disposition Schedule

RFA—Request for Action

SAC—Self Assessment Checklist

SAR—Security Access Requirement

SI—Self Inspection

SIPRNet—Secret Internet Protocol Router Network

SMO—Security Management Office

SPE—Security Program Executive

STEPP—Security Training, Education, and Professionalization Portal

UMD—Unit Manpower Document

UPC—Unit Program Coordinator

USAFA—United States Air Force Academy

vMPF—Virtual Military Personnel Flight

VPN—Virtual Private Network

WIFI—Wireless Fidelity

Terms

Term—Definition

Classified Message Incident—A higher classification level of data is transferred to a lower classification level system/device via messaging systems (i.e., email or instant messaging).

Classified Information Spillage—Security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification. (Committee on National Security Systems Instruction No. 4009).

CNWDI—A DoD designation for TOP SECRET or SECRET RD weapon data revealing the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munitions, or test device.

Data Spillage—Occurs whenever classified information or CUI is transferred onto an information system not authorized for the appropriate security level or not having the required CUI protection or access controls. For example, when a user takes a file such as a word document and copies it to removable media (e.g., DVD or CD) from SIPRNET and then the user takes that media and loads the data onto a NIPRNET computer. A classified data spillage is a security violation. A data spillage is not necessarily a CMI.

Degaussing (or Demagnetizing)—Process for reducing the magnetization of a storage device to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored data unreadable and unintelligible, and ensuring that it cannot be recovered by any technology known to exist. (National Security Agency/Central Security Service Policy Manual 9-12).

Information Protection—Information Protection is a subset of the Air Force Security Enterprise and consists of the core security disciplines (Personnel, Industrial, and Information Security) used to determine military, civilian, and contractor personnel's eligibility to access classified information, ensure the protection of classified information released or disclosed to industry in connection with classified contracts, and protect classified information and CUI that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security.

Restricted Data (RD—All data concerning design, manufacture, or utilization of nuclear weapons; the production of Special Nuclear Material (SNM) and the use of SNM for production of energy, but not data declassified or removed from the RD category pursuant to section 2162 of The Atomic Energy Act of 1954, as amended.

Remanence Security—Residual information remaining on data media after clearing. (Committee on National Security Systems Instruction No. 4009).

Security Access Requirement (SAR) Code—The Security Access Requirement code identifies the day-to-day level of access to classified information required by the position.

Sensitive Information—Information that the loss, misuse, or unauthorized access to or

modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Department of Defense 5400.11-R but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept SECRET in the interest of national defense or foreign policy. **Note:** Systems that are not national security systems, but contain sensitive information are subject to be

protected according to the requirements of the Computer Security Act of 1987 (Public Law 100-235). (Committee on National Security Systems Instruction No. 4009).

Attachment 2

EMERGENCY PLAN FOR CLASSIFIED INFORMATION/MATERIAL

A2.1. Emergency Plan

Emergency plans to protect classified information/material in case of fire, natural disaster, civil disturbance, terrorist activities or enemy action to minimize the risk of compromise and for the recovery of classified information are required IAW DoDM5200.01V3_DAFM16-1404V3; *Information Security Program Protection of Classified Information*, Enclosure 2; paragraph 10.

This guide should be used as a quick reference to aid in determining whether to return the material to the security container or to hand-carry until declared safe. Personnel who access classified material should be aware of the appropriate actions to take while balancing personal safety along with the need to continually safeguard the material. Include this guide with unit security operating instructions and post it in or in proximity to the classified area.

EVENTS MOST LIKELY TO OCCUR AT USAFA	TIME AVAILABLE	NO TIME AVAILABLE
1. A fire has been reported in the immediate area.	Return to Security Container	Hand-carry with discretion
2. A tornado has been reported in the immediate area.	Return to Security Container	Hand-carry with discretion
3. An explosion has occurred in the immediate area.	Hand-carry with discretion	Leave it & protect yourself
4. A bomb threat has occurred in the immediate area.	Return to Security Container	Hand-carry with discretion
5. An active shooter situation has occurred in the immediate area.	Return to Security Container	Leave it & protect yourself
6. A prolonged electrical outage has occurred.	Return to Security Container	N/A

TIME CONSTRAINTS: If time is available to return the classified material to a security container, ensure it is locked. When hand-carrying classified material outside a secure environment, ensure it is not readily identifiable by placing it in a folder, case, or some other unmarked medium. Maintain control of the material until it can be returned to a security container.